

8>

Станислав СМЫШЛЯЕВ
«КРИПТО-ПРО»
Лев ШУМСКИЙ
Ассоциация ФинТех
**Безопасная
с фундамента**



12>

Василий ПИСКАРЕВ
Госдума РФ
**«Суверенный интернет»
и киберэтика**



18>

Артем СУДАРЕНКО
Банк России
Ожидается новая норма

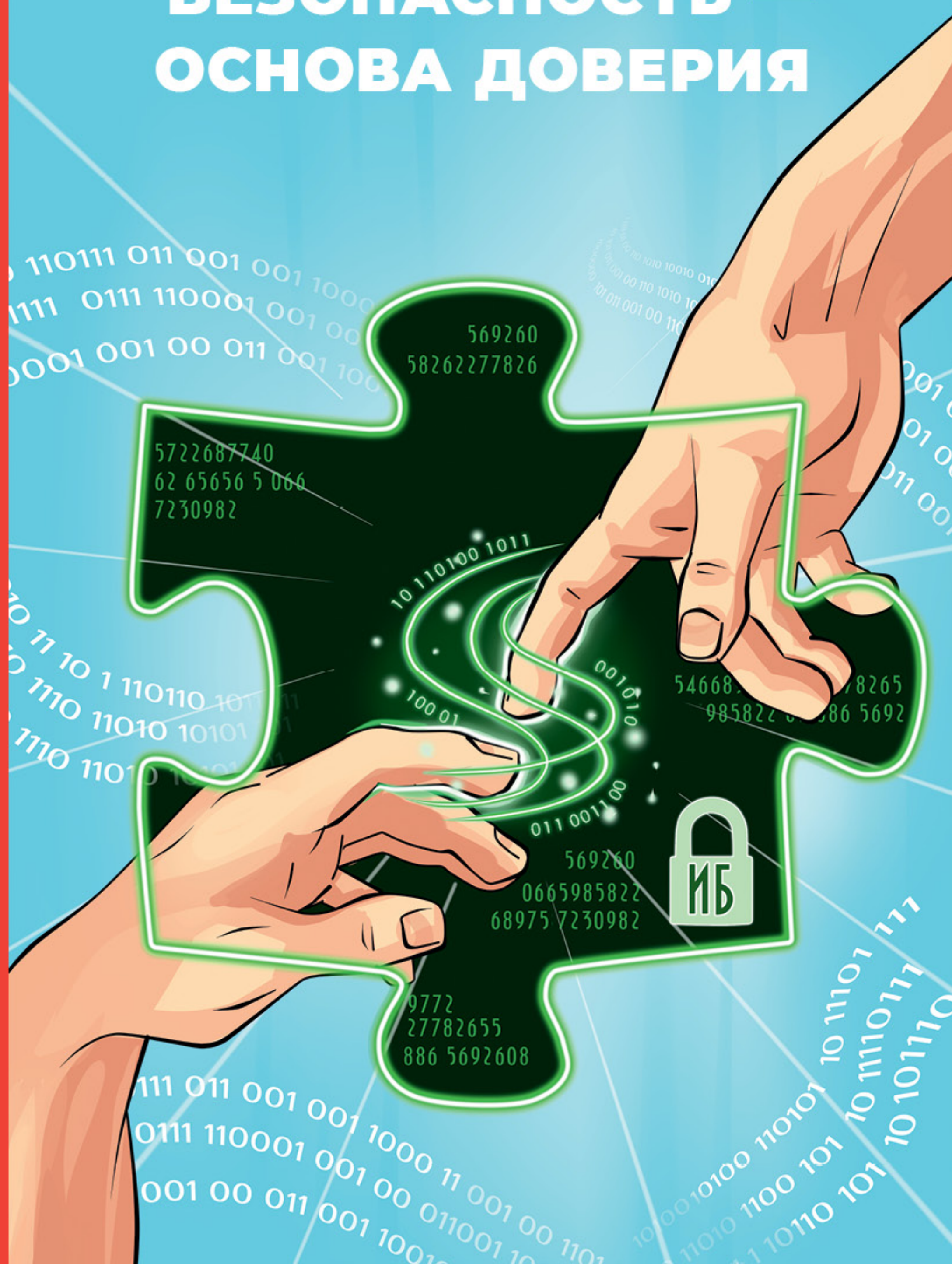
84>

Татьяна НИКИТИНА
МЧС России
**Цифровая
модернизация ОБЖ**

113>

Александр БОДРИК
MoscowCyber.io
**Московская
кибер-шпана**

ВСТРОЕННАЯ БЕЗОПАСНОСТЬ — ОСНОВА ДОВЕРИЯ



**ПРАКТИКА ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ
И ПОСТРОЕНИЯ ЦЕНТРОВ МОНИТОРИНГА ИБ**



SOC-ФОРУМ 2019

19–20 ноября 2019 года, г. Москва,
Конгресс-парк гостиницы
«Рэдиссон Коллекшн Отель Москва»

Регистрация:
SOC-FORUM.IB-BANK.RU



Павел БЫЛЕВСКИЙ

шеф-редактор
BIS Journal

Электронными сервисами, в том числе финансовыми, пользуются уже подавляющее большинство граждан, независимо от профессии, возраста и принадлежности к социальным группам. Но огромные преимущества цифрового, информационного общества оказались обременены кибеугрозами, деятельностью криминалитета и злоумышленников. Существуют многочисленные и разнообразные киберугрозы имущественного, финансового и репутационного ущерба для граждан.

Одним из новомодных решений в сфере информационной безопасности является встроенная защита. Прекрасно, когда пользователь не тратит время на поиск дополнительных средств, не беспокоится об их совместимости со своим устройством и программным обеспечением. Просто делает своё дело, особенно не задумываясь, как не допустить технических сбоев и не поддаться на уловки злоумышленников. Безопасность обеспечивается как бы сама собой, но на самом деле для этого необходимы тщательно разработанные решения и их регулярное обновление.

Однако и самому пользователю необходима своего рода «встроенная защита». А именно понимание угроз, которые сопутствуют очевидным преимуществам цифровой среды, знание правил безопасности и привычка их выполнять. Специалисты могут только подсказать пользователю, что и как нужно делать, но потрудиться ему придётся самому.

Государственные и корпоративные возможности обеспечивать информационную безопасность должны дополняться киберграмотностью граждан в сфере их личной ответственности. В настоящее время государственные органы, включая систему образования, компании, оказывающие электронные услуги, общественные организации формируют систему массового обучения киберграмотности.

Создаются учебные курсы, методические пособия, обучаются педагоги, развиваются различные формы обучения и каналы информирования населения. Киберграмотность становится важной составляющей «гражданской обороны» в сфере электронных сервисов и киберсреды. Без неё трудно представить дальнейшее успешное развитие информационного общества, цифровой экономики, электронных сервисов.

Каждый гражданин должен осознать угрозы, изучать новейшие приёмы злоумышленников, знать, как не дать себя облапошить. Ликвидировать свою безграмотность в вопросах информационной безопасности, овладеть этой культурой. И тогда эти необходимые навыки будут работать автоматически, не хуже, чем встроенная защита компьютерно-телекоммуникационных сервисов и устройств.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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

Сычёв А.М. — Первый заместитель директора Департамента информационной безопасности Банка России, доктор технических наук

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

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

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

Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПО», 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 Групп «Авангард», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)

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

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

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

Музипов Ф.Х. — председатель правления НП «ПСИБ»

Некрасов И.В. — главный редактор журнала

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

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

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

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

ЭКСПЕРТНАЯ ГРУППА

Одувалов М.В. — эксперт BIS Journal

Филипчук А.А. — технический директор ГК ЦРТ

Калашникова Е.В. — Банк ВТБ (ПАО)

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**

Шеф-редактор: **Былевский П.Г.**

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

Арт-директор: **Мельников Н.С.**

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

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

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

Куликов В.А., Бродская М.А., к.т.н.

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

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

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

Цветокорректор: **Наumenko М.Б.**

Корректор: **Бальтерманц Л.Ф.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Групп «Авангард»

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

Координаты: 55.779380, 37.611150

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 № ФС77-61378 от 10 апреля 2015 г. Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность банков».

Перепечатка и воспроизведение иными способами без разрешения редакции запрещаются. При использовании материалов ссылка на журнал обязательна. Мнение редакции может не совпадать с мнением авторов. Присланные материалы не рецензируются и не возвращаются.

Подписан в печать 05.07.2019. Тираж 7000 экз.

Заказ №24219. Цена договорная.

Отпечатан в типографии

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

© BIS Journal, 2019



НОВОСТИ

5 В России, в мире, криминал

ТЕМА НОМЕРА

8 **Встроенная безопасность**
Станислав Смышляев (КРИПТО-ПРО),
Лев Шумский (Ассоциация ФинТех)
Безопасная с фундамента

РЕГУЛЯТОРЫ

- 12 **Законодательство**
Василий Пискарев
(Государственная Дума РФ)
«Суверенный интернет» и киберэтика
- 18 **Нормативно-правовая база**
Артём Сударенко (ФинЦЕРТ Банка России)
Ожидается новая норма
- 20 **КИИ**
Сергей Вихорев (ИТ-Экспертиза)
Дайте мне точку опоры, и я поверну...

БАНКИ

- 26 **Круглый стол**
Анна Воробьева (BIS Journal)
Видеть на 360°
- 29 **Точка зрения**
Василий Дягилев (Check Point)
GENERATION V
- 31 **Технологии**
Диана Князева (Сбербанк)
Безбумажный банк
- 35 **Биометрия**
Максим Федотенко (Сбербанк)
**Технология защиты от угрозы
подмены биометрического сканера**
- 44 **Импортозамещение**
Александр Баранов (НИУ ВШЭ)
Главное — выбрать направление удара
- 47 **Импортозамещение**
Алексей Смирнов (Базальт СПО)
Технологическая независимость в ИТ
- 50 **Импортозамещение**
Дмитрий Горелов (Актив),
Станислав Смышляев (КРИПТО-ПРО)
**Отечественная криптография
в Рунете**



УГРОЗЫ И РЕШЕНИЯ

54 Платформы

Виктор Сердюк, Роман Ванерке
(ДиалогНаука)
Цифровая киберразведка

56 Защита

Антон Тихонов (ГК MONT)
Увидеть невидимое

59 Профиль компании

Дмитрий Новиков (ITP Services)
**Наш бизнес – предоставление
эффективных сервисов для
противостояния киберугрозам**

60 Управление сетью

Екатерина Степанова,
Анастасия Петлякова (АМТ-ГРУП)
Куда? кому? как? в вашей сети

62 Комплаенс

Дмитрий Кандыбович (StaffCor)
Система особого назначения

ИНФРАСТРУКТУРА

64 Деловые мероприятия

Валерия Мещерякова (BIS Journal)
СТCrypt 2019

66 Деловые мероприятия

Никифор Ковалёв (BIS Journal)
Sberbank ICC 2019

69 Деловые мероприятия

Антон Реут (BIS Journal)
«Код ИБ» в Москве 2019

70 Деловые мероприятия

Николай Кольский (BIS Journal)
CISO Форум 2019

71 Деловые мероприятия

Марк Новоначный (BIS Journal)
Think Summit Москва

72 Деловые мероприятия

Валерия Мещерякова (BIS Journal)
Наличные в XXI веке

74 Деловые мероприятия

Павел Никифоров (BIS Journal)
Critical Communications Russia 2019

76 Биометрия

Сергей Мельников (Лингвистические
и информационные технологии)
Задача по биометрии: кто написал txt?



HI-HUME

- 80 Психология**
Лев Палей (эксперт ИБ)
ИБ-психолога вызывали?
- 82 Новации**
Павел Былевский (BIS Journal)
Ожидаем прибавления
- 84 Культура ИБ**
Татьяна Никитина (МЧС России)
Предмету ОБЖ — цифровую модернизацию

ОБРАЗОВАНИЕ И КАРЬЕРА

- 87 Просвещение**
Марина Бродская (BIS Journal)
Хакеры-«просветители»
- 90 Мысли вслух**
Валерий Куликов (BIS Journal)
Что нам мешает обустроить ИТ- и ИБ-образование?
- 92 Обзор**
Екатерина Зобова (ФСРБИТ)
Накануне
- 94 Обзор**
Марина Бродская (BIS Journal)
Мировая проблема



80



98

СУБЪЕКТЫ

- 98 История**
Борис Столпаков (историк криптографии)
Завод Кулакова
- 103 История**
Борис Столпаков (историк криптографии)
Радиомолчание порой дороже золота
- 109 Кейсы ИБ**
Анастасия Скогорева (BIS Journal)
Чёрное зеркало
- 113 Заметки безопасника**
Александр Бодрик (MoscowCyber.io)
Московская кибер-шпана
- 114 BIS TV**
Тамара Чечёткина (BIS TV)
Подсевшие на Игру
- 116 Портрет читателя**
Молодой, образованный, любящий IT



114

ЗАПРЕТ НА ФОТО

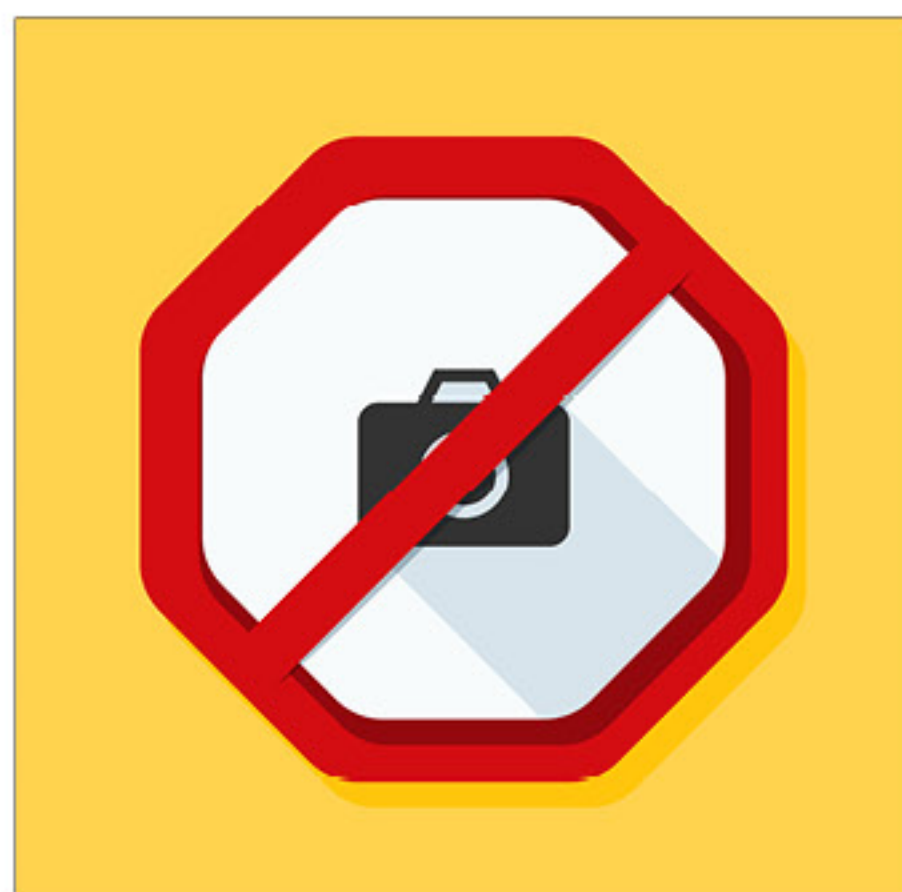
«Сбербанк», ВТБ, «ЮниКредит» и «ФК Открытие» запретили сотрудникам фотографировать экраны компьютеров с личных мобильных устройств. Сам факт съёмки, однако, доказать очень тяжело.

Заместитель руководителя лаборатории компьютерной криминалистики Group-IB Сергей Никитин считает, что такой запрет — способ борьбы с «пробивом» данных о клиентах. Хакеры размещают объявление в даркнете, чтобы выяснить баланс карты жертвы, паспортные данные и другое. Фотографии с данными стоят от 800 до 8 тыс. рублей, и делают их сообщники мошенников — инсайдеры в разных банках.

Директор департамента информационной безопасности «ФК Открытие» Владимир Журавлёв считает, что на основе фотографий персональных данных клиентов можно изготовить поддельные документы. Их могут использовать для снятия денег с чужо-

го счёта и участия в мошеннических схемах.

Зампред «Сбербанка» Станислав Кузнецов рассказал, что системы банка обычно не позволяют передавать служебные данные в третьи руки: «Если им удалось по какой-то причине передать это преступникам, мошенникам либо третьим лицам, мы передаем материалы в правоохранительные органы».



НАРУШЕНИЯ НАЙДЕНЫ ВО ВСЕХ БАНКАХ

Банк России обнаружил нарушения требований кибербезопасности во всех проверенных банках в 2018–2019 годах. Об этом рассказала глава Банка России Эльвира Набиуллина на Международном конгрессе по кибербезопасности ICC.

С прошлого года Банк России как регулятор имеет полномочия осуществлять надзор за финансовыми институтами с точки зрения того, как они выполняют требования по кибербезопасности.

«В прошлом году мы проверили 58 банков, в этом году 75, и во всех

были найдены проблемы. Нарушения — нельзя сказать, что критические, но они могут стать серьезными, если финансовые институты не будут придавать этому значения», — отметила Эльвира Набиуллина.

«Цифры, например, в финансовом секторе, в целом, показывают достаточно благополучную ситуацию. Да, в прошлом году, например, у нас уровень атак вырос на 30%. Но потери пока, которые декларированы финансовыми институтами, это две тысячи процентов», — сказала она.



ЕЩЕ ОДИН НАЦПРОЕКТ

В России создадут Национальную стратегию развития искусственного интеллекта. Соответствующий проект Минкомсвязь разработала совместно со Сбербанком и экспертным сообществом, сообщил глава регулятора Константин Носков.

«Стратегию обсудили на площадке Аналитического центра при правительстве, учли ряд предложений экспертов», — сказал Носков. Он уточнил, что это будет отдельный федеральный проект по искусственному интеллекту в рамках национальной программы «Цифровая экономика». Поручение внести в правительство проект Национальной стратегии по развитию искусственного интеллекта дал по итогам совещания в конце мая президент Владимир Путин.



БАНКОМАТЫ УСТАРЕЛИ

79% банкоматов в России устарели и не поддерживаются производителями. Об этом на открытии OFFZONE 2019 рассказал директор блока экспертных сервисов BI.ZONE Евгений Волошин.

Для устранения имеющихся уязвимостей в таких банкоматах производители советуют просто менять их на новые. Соответственно, банкам приходится самостоятельно разрабатывать аппаратные закладки для устранения брешей. Однако и тут есть проблема: только крупные банки могут позволить себе лаборатории, на базе которых возможно создать такие закладки.

Чтобы избежать серьёзных финансовых потерь, банкам следует тщательно заботиться о защищённости встраиваемых систем. В помощь руководителям и ИБ-специалистам BI.ZONE представил результаты глобального обзора компании — отчет «Атаки на встраиваемые системы».

ВЗЛОМАЛИ КРУПНЕЙШЕГО

Агрегатор контента Flipboard заявил о взломе. Хакеры уже второй раз за год получили доступ к его пользовательским данным. Ежемесячная аудитория сервиса составляет 150 млн человек.

Кроме этого, по словам представителей Flipboard, злоумышленники, по всей вероятности, сделали копии некоторых баз данных в период с июня 2018 года по март 2019 года, а также 21 и 22 апреля нынешнего года. Это были базы с важными сведениями об учетных записях пользователей (адреса электронной почты, никнеймы и пароли). Flipboard сбросил все пароли пользователей, поэтому при следующем входе надо будет создать новый пароль для аккаунта.



КОЛЛЕКТИВНЫЙ ИСК ПРОТИВ APPLE

Три пользователя iTunes из Род-Айленда и Мичигана подали в суд Сан-Франциско на компанию Apple. Мотив: корпорация раскрывает и продает персональные данные жителей этих штатов без их согласия.

Согласно заявлению истцов, любой человек может приобрести сортируемый по полу, возрасту и музыкальным предпочтениям список пользователей iTunes. Сам иск подан от имени сотен тысяч жителей обоих штатов.

Требования к Apple заключается в выплате 250 долларов за каждого пострадавшего клиента из Род-Айленда и по 5000 долларов за каждого жителя Мичигана, чьи данные были раскрыты. Такой разброс в размерах компенсаций вызван различиями в законодательствах штатов о персональных данных. Apple пока не предоставили комментариев ситуации.

ИРАНСКИЕ ХАКЕРЫ АТАКУЮТ США

Иран существенно усилил кибератаки на правительственные учреждения и объекты критической инфраструктуры США. По данным специалистов CrowdStrike и FireEye, за последние несколько недель хакерские группировки, предположительно работающие на иранское правительство, засыпали американские госучреждения и нефтегазовые компании фишинговыми письмами.

Пик атак был зафиксирован после введения в июне администрацией Дональда Трампа санкций в отношении иранских нефтехимических компаний. Фишинговые письма были замаскированы под легитимные, но содержали малвари. Одни из них выдавались за приглашения от Исполнительного офиса президента на должность экономического советника. Другие носили более общий характер и маскировались под уведомления от Microsoft Outlook об обновлении адресной книги. Об успешности кибератак не сообщается.

Эксперты из CrowdStrike назвали группировку, стоящую за атаками, Refined Kitten. Уже не первый год она атакует энергетический и оборонный секторы США, Саудовской Аравии и ОАЭ.



ДЕНЬГИ ПОШЛИ... К СТАРТАПАМ

Стартапы IronScales, Vade Secure и Valimail, специализирующиеся на борьбе с фишингом, за одну неделю привлекли совокупно \$139 млн.

Калифорнийский сервис Valimail, проверяющий подлинность входящих

сообщений, привлек 45 млн долларов от венчурной компании Insight Partners. Общая сумма инвестиций в стартап теперь составляет 84 млн долларов. Они пойдут на расширение сервиса до международного уровня и найм новых инженеров.

Израильский стартап IronScales, использующий ИИ для обнаружения спама и атак на ИТ-системы, собрал 15 млн долларов — лидером раунда инвестиций стала K1 Investment Management.

Калифорнийская компания Vade Secure, предупреждающая о фишинговых сайтах и вирусах, получила 79 млн долларов от General Catalyst и основателя маркетинговой компании Neolane Стефана Дитриха.

Генеральный директор Valimail Александр Гарсия-Тобар подчеркнул, что его стартап не будет конкурировать с этими компаниями. С одной из них, возможно, он договорится о сотрудничестве.



ШИФРОВАЛЬЩИК ВЕРНУЛСЯ

Group-IB зафиксировала новые масштабные атаки вируса-шифровальщика Troldeh (Shade) на российские компании. Злоумышленники отправляют письма от имени сотрудников крупных авиакомпаний, автодилеров и СМИ. Только в июне обнаружено более 1100 фишинговых писем, содержащих Troldeh, всего же во втором квартале 2019 года их количество превысило 6 000.

Troldeh, также известный под именами Shade, XTBL, Trojan.Encoder.858, Da Vinci, No_more_ransome — это вирус, который шифрует файлы на устройстве пользователя и требует выкуп за восстановление доступа к информации. Его центр управления размещен в сети Tor и постоянно перемещается. Troldeh продается и сдается в аренду в даркнете. Теперь он не только шифрует файлы, но еще майнит криптовалюту и генерирует трафик на веб-сайты для увеличе-



ния посещаемости и доходов от онлайн-рекламы.

Масштаб атак во втором квартале 2019 почти в 2,5 раза больше, чем за весь 2018-й год. На июнь пришелся новый пик активности. Письма, содержащие Troldeh, отправляются якобы с почтовых ящиков авиакомпаний (например, «Полярные авиалинии»), автодилеров («Рольф») и от СМИ (РБК, Новосибирск-online).

ЭЛЕМЕНТЫ КИБЕРВОЙНЫ

По данным надежного источника, были зафиксированы кибератаки иностранных спецслужб на российские системы управления транспортом, банковской сферой и энергетикой. Источник назвал их «элементами кибервойны» и отметил, что активность иностранных спецслужб в последние годы стала нарастать. «Однако эти действия нам удастся нейтрализовать», — добавил он.

15 июня газета The New York Times со ссылкой на источники в администрации США сообщила, что Вашингтон пытался осуществить кибератаки

на российские системы управления энергосетями. Издание отмечало, что американские власти наблюдали за российскими сетями с 2012 года, однако в этом году их стратегия стала более агрессивной. Дональд Трамп отверг эту информацию и обвинил газету в госизмене.

Комментируя эту статью, в Минэнерго России заявили, что им не поступало сообщений об атаках на объекты энергетики. В министерстве отметили, что российские энергетические компании самостоятельно обеспечивают защиту своих информационных ресурсов от кибератак.



ВСПЛЫЛИ БАЗЫ ДАННЫХ ТРЕХ БАНКОВ

Личные данные 900 тыс. клиентов «ОТП банка», «Альфа-банка» и «ХКФ банка» оказались в открытом доступе. Сами банки заявили, что об источнике этих баз данных не знают и организовали проверки.

В двух базах содержатся данные клиентов «Альфа-банка». В одной — сведения о более чем 55 тыс. клиентов: ФИО, телефоны, домашний и рабочий адреса. В другой — 504 записи. Кроме ФИО и телефонов она содержит паспортные данные и остаток на счете в отделении «Альфа-банка», ограниченный диапазоном 130–160 тыс. рублей. Базы находятся в открытом доступе как минимум с мая 2019 года. Еще одна база содержит сведения о 24,4 тыс. клиентов «ХКФ банка». База «ОТР банка» содержит данные о 800 тыс. человек по всей России: ФИО, телефоны, почтовые адреса и другую информацию.

В ЧЕЛЯБИНСКЕ ПОЙМАЛИ ХАКЕРА

Центральный районный суд Челябинска вынес приговор жителю города, который с помощью вредоносного ПО незаконно получал доступ к пользовательским данным граждан.

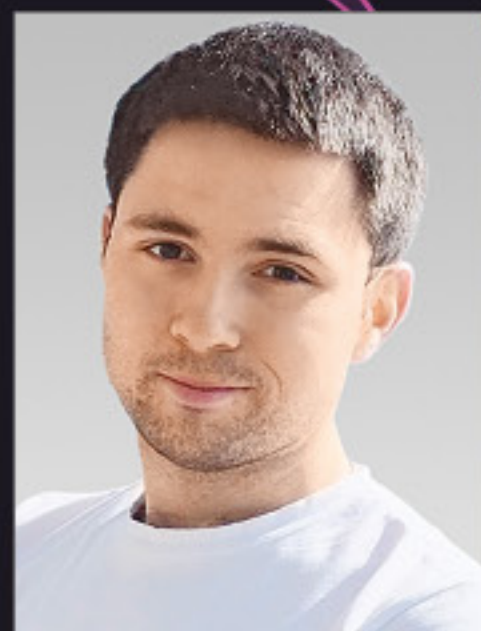
С помощью вредоносных программ злоумышленник получал доступ к личной информации в электронных платежных системах, а также учетным записям в социальных сетях. Однако снять деньги ему помешали сотрудники УФСБ по Челябинской области.

Суд признал мужчину виновным по ч. 1 ст. 272 (неправомерный доступ к компьютерной информации), ч. 1 ст. 273 (создание, использование и распространение вредоносных компьютерных программ) и назначил наказание в виде 10 месяцев ограничения свободы.

Новости подготовили
Анна Воробьева и Валерия Мещерякова

БЕЗОПАСНАЯ С ФУНДАМЕНТА

ВСТРОЕННАЯ БЕЗОПАСНОСТЬ
И ПЕРСПЕКТИВЫ ПЛАТФОРМЫ
МАСТЕРЧЕЙН



Станислав СМЫШЛЯЕВ
директор по информационной
безопасности компании
«КРИПТО-ПРО», к. ф. – м. н.



Лев ШУМСКИЙ
директор по
информационной безопасности
Ассоциации ФинТех



Ассоциация ФинТех (АФТ) готовит блокчейн-платформу Мастерчейн к промышленной эксплуатации. В ближайшее время должна завершиться её сертификация на соответствие требованиям ФСБ. Первые пилотные банковские сервисы на платформе заработали ещё в 2018 году, и участники Ассоциации готовы расширять количество проектов.

Минувший 2018-й стал для глобального блокчейн-сообщества годом открытий. С одной стороны, интерес к технологии растёт: стартовал ряд заметных проектов, бизнес и государства анонсировали амбициозные планы. По данным IDC¹, глобальные инвестиции в блокчейн в 2018 году выросли почти

на 60% и превысили 1,5 млрд долл. С другой стороны, технологией всерьёз заинтересовались киберпреступники: по данным американской компании CipherTrace², в 2018 году хакеры атаковали блокчейн и криптобиржи, похитив свыше 950 млн долларов — в 3,6 раз больше, чем в 2017 году.

ПЛАТФОРМА ДЛЯ РОССИЙСКИХ БАНКОВ

По данным компании Group-IB, специализирующейся на кибербезопасности, в 2018 году в 70% случаев хакеры атаковали именно финансовый сектор³. По мнению экспертов, одна из причин этих атак — в том, что банки неспособны централизованно управлять своей сетью. Технология распределённых реестров приносит в финансовую среду новые надёжные способы защиты информации. Операции, которые фиксируются в блокчейне, нельзя незаметно подделать или изменить. Кроме того, технология позволяет ускорить запуск новых услуг, упрощает процедуры финансовой отчётности и внутреннего финансового контроля, помогает оптимизировать затраты на проведение транзакций, повышает лояльность потребителей.

Особенность Мастерчейна в том, что эта платформа удовлетворяет требованиям российского законодательства в области ИБ, в частности, № 63-ФЗ «Об электронной подписи» и приказу ФСБ № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра». Здесь используется российская криптография, и в 3-м квартале 2019 года завершается процедура её сертификации в ФСБ в соответствии с требованиями к средствам криптографической защиты информации (СКЗИ).

ПЕРВАЯ ПРОМЫШЛЕННАЯ ПЛАТФОРМА

В рамках пилотных проектов «Учет электронных закладных», «Цифровая банковская гарантия», «Цифровой аккредитив» на платформе Мастерчейн участники АФТ уже создали несколько десятков узлов блокчейн-сети. Осенью 2018 года Сбербанк и Райффайзенбанк, а затем и другие участники АФТ (Банк ВТБ, «Дом.рф» и Ак Барс Банк) провели первые сделки по учёту электронных закладных. В начале 2019 года Абсолют Банк выпустил цифровую банковскую гаран-

¹ [http://www.tadviser.ru/index.php/Статья:Блокчейн_\(мировой_рынок\)](http://www.tadviser.ru/index.php/Статья:Блокчейн_(мировой_рынок))

² https://ciphertrace.com/wp-content/uploads/2019/01/crypto_aml_report_2018q4.pdf

³ <https://www.group-ib.ru/media/banks-readiness/>

тию на поставку продуктов питания в Медсанчасть №59 Федерального медико-биологического агентства России.

Летом начнётся промышленная эксплуатация децентрализованной депозитарной системы (ДДС) на Мастерчейне. В первую волну запуска вошли шесть компаний: Райффайзенбанк, Сбербанк, Газпромбанк, ГК «Регион», Ак Барс Банк и Абсолют Банк. При этом нет необходимости пересматривать внутренние регламенты и процедуры: финансовые структуры давно работают с отечественной криптографией, их системы соответствуют требованиям регуляторов.

ПЛАТФОРМА, БЕЗОПАСНАЯ НА ФУНДАМЕНТАЛЬНОМ УРОВНЕ

Встраивание российских криптографических алгоритмов вместо зарубежных при построении систем — самая простая и незначительная из переработок. Действительно, включить в комплект поставки российского криптопровайдера и перенаправить на него криптографические вызовы — дело нехитрое. Но для соответствия требованиям ФСБ России к средствам криптографической защиты информации (СКЗИ) этого ничтожно мало.

Так и Мастерчейн, изначально основанный на платформе Ethereum, для соответствия российским требованиям был переработан с нуля в части информационной безопасности, включая ролевую модель, ключевую систему, протоколы установления защищенных соединений, принципы аутентификации и авторизации, а также протоколы сопряжения с подсистемами обработки конфиденциальных данных.

В соответствии с действующими требованиями, при криптографической защите должны использоваться «... криптографические механизмы, утверждённые в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований». В Мастерчейне целостность данных обеспечивается в соответствии с ГОСТ Р 34.11–2012 «Функция хэширования» (алгоритм, кстати, является частью международного стандарта ISO/IEC 10118–3), а электронная подпись — в соответствии с ГОСТ Р 34.10–2012. При этом сохранены свойственные платформе неканонические алгоритмы формирования и проверки электронной подписи: ради них с чистого листа провели анализ стойкости.

На существующих блокчейн-платформах, как правило, не уделяют должное внимание стандартным для СКЗИ вопросам обеспе-

чения защиты от несанкционированного доступа к функциям, ключам и самой обрабатываемой информации. В Мастерчейне это учли: были существенно переработаны такие процедуры, как идентификация/аутентификация пользователей при доступе к подписи транзакций и включении блоков, аутентификация узлов при доступе, контроль целостности программного обеспечения и ключевой информации.

Аутентификация субъектов при доступе к узлам обеспечивается с помощью протокола TLS с учётом методических рекомендаций Технического комитета 26 (ТК 26) МР 26.2.001–2013 «Использование наборов алгоритмов шифрования на основе ГОСТ 28147–89 для протокола безопасности транспортного уровня (TLS)» и рекомендаций по стандартизации Р 1323565.1.020–2018 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)» с использованием дополнительных ролей, указываемых в сертификатах.

Сертификаты (отдельно для каждого из выполняемых в рамках работы системы протоколов) выпускает уполномоченный удостоверяющий центр по шаблонам с дополнительными идентификаторами — при выполнении операций они позволяют определить наличие у владельца ключа соответствующих разрешений.

Локальный доступ при этом возможен только для выполнения задач конфигурирования и обслуживания узла администраторами безопасности (сети или организации).

Дополнительная авторизация основана на хранящемся в блокчейне особом смарт-контракте. Он содержит белый список пользователей, который определяет роль каждого субъекта и доступные для него операции. Менять этот список может администратор по информационной безопасности при добавлении/исключении пользователей из системы.

Существующие блокчейн-платформы не предусматривают ни смену ключей (причём как в случае истечения срока действия, так и в случаях компрометации), ни специальную защиту ключей при их хранении. Но в Мастерчейне реализован и используется криптопровайдер «КриптоПро CSP» (или даже «КриптоПро HSM»), благодаря чему выполняются требования по контролю целостности, проверкам сроков действия ключей, работе с сертификатами, с датчиками случайных чисел, аудиту и реализации всех криптографических протоколов. Конечно, такие требования к верхнеуровневым модулям, как отображение

подписываемых документов и безопасная работа с криптографическим ядром, выполняются в коде прикладных компонент Мастерчейн в полном объёме.

Одна из важных возможностей, реализованных в Мастерчейне, — работа с конфиденциальными данными. Обеспечение ролевого доступа — классическая задача, не вызывающая трудностей. Хранение и управление правами доступа непосредственно в блокчейне — тоже. Но вот как быть с необходимым для блокчейн-платформы обеспечением неизменности конфиденциальных данных?

Разумное решение — хранить сам документ в отдельном выделенном хранилище с фиксацией некоторого «отпечатка» документа в блокчейне. Однако первое напрашивающееся решение с хранением хеш-значения от документа не выдерживает критики: несмотря на то, что стойкую хеш-функцию на практике обратить невозможно, это не действует, когда про хешируемые данные известно почти всё. Например, если единственными конфиденциальными данными в некотором документе является PIN-код из четырёх цифр, то по значению хеша и известному формату документа восстановить этот PIN-код можно за 10 тысяч вычислений значения хеш-функции — то есть мгновенно.

Поэтому в Мастерчейне в виде «отпечатков» используются не хеш-значение, а код аутентификации сообщения HMAC (hash-based message authentication code) по Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хеширования». Целостность и неизменность данных он обеспечивает, как и хеш-функция, а за счет хранящегося в секрете случайного 256-битового вектора предотвращает возможность восстановить документ по его «отпечатку» методом перебора.

Подводя итог, Мастерчейн можно без преувеличения назвать примером *secure by design* системы, построенной с самого фундамента с учётом требований по информационной безопасности. Криптографические механизмы и протоколы проанализированы в релевантных моделях нарушителя, реализация всей криптографической защиты проверена по требованиям ФСБ России по классам КС1 и КС2.

СВЕТЛОЕ ЗАВТРА БЛОКЧЕЙНА

Мастерчейн не заменит все классические базы данных и системы электронного документооборота. Но он одновременно обеспечивает

*Мастерчейн можно без преувеличения назвать примером *secure by design* системы, построенной с самого фундамента с учётом требований по информационной безопасности*

конфиденциальность и надёжное хранение данных при безопасной аутентификации каждого субъекта, юридическую значимость — а значит, возможность реализовывать на одной платформе все те проекты, которые раньше требовали бы «ручного» совмещения технологий с отдельным аудитом безопасности. Причём уделяя всё внимание прикладному функционалу, а не реализовывая и сертифицируя своими руками всё, начиная с самого фундамента.

Мировой опыт показывает, что технологию блокчейн можно использовать в разных отраслях экономики. Например, в 2018 году Министерство энергетики США пообещало создать на технологии распределённых реестров систему безопасности электростанций. Она призвана предотвращать удалённые атаки на системы электроснабжения. В Китае на базе блокчейна и интернета вещей (Internet of things, IoT) разработан сервис кредитования под залог автотранспорта.

Да и в сфере финансов заявлен ряд революционных проектов. Например, компания Visa анонсировала создание на блокчейне альтернативы системе межбанковского взаимодействия SWIFT (Society for Worldwide Interbank Financial Telecommunications). Компания предлагает использовать для международных P2P-переводов и B2B-платежей блокчейн-платформу Visa B2B Connect. Канадский и сингапурский центробанки смогли провести трансграничный перевод, используя разные блокчейн-сети (Corda и Quorum соответственно).

* * *

По данным ЕГРЮЛ, в России на январь 2018 года было зарегистрировано 50 юрлиц, использующих технологию блокчейн. Среди сфер деятельности, помимо финансов и ИТ, указывались право, оптовая торговля, услуги дополнительного образования. Очевидно, что в будущем технология получит широкое распространение — а платформа Мастерчейн обеспечит при этом высокий уровень защищённости информации.



Василий ПИСКАРЕВ
председатель комитета
Госдумы РФ по безопасности
и противодействию
коррупции

«СУВЕРЕННЫЙ ИНТЕРНЕТ» И КИБЕРЭТИКА

НОВЫЕ ПОДХОДЫ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В этом году в России отметили 25-летие национального сегмента интернета. За четверть века в этой сфере мы шагнули далеко вперед. Сегодня, по данным статистики, Рунет насчитывает 109 млн пользователей «всемирной паутины» и 6 млн веб-страниц в доменных зонах.ru,.rf,.su¹. Интернет прочно вошел в нашу повседневную жизнь, позволяя, не выходя из дома, посетить библиотеку и получить необходимую информацию, оплатить коммунальные услуги, послать открытку другу, или совершить видеозвонок.

Однако наряду с множеством полезных качеств, интернет открывает и массу возможностей для совершения противоправных действий — распространения недостоверной информации, пропаганды экстремистских и террористических идей, рекламы наркотиков.

РОССИЯНАМ — СУВЕРЕННЫЙ РУНЕТ

Федеральный закон от 1 мая 2019 года № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных техно-



логиях и о защите информации»² журналисты окрестили «законом о суверенном интернете». Объясню, почему Комитет по безопасности и противодействию коррупции поддержал его концепцию.

Цель принятия закона — обеспечить создание инфраструктуры, которая сохранит работоспособность отечественных интернет-ресурсов в случае, если российским операторам связи будет перекрыт доступ к корневым серверам интернета за рубежом. В условиях применяемого западными странами в отношении России санкционного режима и такое развитие событий исключить нельзя. Как недавно образно заметил глава Правительства России Дмитрий Медведев, необходимо, чтобы «не мы отключили, а чтобы нас не отклю-

¹ <https://riamo.ru/article/351506/yubilej-runeta-kak-vyglyadeli-poiskoviki-i-sotsseti-20-let-nazad.xl>

² <http://publication.pravo.gov.ru/Document/View/0001201905010025>



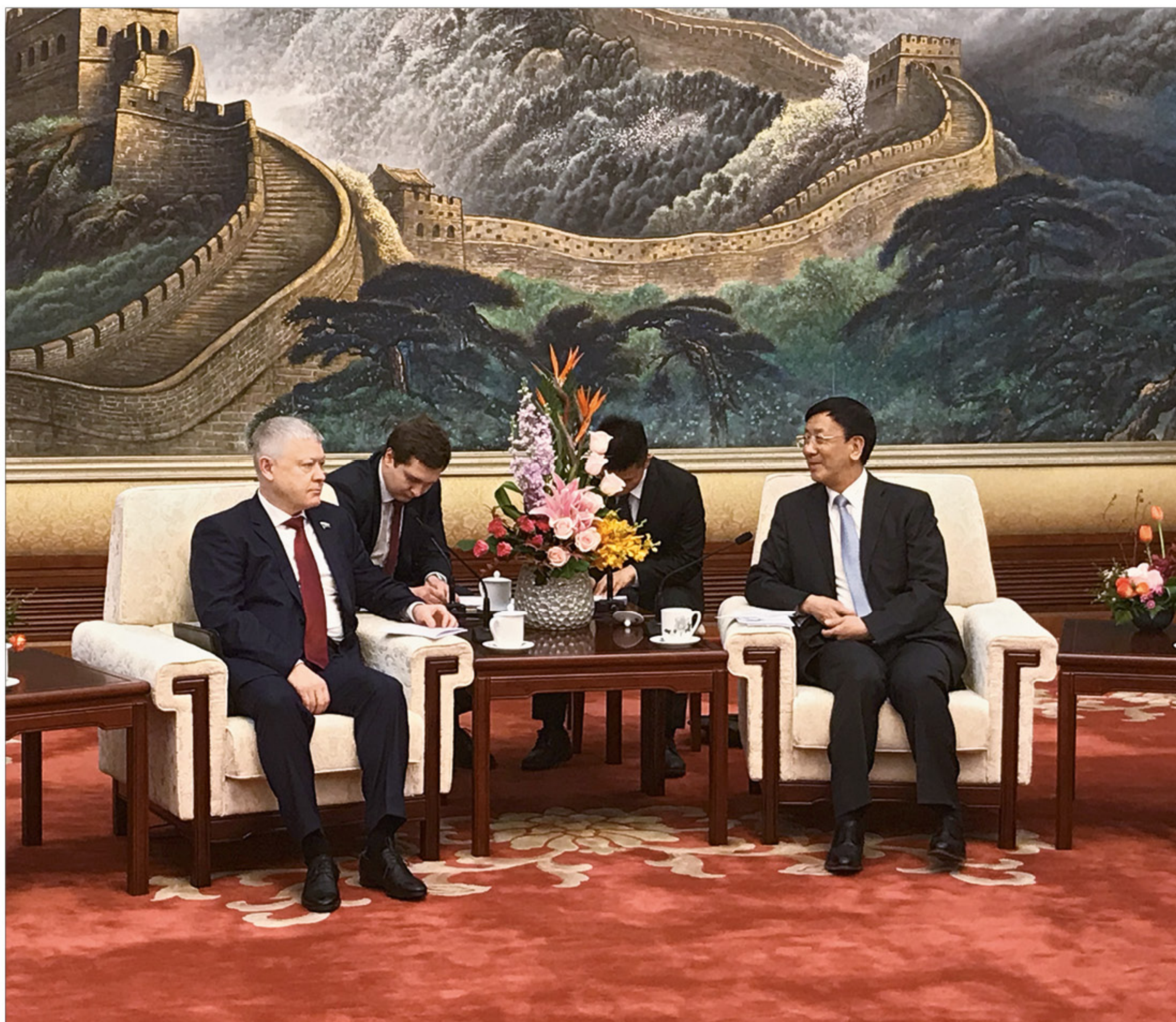
чили», и для этого нужно российскому сегменту интернета «придать устойчивости»³.

С каждым днём интернет играет всё большую роль в нашей повседневной жизни и принимаемые меры безопасности должны быть адекватными угрозе. Ведь если произойдет отключение России от глобального интернета, даже в случае техногенной аварии, например, повреждения кабеля, выполнение многих ставших для нас привычными операций может стать невозможным. И речь не только о доступе к различным базам данных, но и о проведении банковских операций, работе кассовых аппаратов в супермаркетах, управлении объектами инфраструктуры.

³ <https://dailystorm.ru/news/kitaya-v-rossii-ne-budet-medvedev-prokommentiroval-zakon-o-suverennom-runete>

События в Венесуэле, где в результате повторяющихся кибератак из-за рубежа периодически оставалось без электричества большинство штатов, показывают, как важно иметь прочную защиту от воздействия извне и достаточную надежность национального сегмента интернета. А недавнее сообщение газеты The New York Times⁴ о том, что в последнее время США усилили развертывание киберинструментов для внедрения в энергосистему России и проведения кибератак, лишь подтверждает целесообразность предпринимаемых российскими законодателями и Правительством шагов. В этих условиях понятна необходимость создания отечественных программных продуктов, организации разработки и собственного производства компьютерной техники и элементной базы.

⁴ <https://www.vesti.ru/doc.html?id=3158300>



В Китае разделяют позицию России в стремлении утвердить правила ответственного поведения государств в киберпространстве. На фото: переговоры председателя Комитета Госдумы по безопасности и противодействию коррупции Василия Пискарева с заместителем председателя Постоянного Комитета ВСНП Цао Цзяньмином

ОТПОР ВНЕШНИМ КИБЕРУГРОЗАМ

Очевидно, что принятие Государственной Думой РФ два года назад Федерального закона от 26 июля 2017 года № 187-ФЗ «О защите критической информационной инфраструктуры»⁵ и последующее создание Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России (ГосСОПКА) были своевременными шагами. Несмотря на предпринимаемые в этот период массированные атаки на российские компьютерные сети, серьезных сбоев в работе информационных систем критически важных объектов зарегистрировано не было.

В связи с этим понятно стремление России закрепить на международном уровне идеи суверенного интернета и ответственного поведения в информационном пространстве. Наша страна выступает с такими предложениями на протяжении уже почти двух десятков лет. Однако лишь недавно они получили ощутимую поддержку на уровне ООН. В декабре минувшего года в Нью-Йорке за предложенный Россией документ о создании в Генеральной Ассамблее ООН рабочей группы по противодействию киберпреступности проголосовали 119 стран. Интересно, что среди тех, кто голосовал против предложенной Россией резолюции, были США, Великобритания и Украина. С территории именно этих стран Россия подвергалась массированным информационным атакам.

⁵ <http://publication.pravo.gov.ru/Document/View/0001201707260023>

На Международном форуме «Развитие парламентаризма», проходившем в Москве в июне 2018 года, в рамках секции по вопросам безопасности мы тесно общались с немецким коллегой — главой германского Совета по кибербезопасности Хансом Вильгельмом Дюном, который отметил, что у наших стран общие проблемы и имеется полная заинтересованность в совместной работе, обмене информацией, практиками. Поддержал Дюн и российскую инициативу выработать единые требования безопасности в интернете.

Наша страна предложила разработать и принять на уровне ООН правила ответственного поведения в информационной сфере. Созданная для этого рабочая группа, рассмотрит различные аспекты, включая и вопросы кибербезопасности. Показательно, что поддержку в ООН получила российская позиция, направленная не на конфронтацию и развязывание информационных войн, а на объединение международных усилий в противодействии кибертерроризму и киберпреступности.

МЕЖДУНАРОДНАЯ ПОДДЕРЖКА

Предложения России о сотрудничестве в сфере информационной безопасности, обмене информацией о киберугрозах, сближении законодательных норм, принятых в различных государствах, ранее нашли поддержку на уровне стран-участниц организаций БРИКС, ШОС и ОДКБ. Недавно очередной обмен мнениями при активном участии Комитета Госдумы по безопасности и противодействию коррупции, который выступил одним из организаторов форума, состоялся в Ханты-Мансийске в рамках 3-й Международной конференции по информационной безопасности «Инфофорум-Югра». Форум зарекомендовал себя как авторитетная площадка по выработке совместных решений в сфере кибербезопасности на международном уровне, по обмену опытом и идеями между специалистами в сфере информационных технологий.

Комитет Государственной Думы по безопасности и противодействию коррупции наладил прямое взаимодействие с профильными комитетами и комиссиями парламентов Ирана, Китая, Турции, сотрудничает с парламентариями Индии. Обмен опытом идет, в том числе, и в сфере кибербезопасности, где каждой из стран наработан свой интересный опыт. К примеру, в Иране организована разветвленная сеть организаций по обеспечению кибербезопасности, и в том числе киберполиция — профильное подразделение в составе Сил охраны правопорядка.

Хотел бы обратить внимание и на опыт Китая, которым партнеры поделились с нами в ходе визита делегации Комитета в Пекин в феврале этого года. Вопросам информационной безопасности и защите национального сегмента ин-



Переговоры Василия Пискарева с председателем Собрания исламского совета (Меджлиса) Исламской Республики Иран Али Лариджани

тернета от негативного воздействия на сознание молодежи в КНР уделяют большое внимание. В Китае разделяют позицию России в стремлении утвердить правила ответственного поведения государств в киберпространстве. Основы сотрудничества двух стран закреплены в Совместном заявлении⁶, подписанном 5 июня этого года по итогам государственного визита Председателя КНР Си Цзиньпина в Российскую Федерацию.

Россия и Китай, в частности, договорились «укреплять обмен в области законодательного регулирования деятельности в информационном пространстве». Наши страны намерены «продолжить работы в целях дальнейшей выработки в рамках ООН правил ответственного поведения государств в информационном пространстве и разработки универсального, юридически обязывающего документа по противодействию использованию информационно-коммуникационных технологий в преступных целях». Кроме того, Россия и Китай договорились «обеспечивать мирное и безопасное функционирование сети «Интернет» на основе равноправного участия всех государств в данном процессе».

ЗАЩИТА ДЕТЕЙ И ПОДРОСТКОВ

Одним из важных аспектов ответственного поведения в киберпространстве безусловно является защита детей и подростков от вовлечения их в преступную деятельность. Я имею в виду распространение в интернете информации, направленной на склонение несовершеннолетних к совершению опасных для их жизни и жизни окружающих противоправных действий.

В последние годы мы столкнулись с таким явлением в соцсетях, как «группы смерти», «Колумбайн-сообщества», игры «Синий кит», «Беги и умри» и другие. Рост числа самоубийств

⁶ <http://www.kremlin.ru/supplement/5413>

среди детей вынудил нас к поиску законодательных мер по блокировке такого опасного контента. Ряд поправок, внесенных в действующие законы, позволил выработать необходимые механизмы оперативного реагирования на распространение информации о способах совершения самоубийства, призывов к суициду и иных форм вовлечения и принуждения детей к противоправным действиям.

В частности, принятым Госдумой Федеральным законом от 18 декабря 2018 года № 472-ФЗ «О внесении изменений в статью 15¹ Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и жизни»⁷ введен ускоренный порядок ограничения доступа к любому виду запрещенной информации в случае ее повторного размещения, то есть незамедлительно.

ДЕЙСТВЕННОСТЬ ПРОТИВОДЕЙСТВИЯ

В результате своевременно принятых мер удалось стабилизировать ситуацию, сгладить ее злободневность и общественный резонанс, снизить число детских суицидов. Сейчас оперативно перекрывается доступ к смертоносному контенту в сети, а его распространители привлекаются к ответственности. Положительную роль при этом сыграли введенные нами в Уголовный кодекс Российской Федерации статьи 110.1 и 110.2, предусматривающие за посягательство на жизнь и здоровье детей (в том числе — с использованием сети «Интернет») суровое наказание вплоть до 15 лет лишения свободы.

В Единый реестр интернет-ресурсов, содержащих информацию, распространение которой в России запрещено, по информации Роспотребнадзора внесено более 76 000 сайтов и (или) указателей страниц сайтов с наличием запрещенной информации по линии «призывы к самоубийству». Блокируется около 400 URL, с остальных URL запрещенная информация уже удалена.

Кроме того, борьба с распространением суицидального контента осуществляется Роскомнадзором в сотрудничестве с Mail.ru Group в рамках созданной рабочей группы. По данным Роскомнадзора, в результате такого сотрудничества удалено либо ограничен доступ к запрещенной информации на 122 000 страниц социальных сетей «ВКонтакте», «Мой Мир» и «Одноклассники».

По признанию специалистов Роскомнадзора, энергичные меры, предпринятые государственными органами, вынудили злоумышленников, осуществляющих деструктивное воздействие на подрастающее поколение с использованием современных телекоммуникаций, сместить криминально ориентированные акценты в сторону распространения и пропаганды информации о криминальной субкультуре (в частности, о движении «А.У.Е» и движении «скулшутинг», призывающем к нападению на учащихся школ). Приходится принимать меры и в отношении подобных сайтов и сетевых сообществ.

«НЕТ» НАРКОТИКАМ

1 мая 2019 года Президент России В. В. Путин подписал внесенный в Госдуму по моей инициативе закон, направленный на защиту детей и подростков от рекламы и распространения в интернете и средствах массовой информации новых наркотиков. В частности, устанавливается запрет публиковать в СМИ и интернете сведения о способах изготовления и местах приобретения новых потенциально опасных психоактивных веществ, например, «солей» и «спайсов», а также о способах и местах культивирования наркосодержащих растений⁸.

Новый закон позволит правоохранительным органам оперативно пресекать деятельность тех, кто, манипулируя общественным сознанием, создает положительный образ наркомана. В то же время наркосбытчики лишатся возможности призывать своих клиентов к покупке наркотиков и потенциально опасных психоактивных веществ через интернет. Практические наработки в этом направлении уже имеются, а реакция пользователей интернета не заставила себя ждать. Так, 28 мая 2019 года общество оперативно отреагировало на появление запрещенной рекламы наркотиков в Facebook, и противоправный контент был удален. Это свидетельствует о том, что закон востребован обществом. А главная задача депутатского корпуса — своевременно принимать нужные стране и гражданам законы.

Примечательно, что этот Федеральный закон был создан в сотрудничестве с Молодежным парламентом при Государственной Думе. Именно молодые парламентарии предложили нам обратить внимание на существующий пробел в законодательстве и приняли участие в разработке законопроекта. Такое сотрудничество с молодыми политиками, которые, что называется, изнутри чувствуют и понимают проблемы молодежи, готовы вырабатывать и предлагать свои решения, мы собираемся продолжить (и в том числе — в форме поддержки киберволонтерства).

Мы также хорошо понимаем, что для успешного противодействия названным выше угрозам необходимо поддерживать создание в российском сегменте «всемирной паутины» благоприятной интернет-среды, пропаганду здорового образа жизни и создание в социальных сетях групп и страниц, где, наряду с позитивным контентом, в популярной и доступной для молодежи форме будет рассказано об опасностях, которые подстерегают подростков на просторах интернета.

По этим вопросам мы также готовы к сотрудничеству с Молодежным парламентом. Мы открыты к диалогу со всеми, кто заинтересован в созидательном развитии отечественного сектора интернета, в формировании понятной молодому поколению и одновременно безопасной цифровой среды.

⁷ <http://publication.pravo.gov.ru/Document/View/0001201812180020>

⁸ <http://publication.pravo.gov.ru/Document/View/0001201905010033>



АССОЦИАЦИЯ
БАНКОВ
РОССИИ

XVII Международный банковский форум

Банки России - XXI век



В рамках форума пройдет XXI Банковская конференция «Взаимодействие финансового и реального секторов в условиях цифровизации экономики: Россия и международная практика» и круглые столы по актуальным вопросам развития финансового рынка.

Генеральный спонсор



КОММЕРЧЕСКИЙ БАНК
КУБАНЬ КРЕДИТ

Главный спонсор-спонсор регистрации



БАНК
ЦЕНТР-ИНВЕСТ

Контакты оргкомитета:

Тел./факс +7 (495) 785-29-93,
+7 (495) 785-29-88

Почта: event@asros.ru

www.asros.ru

11-14 сентября 2019 года

г. Сочи, отель «Radisson Blu Resort & Congress Centre»



Артём СУДАРЕНКО
заместитель
руководителя ФинЦЕРТ
Банка России

ОЖИДАЕТСЯ НОВАЯ НОРМА

БАНКИ ОБЯЖУТ РЕГУЛЯРНО АКТУАЛИЗИРОВАТЬ АДРЕСА ЭЛЕКТРОННОЙ ПОЧТЫ КЛИЕНТОВ

Проблема деактуализации адресов электронной почты клиентов финансовых организаций возникла в связи с тем, что на сегодняшний день этот канал связи является одним из основных инструментов взаимодействия банка и клиента. На почту могут приходить как рекламные акции продуктовой линейки кредитной организации, так и важная информация о состоянии счета (банковские выписки).

Е-MAIL ПО-ПРЕЖНЕМУ ВАЖЕН

Зачастую клиенты банков без должного внимания относятся к присылаемой по электронной почте информации, направляемой банком, воспринимая рассылки исключительно как навязчивый маркетинг. Вследствие такого отношения бывает, что указывают в договоре обслуживания либо несуществующий адрес электронной почты, либо чужой. Таким образом, клиент сам повышает риск разглашения своей банковской тайны и персональных данных.

Недостоверный адрес электронной почты клиента финансовой организации может доставлять как технические неудобства (неполучение или несвоевременное получение полезной информации), так и приводить к существенному ущербу (репутационному, хищению денежных средств и т.п.). Кли-

ент сам подвергает себя рискам некорректного управления состоянием своего счета, контроля за погашением кредита, разнообразных финансовых потерь. Но в таком случае есть и подводная часть айсберга: сведения о держателе счета могут собираться третьими лицами, в том числе злоумышленниками.

В настоящее время банки на должном уровне решили вопросы актуального подтверждения принадлежности конкретным пользователям средств дистанционного взаимодействия (SIM-карт, номеров и устройств мобильной связи и т.п.). Потому что эти устройства выступают как инструменты электронных платежей, т.е. с их помощью которых можно осуществить перевод денежных средств.

РИСКИ ДЕАКТУАЛИЗАЦИИ

Риски финансовых потерь здесь явные. Вряд ли кто-то пожелает без подтверждения привязывать к мобильному банкингу свой телефон, тем более, не станет использовать неизвестно чей. В вопросах, напрямую не связанных с переводами денежных средств, понимания необходимости актуализировать для банков свою персональную информацию, к сожалению, нет.

Используя собранные данные клиентов, злоумышленник в дальнейшем может использовать методы социаль-

ной инженерии, что в конечном счете также приведёт к потере денег клиента банка. Деактуализированные адреса электронной почты клиентов делают их потенциальными мишенями спама, фишинга, рассылок вредоносного программного обеспечения, хищения конфиденциальной информации и т.п.

Деактуализированные адреса электронной почты клиентов делают их потенциальными мишенями спама, фишинга, рассылок вредоносного программного обеспечения, хищения конфиденциальной информации

Кроме введения верификации банками адресов электронной почты клиентов, существуют и другие меры защиты дистанционных сервисов от злоумышленников: переход к «подтверждённым», «авторизованным» средствам телекоммуникаций (номерам и SIM-картам мобильной связи, IP- и MAC-адресам устройств, аккаунтам в социальных сетях и т.п.). Подтверждённые белые списки дают большую вероятность, что операция совершается самим клиентом, что информация от банка попадёт именно к нему.

Банки собирают и анализируют информацию о технических средствах, которыми клиент пользуется для электронного банкинга. Законодательство и другие нормативные документы предписывают банкам сбор такой технической информации для оценки профиля клиента, чтобы определить вероятность того, что операцию совершает легальный держатель счета, а не злоумышленник.

ЗНАЙ СВОЕГО КЛИЕНТА

В настоящее время Государственная Дума РФ работает над законопроектом, обосновывающим создание системы проверки банками и операторами платёжных систем сведений о владельцах SIM-карт. В марте 2019 года прошло первое чтение. Этот законопроект, как и требование банкам проверять и регулярно актуализировать адреса электронной почты клиентов, развивают нормативно-правовую базу выполнения принципа KYC (от англ. know your customer — знай своего клиента).

Существуют разные способы актуализации банками персональных данных клиентов, включая адрес электронной почты. Например, первичное подтверждение, что клиент имеет доступ к почтовому ящику или номеру телефона путём направления на него ссылки или одноразового кода подтверждения. Альтернативой может являться размещение данных в личном кабинете и направление клиенту ссылки на соответствующий раздел. При этом для доступа по такой ссылке потребуются аутентификация в личном кабинете.

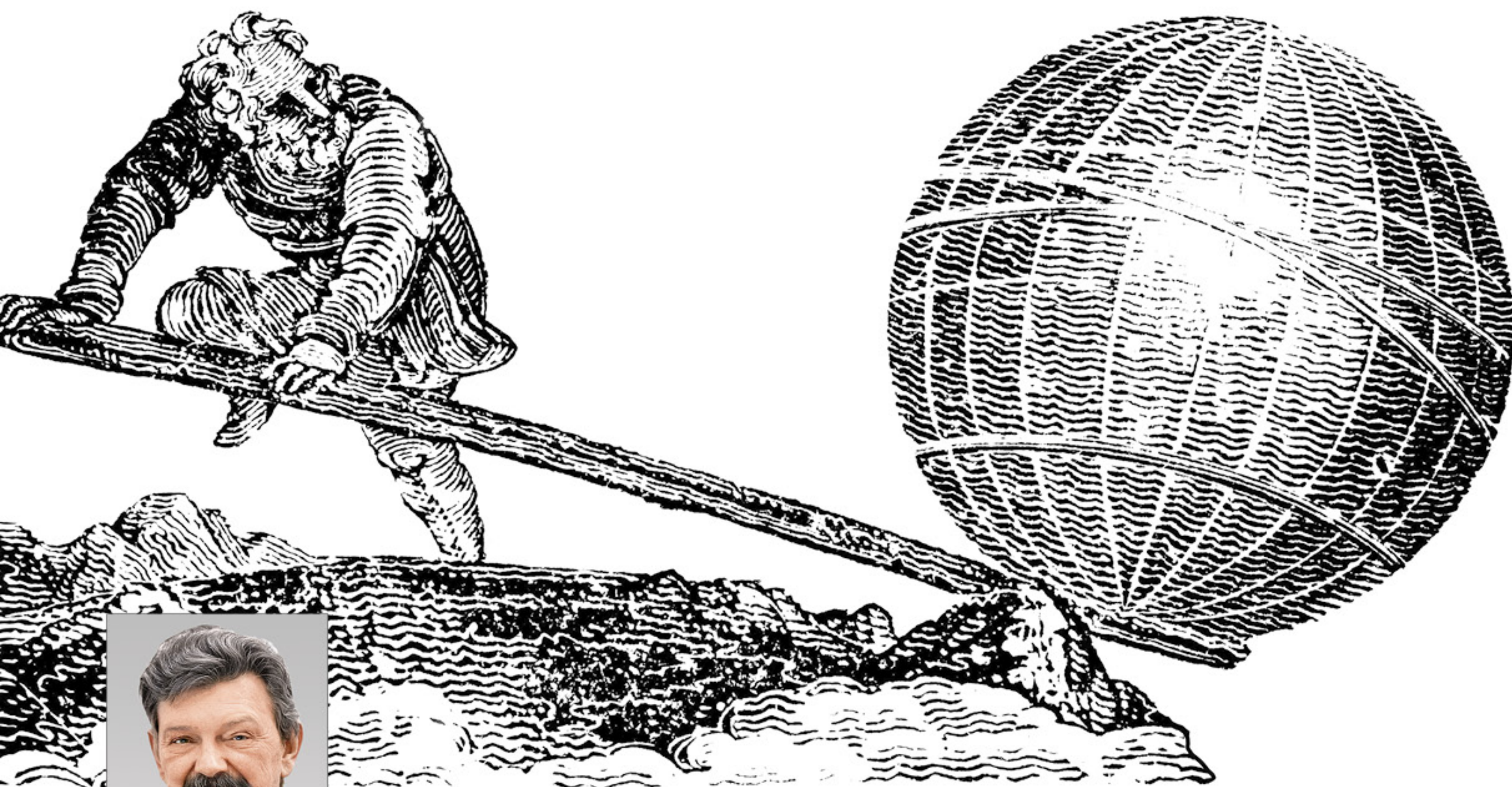
Все способы подтверждения позволяют снизить вероятность раскрытия защищаемых данных третьим лицам, однако они не предоставляют стопроцентной гарантии, что клиент ознакомится с нужной информацией вовремя. Это всецело на совести самого клиента. К проработке вопроса



о верификации электронной почты привлечены крупные банки, работающие как с физическими, так и с юридическими лицами.

* * *

Нормативные документы Банка России устанавливают требования к порядку защиты информации без установления конкретных технологий. Однако мы можем направлять поднадзорным организациям методические рекомендации и информационные письма с целью доведения до них сведений о лучших практиках. Подобные документы являются общедоступными и публикуются на сайте Банка России, поэтому могут использоваться в других отраслях и сферах.

**Сергей ВИХОРЕВ**

советник генерального директора
по информационной безопасности
ООО «ИТ-Экспертиза»

ДАЙТЕ МНЕ ТОЧКУ ОПОРЫ, И Я ПОВЕРНУ...

ЭССЕ О БИЗНЕСЕ, ПРОЦЕССАХ И КАТЕГОРИРОВАНИИ КИИ

Если начать «гуглить» на тему категорирование КИИ — вывалится огромное количество сайтов на эту тему. Но, к сожалению, всё это будет в основном пересказ 127 постановления или вариации на тему известной «лестницы» процесса категорирования объектов КИИ из презентации ФСТЭК России. То есть все говорят, ЧТО надо сделать, но почти никто не говорит КАК надо сделать. А хочется знать... Попробую в силу своего разумения поговорить именно о том, КАК надо делать.

Но, вначале оговорюсь. Уже в первых строках Правил категорирования объектов КИИ упоминаются некие процессы (управленческие, технологические, производственные, финансово-экономические и иные процессы в рамках выполнения функций или осуществления видов деятельности субъектов). И тут у многих технарей-ибэшников (а именно на их

плечи, в основном, взваливают категорирование) возникает когнитивный диссонанс. Зачастую технарь за счёт профессиональной деформации сознания связывает процесс с совокупностью последовательных действий некоей системы. На самом деле речь идёт о более высокоуровневой модели процессов, непосредственно связанных именно с выполнением функций, возложенных на юридическое лицо, или осуществлением им определённых видов деятельности. Хотя и не люблю вводить новые сущности, но чтобы отделить мух от котлет, буду использовать термин «бизнес-процесс» (это наиболее близко отражает суть), но не совсем в классическом определении¹.

¹ Бизнес-процесс для этих целей — это совокупность взаимосвязанных мероприятий или работ, направленных на выполнение функций (полномочий) или осуществления видов деятельности юридическим лицом

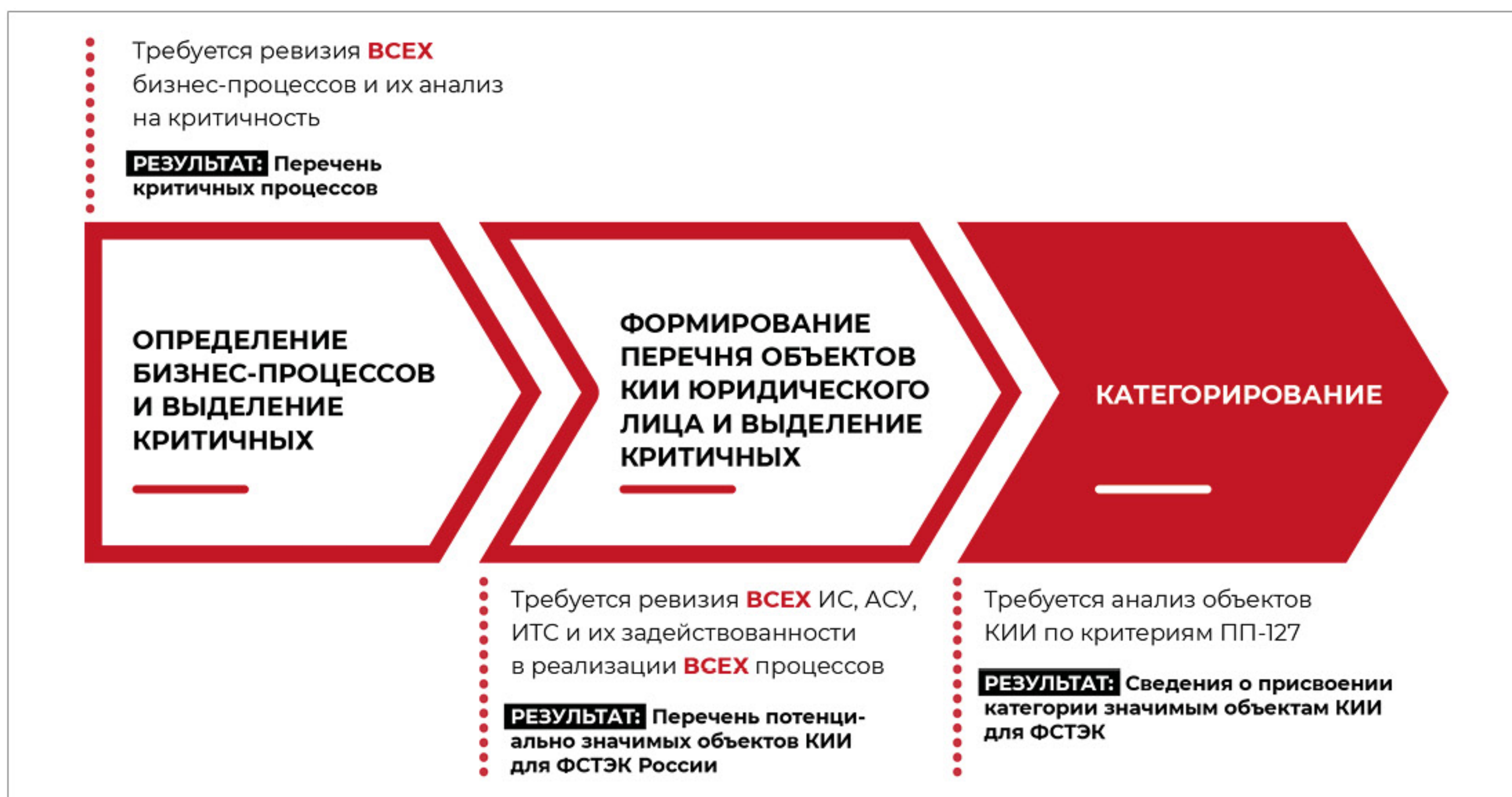


Рисунок 1. Состав и содержание подпроцессов, осуществляемых в процессе категорирования

И ГДЕ ТА ПЕЧКА, ОТ КОТОРОЙ ТАНЦЕВАТЬ?

К задаче категорирования информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, как объектов КИИ (буду их обобщённо называть — системы, пока это ещё не объекты КИИ — толкач муку покажет!) применим процессный (опять процесс!) подход. При этом априори будем считать, что юридическое лицо уже определилось со своей принадлежностью к областям (сферам) деятельности, установленных законом и аксиоматично является субъектом КИИ. Анализируя Правила категорирования, можно процесс категорирования рассматривать как совокупность ряда подпроцессов:

- ♦ определение бизнес-процессов юридического лица и выделение критичных;
- ♦ формирование Перечня объектов КИИ и выделение критичных;
- ♦ категорирование значимых объектов КИИ.

Состав этих подпроцессов и их содержание приведён на рис. 1.

В рамках журнальной статьи, даже очень большой, рассмотреть весь процесс категорирования вряд ли получится. Но практический опыт показывает, что начало начал этого процесса — это выявление и систематизация именно бизнес-процессов, которые реализует юридическое лицо. На этом остановимся и с этого места будем говорить поподробнее.

Подпроцесс определения бизнес-процессов в деятельности юридического лица и выделения среди них критичных предполагает проведение анализа всех управленческих, технологических, производственных, финансово-экономических и иных бизнес-процессов юридического лица. Подпроцесс включает следующие процедуры:

- ♦ составление перечня всех управленческих, технологических, производственных, финансово-экономических и иных бизнес-процессов в деятельности юридического лица;
- ♦ высокоуровневую оценку негативных последствий от нарушения бизнес-процессов в деятельности юридического лица по каждому критерию, определённом постановлением Правительства РФ от 08.02.2018 г. № 127;
- ♦ формирование Перечня критичных бизнес-процессов в деятельности юридического лица.

При составлении Перечня бизнес-процессов надо учитывать, что:

- ♦ под управленческими бизнес-процессами понимаются любые процессы в деятельности юридического лица, направленные на управление выполнением функций (полномочий) или осуществления видов деятельности юридическим лицом. Управленческие бизнес-процессы представляют собой совокупность циклических действий, связанных с выявлением проблем, поиском и организацией выполнения принятых решений для управляемых объектов;
- ♦ под технологическими бизнес-процессами понимаются любые процессы в деятельности юридического лица, которые обслуживают основные бизнес-процессы, направленные на выполнение функций (полномочий) или осуществление видов деятельности юридическим лицом;
- ♦ под производственными бизнес-процессами понимаются любые процессы в деятельности юридического лица, направленные на достижение конечного результата выполняемых функций (полномочий) или видов деятельности юридического лица. Производственные процессы являются линейными процессами на выходе которых предполагается определённый результат;



Рисунок 2. Состав и содержание подпроцесса определения бизнес-процессов юридического лица

♦ под финансово-экономическими бизнес-процессами понимаются любые процессы в деятельности юридического лица, связанные с экономическими, финансово-денежными, учётными, фискальными аспектами деятельности юридического лица, а также с обеспечением текущей деятельности юридического лица посредством реализации финансовых прав и исполнения финансовых обязательств.

Ладно, какие бизнес-процессы анализировать вроде бы понятно (рис. 2). Но где взять эти самые бизнес-процессы, какие из них характерны для конкретного юридического лица? И вот тут начинаются первые трудности процесса категорирования. Самое простое, это когда бизнес-процессы в организации уже описаны: бери, оценивай, выбирай критичные. Сейчас многие организации, используя опять-таки процессный подход, стремятся правильно наладить свой бизнес и составляют Реестры своих бизнес-процессов. Это характерно для многих организаций кредитно-финансовой сферы, организаций, оказывающих услуги связи и даже производственных предприятий. В этом случае, в качестве источника знаний о существующих бизнес-процессах могут выступать:

- ♦ реестр бизнес-процессов организации;
- ♦ регламенты выполнения функций;
- ♦ технологические карты;

- ♦ диаграммы потоков данных;
- ♦ диаграммы потоков работ.

Но, к глубокому сожалению, описывают бизнес-процессы далеко не все организации. И что будем делать? Если подходить по-взрослому, если бизнес-процессы не описаны, необходимо использовать референтные² (типовые) модели бизнес-процессов. Слава Богу, сейчас таких моделей много, для примера:

- ♦ Классификатор типовых бизнес-процессов (APQC)³;
- ♦ Восьмипроцессная модель (ITSM)⁴;
- ♦ Модель eTOM (сфера связи)⁵;
- ♦ Референтная модель BIAN⁶;

² Референтная модель — концептуальная модель, формализующая рекомендованные практики ведения бизнеса в определённой области и включающая функциональную структуру, объектную модель предметной области, процессную модель, функциональную модель, набор потенциальных точек контроля, набор операционных показателей деятельности, эталонные схемы организации бизнеса, готовые наборы функций и процессов

³ APQC — American Productivity & Quality Center

⁴ ITSM — Information Technology Service Management

⁵ eTOM — Enhanced Telecom Operations Map

⁶ BIAN — Banking Industry Architecture Network

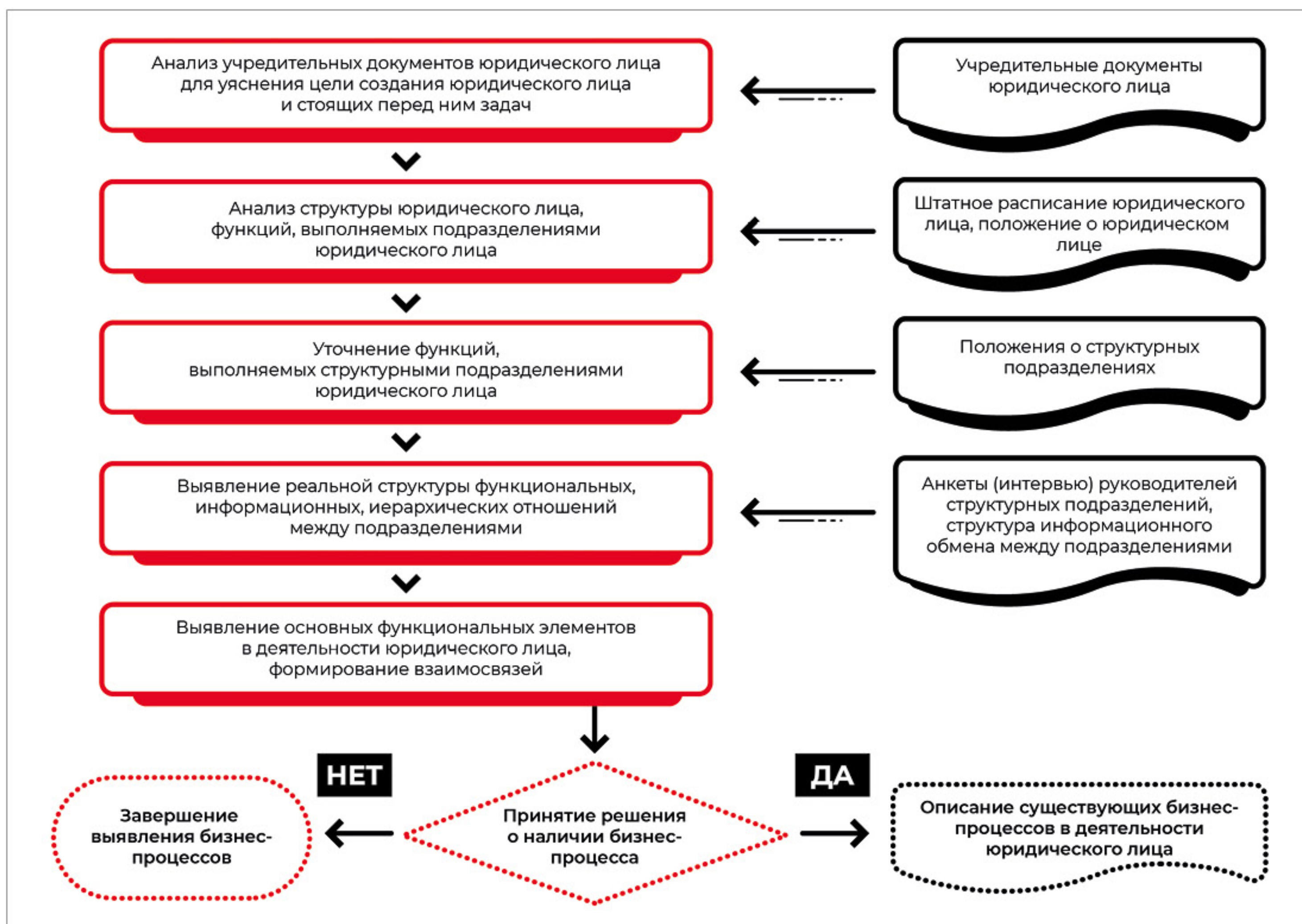


Рисунок 3. Алгоритм упрощённого выявления бизнес-процессов

- ♦ Отраслевые приложения стандартов серии ISO 9000;
- ♦ Стандарты качества банковской деятельности (АРБ)

Правда, надо отметить, что адаптация референтных моделей для нужд своей организации — дело хотя и полезное, и нужное, но достаточно хлопотное и затратное как по времени, так и по средствам. Всегда остаётся риск не успеть в срок.

И тогда придётся включать смекалку, знания и опыт членов комиссии и пытаться упрощённо описать бизнес-процессы исходя из выполняемых юридическим лицом функций (полномочий) или осуществляемых им видов деятельности. Здесь надо будет на основе анализа учредительных документов, структуры организации, поставленных перед подразделениями задачами, выстроить реальную структуру взаимодействия, необходимую для решения поставленных задач и принять решение о наличии того или иного бизнес-процесса. Алгоритм упрощённого выявления бизнес-процессов в деятельности юридического лица приведён на рис. 3.

Важно чтобы попытаться выявить ВСЕ бизнес-процессы, которые реализуются в организации (пока на этом этапе об их критичности речь не идёт). Важно ничего не упустить. И вот, когда эта титаническая работа закончена, выявлены все бизнес-процессы, составлен Реестр бизнес-процессов — первый этап можно считать завершённым.

ПЕЧКУ НАШЛИ. ЧТО ДАЛЬШЕ?

Но трудности только начинаются. Теперь, по идее, надо оценить насколько эти бизнес-процессы критичны и отбросить те, которые не представляют интерес, как некритичные. Но критериев оценки именно бизнес-процессов с точки зрения их критичности в Правилах категорирования — нет! А рассчитывать показатели критериев критичности, наверное, ещё рано. И комиссия может впасть в ступор.

Давайте немного порассуждаем. Зачем мы определяем критичные бизнес-процессы? Чтобы определить, какие системы задействованы для их реализации, отбросить те системы, которые не задействованы и уж потом, на основе расчёта показателей критериев значимости, определить насколько эти системы значимы. Следовательно, при оценке критичности бизнес-процесса сам показатель критерия — не важен, а требуется только определить: насколько потенциально этот бизнес-процесс может повлиять на причинение ущерба или нарушение функций. То есть на этом этапе нас интересует только высокоуровневая оценка критичности бизнес-процессов.

Итого: показатели критериев нас сейчас не интересуют (это мы будем считать позже), но мы должны учесть критерии, указанные в Правилах категорирования. Такую оцен-

Так как чётких критериев нет, влияние бизнес-процесса на ту или иную значимую сферу придётся оценивать интуитивно-экспертным методом с учётом критериев, установленных Правилами категорирования

ку можно провести на основе анализа влияния и потенциальных последствий от нарушения бизнес-процесса на ту или иную критичную сферу, для которой определены группы критериев значимости (для высокоуровневой оценки этого достаточно):

- ♦ социальной;
- ♦ политической;
- ♦ экономической;
- ♦ экологической;
- ♦ обеспечения обороны страны, безопасности государства и правопорядка.

И здесь, так как чётких критериев нет, влияние бизнес-процесса на ту или иную значимую сферу придётся оценивать интуитивно-экспертным методом с учётом критериев, установленных Правилами категорирования.

При оценке критичности бизнес-процесса с точки зрения социальной значимости оценивается влияние бизнес-процесса на возможный ущерб, причиняемый жизни или здоровью людей, возможность прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальное время отсутствия доступа к государственной услуге для получателей такой услуги.

Бизнес-процесс считается способным причинить ущерб жизни и здоровью людей, если он задействован (обеспечивает) в управлении или обеспечении работоспособности механизмов и устройств, нарушение функционирования которых может привести:

- ♦ к авариям, катастрофам с человеческими жертвами;
- ♦ к бактериологическому, радиационному или химическому заражению;
- ♦ к отключению приборов, обеспечивающих жизненно важные функции организма;
- ♦ к нарушению технологий производства и хранения фармацевтической и медицинской продукции;
- ♦ к иным последствиям, пагубно влияющим на жизнь и здоровье людей.

Бизнес-процесс считается способным повлиять на прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, если он задействован:

- ♦ в управлении, контроле или мониторинге и эксплуатации объектами обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи;
- ♦ в обеспечении бесперебойного функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи;

♦ в поддержании качества функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи.

Бизнес-процесс считается способным привести к нарушению максимального времени отсутствия доступа в оказании государственных

услуг, если он задействован:

- ♦ в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры доступа к государственной услуге;
- ♦ в аналитической, экспертной, учётной деятельности, необходимой для обеспечения функционирования государственных органов власти, оказывающих госуслуги;
- ♦ в обеспечении взаимодействия государственных органов власти, оказывающих госуслуги.

При оценке критичности бизнес-процесса с точки зрения политической значимости, оценивается влияние бизнес-процесса на возможность причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики. Бизнес-процесс считается оказывающим влияние на функционирование органа государственной власти, если он задействован:

- ♦ в аналитической, экспертной, учётной деятельности, необходимой для принятия управленческих решений органом государственной власти;
- ♦ в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры взаимодействия органов государственной власти;
- ♦ в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры оповещения населения о чрезвычайных ситуациях;
- ♦ в поддержании бесперебойного функционирования элементов системы управления, необходимой для реализации возложенных на орган государственной власти полномочий.

При оценке критичности бизнес-процесса с точки зрения экономической значимости оценивается влияние бизнес-процесса на возможность причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры или бюджетам Российской Федерации.

Бизнес-процесс считается оказывающим влияние на возможность причинения прямого и косвенного ущерба государственной корпорации, государственным унитарным предприятиям, государственной компании, стратегическому акционерному обществу⁷, стратегическому предприятию⁸, а также ущерба бюджетам Российской Федерации, если он задействован:

⁷ Указ Президента РФ от 04.08.2004 № 1009 «Об утверждении перечня стратегических предприятий и стратегических акционерных обществ»

⁸ Распоряжение Правительства РФ от 20.08.2009 № 1226-р «Об утверждении перечня стратегических предприятий и организаций»

- ♦ в аналитической, экспертной, учётной деятельности, необходимой для принятия управленческих решений руководством государственной корпорации, государственного унитарного предприятия, государственной компании, стратегического акционерного общества, стратегического предприятия;

- ♦ в управлении, контроле или мониторинге технологическим циклом производства, включая поставки, логистику, взаимодействие с контрагентами;

- ♦ в управлении, контроле или мониторинге комплексом программных и программно-аппаратных средств, предназначенных для контроля за технологическим или производственным оборудованием (исполнительными устройствами) и производимыми ими процессами;

- ♦ в обеспечении взаимодействия с организациями кредитно-финансовой сферы, включая страховые компании, биржи, банки, казначейство, налоговые органы.

Бизнес-процесс считается оказывающим влияние на возможность прекращения или нарушения проведения банковских операций, если он задействован в выполнении любых операций по банковским счётам или без открытия банковского счёта, включая билинговые и клиринговые операции.

При оценке критичности бизнес-процесса с точки зрения экологической значимости оценивается уровень воздействия бизнес-процесса опасных производственных объектов⁹ на окружающую среду. Бизнес-процесс считается оказывающим воздействие на окружающую среду, если он задействован в управлении или обеспечении работоспособности механизмов и устройств опасных производственных объектов, нарушение функционирования которых может привести к авариям, инцидентам или катастрофам в результате которых возможны:

- ♦ сброс загрязняющих веществ в водоёмы и на территории;
- ♦ повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосфере;
- ♦ ухудшение состояния земель;
- ♦ иные вредные воздействия.

При оценке критичности бизнес-процесса с точки зрения значимости для обеспечения обороны страны, безопасности государства и правопорядка оценивается уровень воздействия бизнес-процесса на прекращение или нарушение функционирования пункта управления (ситуационного центра) государственных органов власти или государственной корпорации, информационных систем в области обеспечения обороны страны, безопасности государства и правопорядка, снижение показателей государственного оборонного заказа.

Бизнес-процесс считается оказывающим влияние на прекращение или нарушение функционирования пункта управления (ситуационного центра) государственных органов власти или государственной корпорации, информационных систем в области обеспечения обороны страны,

безопасности государства и правопорядка, если он задействован:

- ♦ в аналитической, экспертной, учётной деятельности, необходимой для принятия управленческих решений органом государственной власти или государственной корпорации в рамках пункта управления (ситуационного центра);

- ♦ в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры пункта управления (ситуационного центра) государственного органа власти или государственной корпорации;

- ♦ в управлении, контроле или мониторинге и поддержании бесперебойного функционирования информационно-телекоммуникационной сети, обеспечивающей деятельность пункта управления (ситуационного центра) государственного органа власти или государственной корпорации по взаимодействию с управляемыми объектами (субъектами);

- ♦ в управлении, контроле или мониторинге и поддержании бесперебойного функционирования элементов инфраструктуры оповещения населения о чрезвычайных ситуациях.

Бизнес-процесс считается оказывающим влияние на снижение показателей государственного оборонного заказа, если он задействован:

- ♦ в управлении, контроле или мониторинге технологическим циклом производства, включая поставки, логистику, взаимодействие с контрагентами;

- ♦ в управлении, контроле или мониторинге комплексом программных и программно-аппаратных средств, предназначенных для контроля за технологическим или производственным оборудованием (исполнительными устройствами) и производимыми ими процессами.

Бизнес-процесс считается критичным, если в ходе высокоуровневой оценки возможных последствий от нарушения бизнес-процесса установлено что, он задействован и оказывает влияние хотя бы по одной группе критериев значимости.

Оценка критичности бизнес-процессов позволит исключить из Реестра бизнес-процессов, те, которые не являются критичными и тем самым в дальнейшем сократить объём расчётов показателей критериев значимости систем.

* * *

Это далеко не весь процесс категорирования объектов КИИ. Каждый этап можно декомпозировать и попытаться есть слона по частям. Автор попытался остановиться только на самом, на его взгляд, главном — на начальной точке отсчёта. Не знаю, насколько получилось, но хотелось показать, что краеугольным камнем, точкой опоры в процессе категорирования объектов КИИ является не информационная система и даже не величина показателей критериев значимости, а правильное выстраивание бизнес-процессов организации и оценка их влияния на ту или иную критичную сферу. Вот та самая печка, от которой надо танцевать.

⁹ Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов»

ВИДЕТЬ НА 360°

КРУГЛЫЙ СТОЛ ФИНЦЕРТ НА IT & SECURITY FORUM 2019



Анна ВОРОБЬЕВА
обозреватель
BIS Journal

В конце мая в Казани прошёл традиционный форум для специалистов — IT&Security Forum 2019. Для ИБ-специалистов финансовой сферы практическим напутствием стал круглый стол ФинЦЕРТ «Мониторинг инцидентов информационной безопасности в организациях финансовой сферы». В дискуссии приняли участие Александр Бабкин (Газпромбанк), Григорий Царёв (ФинЦЕРТ), Вячеслав Яшкин (Ак Барс Банк), Владимир Дмитриев (ICL Системные технологии), Дмитрий Бербер (Золотая Корона), Станислав Гонтаренко (Мандарин Банк). Модератором выступил руководитель ФинЦЕРТ Артём Калашников.

О ТРЕНДАХ. СМЕНА ВЕКТОРА АТАК

Согласно отчёту ФинЦЕРТа за 2018 год, тренды по основным направлениям кибератак следующие: целевые атаки, фишинг, атаки на устройства самообслуживания, DDos-атаки и др. Если раньше главную угрозу представляли атаки извне, то теперь вектор изменился в сторону внутренних атак.

По словам Александра Бабкина (Газпромбанк), внутренние атаки можно разделить на два вида:

- ♦ атаки, связанные со злоупотреблением должностных полномочий (использование доступа для передачи информации);
- ♦ атаки, предполагающие передачу технологии защиты банковского продукта внешнему злоумышленнику.

Крупные банки видят внутренние атаки лучше, поскольку быстрее совершенствуют систему внутреннего контроля, внедряют новые системы защиты. Достаточно активно используется профилирование пользователей, постоянно совершенствуется система контроля доступа.

По мнению Александра Бабкина, тренд по росту числа внутренних атак нельзя назвать глобальным. Это связано, прежде всего, со сложностью ИТ-систем в крупных банках, что требует знания большого количества технологических цепочек. Таким знанием, как правило, обладают единицы.

Если говорить об атаках, связанных с внутренним DDos, то тут ситуация действительно усугубляется. Это связано в первую очередь с активной цифровизацией финансового сектора. Банки часто используют собственные ИТ-наработки, пренебрегая при этом элементарными принципами ИБ при проектировании и внедрении систем. В результате ИТ-системы содержат множество дыр.

Сейчас банки неохотно сообщают о внутренних атаках и сбоях, поскольку формально это не является требованием регулятора. Однако, по утверждению специалиста Газпромбанка, имеет смысл информировать ФинЦЕРТ и о таких атаках. Это позволит регулятору видеть картину на 360 градусов и более эффективно помогать при инцидентах.

Вячеслав Яшкин (Ак Барс Банк) добавил, что вопрос предоставления данных регулятору — это вопрос зрелости и банка в целом и его службы ИБ.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Владимир Дмитриев (ICL Системные технологии) обратил внимание на то, что основная проблема всегда исходит от человека. Поэтому не стоит забывать о гигиене ИБ. Нужно не только информировать друг друга, но и постоянно работать с персоналом и специалистами. Тем более что персонал часто становится причиной и других проблем.

Григорий Царёв (ФинЦЕРТ) рассказал, что сообщество мошенников переходит от атак на технические средства к прямым атакам на сотрудников и клиентов банка. Хищения совершаются через звонки в бухгалтерию или кассу. Злоумышленники представляются высокими руководителями или сотрудниками из технической поддержки, просят помочь в настройке терминалов. С начала 2019 года ФинЦЕРТ зафиксировал пять таких атак, завершившихся хищениями.

Тренд по росту числа внутренних атак нельзя назвать глобальным. Это связано, прежде всего, со сложностью ИТ-систем в крупных банках, что требует знания большого количества технологических цепочек



Артём Калашников (ФинЦЕРТ). Фото: itsecurityforum.ru



Александр Бабкин (Газпромбанк). Фото: itsecurityforum.ru

Не стоит забывать, что социальная инженерия до сих пор успешна только потому, что большинство людей продолжает верить мошенникам, не задумываясь, с какого телефона те звонят. Артём Калашников рассказал, что сейчас в банковском секторе принят ряд решений, например, договор с принятым банком, где прописано, что банк обязан работать со своими клиентами в части осведомлённости всеми доступными каналами связи, указанными в договоре. Статистика показывает, что такие решения пока ещё не эффективны. Соответственно бороться с социальной инженерией нужно комплексно. С одной стороны, повышать образованность клиентов, сотрудников и вообще граждан в вопросах ИБ. С другой стороны, начинать этот процесс нужно с детей. В школах отдельным предметом преподаются ОБЖ, а начиная с 8–9 класса — программирование. Однако в рамках данных программ нет ни слова об информационной безопасности. Этот вопрос нужно решать.

Александр Бабкин предложил максимально маркетизировать киберграмотность и направление ИБ в целом, т.к. той рекламы, которую банки размещают на банкоматах, явно недостаточно.

УВЕДОМЛЕНИЕ ФИНЦЕРТ: ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ ПРОБЛЕМЫ

Одна из основных проблем ФинЦЕРТа — организации не спешат уведомлять о кибератаках. Так, за последние 4–5 месяцев было направлено всего два (2) уведомления об атаках на банкоматы и терминалы самообслуживания, хотя по данным МВД России их было в разы больше.

Обязанность информировать об инцидентах установлена ГОСТом (Стандарт Банка России СТО БР БФБО-1.5-2018), нормативными до-

кументами Банка России и Федеральным законом (167-ФЗ и 187-ФЗ). Для этого создан удобный инструмент — платформа Банка России по обработке инцидентов АСОИ ФинЦЕРТ. Возникает вопрос: почему так трудно, используя платформу и все доступные каналы связи, передавать информацию об инцидентах, возникающих в организациях?

Надо отдать должное, с сентября качество предоставляемой банками информации об инцидентах значительно улучшилось. Банки научились работать с платформой АСОИ, стали правильно заполнять карточки инцидентов. Тем не менее проблемы есть. По словам представителя регулятора, одна из них связана с заполнением операций без согласия. Есть непонимание того, что является соответствием как идентификатором платежа и получателем денежных средств. Зачастую организации предоставляют информацию о счетах тех организаций, которым непосредственно принадлежат некие внутренние счёта, такие как МТС, Билайн и пр. Все эти данные попадают в фид. Таким образом, отображается некорректность и невозможность использования в полном объёме.

Многие организации относятся к этому формально. Зачастую информация либо замалчивается, либо поступает поздно, либо сама по себе малоинформативна. В результате она по сути бесполезна и никому не может помочь, добавил Артём Калашников.

По словам представителей банковского сектора, большинство проблем связаны с рабочими процессами, в частности, есть сложности в функциональности самого инструмента. Тем не менее, всё это оттачивается со временем, посредством плотной совместной работы.

Владимир Дмитриев, как представитель внешнего СОСа и сервис-провайдера, сказал, что хотелось бы обмениваться информацией

В информировании об инцидентах важна смысловая нагрузка и качество предоставляемой информации, а не формальное выполнение законов и нормативов Банка России

автоматизировано: максимально быстро, с возможностью дополнять данные своим контекстом.

Александр Бабкин выделил два типа проблем при взаимодействии: технические и организационные, причём обе на стороне кредитных организаций:

♦ **Технические проблемы.** Чтобы выстроить процесс обработки инцидентов с точки зрения здравого смысла и самих процессов, нужен ряд автоматизированных систем, в том числе и система учёта инцидентов. Во многих организациях банально нет таких платформ: инциденты фиксируются в excel либо на бумаге, так как внедрение соответствующей платформы стоит денег, времени и неких человеческих ресурсов.

Вторая техническая проблема — это интеграция с АСОИ ФинЦЕРТ. Необходимо понять, как подружить две системы на уровне API.

♦ **Организационные проблемы** связаны с неумением сотрудников выявлять инциденты, правильно их обрабатывать и вовремя информировать регулятора. К тому же многие считают, что, если об инциденте не было доложено сразу, то по прошествии пары дней он уже не актуален и потерял все необходимые фиды, поэтому и нет смысла о нём сообщать.

Так, помимо интеграции двух платформ, должна быть техническая возможность поставить признак-инцидент, что данная информация должна быть передана в соответствующую структуру.

Другая организационная проблема: кредитные организации подчас замалчивают информацию об инцидентах, внутренних проблемах и сбоях по причине отсутствия выстроенного процесса. Когда при возникновении инцидента и успешного на него реагирования должен быть организован оперативный процесс, продумана эскалация до определённого уровня руководства, которое и принимает решение об информировании.

Платёжная система «Золотая корона» объединяет множество банков и организаций. По словам ее представителя Дмитрия Бербера, служба ИБ видит все операции, осуществляемые в системе, и им удалось достаточно логично встроить в этот процесс информирование ФинЦЕРТа.

Сотрудник, отрабатывающий тот или иной инцидент, указывает в системе соответствующие поля, а система учёта инцидентов сама решает, какую информацию нужно отправить в запрос ФинЦЕРТу — всё происходит автоматически, быстро и не требует дополнительных ресурсов.

Отмечалось также, что среди причин нежелания включаться в процесс взаимодействия — порог вхождения. Даже для входа в тестовый режим платформы API требуется выполнить чек-лист, который программист, делающий интеграцию, не понимает. Не хватает простых рекомендаций именно для ИТ-специалистов: что отправлять, где отправлять и как защищать. Конечно, инструкция версии 1.01, которая ещё не опубликована, немного улучшит ситуацию, но и этого мало.

ФИНЦЕРТ ПРОДОЛЖИТ РАЗЪЯСНЯТЬ

Сегодня ФинЦЕРТ в тестовом режиме прорабатывает улучшения взаимодействия для пользователей API, разрабатываются соответствующие рекомендации. Банки подключаются, пробуют отправлять уведомления в автоматизированном режиме.

В части мобильного мошенничества ФинЦЕРТ разослал письмо о предоставлении номеров, которые используются кредитно-финансовыми организациями. Данные меры были разработаны совместно с операторами связи. В ближайшее время планируется перенаправить эти номера в Минкомсвязь.

Артём Калашников напомнил, что недавно состоялась презентация, где был предложен ряд направлений, связанных с интеграцией в SIEM-систему, в частности, использование коннекторов. Средства автоматизации позволят, к примеру, сократить время принятия решения на стороне как банка, так и регулятора.

Главный посыл руководителя ФинЦЕРТа: в информировании об инцидентах важна смысловая нагрузка и качество предоставляемой информации, а не формальное выполнение законов и нормативов Банка России. Смысл в том, чтобы информацию принять, понять, что происходит, составить картину и помочь по сути уже всем кредитным организациям.

* * *

Участники дискуссии предложили регулятору разработать методические рекомендации, позволяющие понять важность SIEM системы, API платформы, АСОИ, а также как правильно организовать процесс подготовки и передачи информации.

GENERATION V

УГРОЗЫ ПЯТОГО ПОКОЛЕНИЯ ТРЕБУЮТ НОВОЙ МОДЕЛИ ПОСТРОЕНИЯ ИБ

XIII Всероссийский цифровой IT&Security Forum (ITSF) собрал в Казани ключевых экспертов IT и кибербезопасности. BIS Journal заинтересовало выступление главы представительства Check Point Software Technologies в России и СНГ Василия Дягилева, посвящённое угрозам пятого поколения.

— Василий, вы не впервые рассказываете об атаках будущего. В чём их отличие от предыдущих, и как вы их классифицируете?

— Можно чётко проследить, как эволюционировали атаки и защита от них. Первое поколение атак — Gen I — появилось в 1980-х годах вместе с массовым распространением персональных компьютеров. Возникли вирусные программы, которые распространялись путём копирования самих себя, такие как Brain virus.

Атаки Gen II возникли в 1990-х вместе с появлением сетей и Интернета.

Третье поколение появилось в начале нулевых, когда хакеры научились использовать уязвимости всех компонентов IT-инфраструктуры.

Атаки Gen IV позволили увидеть новую проблему в ИБ: решения обнаруживали атаку только на основе известных сигнатур, которые создаются уже после того, как атака обнаруживается, анализируется и передаётся.

А в 2017 году мир столкнулся с угрозами пятого поколения — крупномасштабными разнонаправленными атаками, вызывающими крупные инфраструктурные и финансовые потери. Их принципиальное отличие — массовость, направленность на целые отрасли, регионы, страны. Такие атаки мультивекторны: они подстраиваются и поражают облачные хранилища, сети, мобильные устройства. Проще говоря, они поражают все слабые стороны IT-инфраструктуры организаций.

— В прошлом году ваша компания провела масштабные исследования угроз пятого поколения. Что изменилось за год?

— Вот несколько ключевых моментов из отчёта Check Point 2019 Security Report: доминирующую роль среди угроз занимали криптомайнеры, в 2018 году они атаковали 37% организаций по всему миру. Не менее опасными оказались

многовекторные ботнеты — ими были заражены 49% организаций, подвергшихся атакам в 2018 году.

В этом году, по сравнению с предыдущим, снизилась активность программ-вымогателей — они затронули лишь 4% организаций по всему миру. Но уверенно растут атаки на облачные хранилища — от них пострадали 18% организаций. В результате 49% компаний планируют увеличить в следующем году бюджет облачной безопасности.

Растёт число многовекторных атак на госпредприятия и бюджетные учреждения, такие атаки проводятся для запугивания, шпионажа или остановки работы предприятия. При этом 97% организаций оказались к ним не готовы.

— Чем отличаются такие атаки в России по сравнению с другими странами? Приведите примеры кейсов из банковской сферы.

— Принципиальных различий между атаками на разные страны нет. Общие тенденции одинаковы. Например, массовость и общедоступность. Сегодня кибератаку может совершить любой пользователь, купив в даркнете вирусную программу, например, GandCrab Ransomware-as-a-Service. Выкуп с жертв делится в соотношении 60/40, где большую часть получает покупатель программы, а меньшую — разработчик. В течение двух месяцев 2018 года они атаковали более 50 тыс. жертв и потребовали от 300 тыс. до 600 тыс. долларов выкупа.

Примеры из финансовой сферы. В сентябре 2017 года Equifax, одно из трёх крупнейших кредитных агентств США, пострадало от нарушения, затронувшего более 145 млн клиентов. Используя уязвимость в программном пакете «Apache Struts», хакеры украли конфиденциальные данные, включая имена, адреса, даты рождения, номера кредитных карт, социального страхования и водительских прав.



Василий ДЯГИЛЕВ
глава
представительства
Check Point Software
Technologies
в России и СНГ

В 2017 году мир столкнулся с угрозами пятого поколения — крупномасштабными разнонаправленными атаками, вызывающими крупные инфраструктурные и финансовые потери.



Если раньше было достаточно добавить новую технологию, подстроенную под каждый тип атаки, то сейчас такой подход не работает. Вредоносное ПО пятого поколения способно обойти все стандартные способы защиты

Deloitte, одна из крупнейших в мире аудиторских компаний, стала жертвой кибератаки, которая оставалась незамеченной несколько месяцев и затронула шестерых крупных клиентов. Считается, что хакеры взломали учётную запись администратора системы электронной почты Deloitte, которая хранилась в облаке Azure.

Летом 2018 года возник ажиотаж вокруг массовой утечки личных данных сотрудников Сбербанка. В сеть попала часть адресных книг сотрудников. Несмотря на заверения банка, что информация не угрожает клиентам, такие утечки всё равно опасны, поскольку приводят к мас-

совому фишингу, который 64% IT-специалистов считают главной угрозой современности.

— Для борьбы с кибератаками пятого поколения уже не подходят методы прошлых лет. Что такое современная защита?

— Если раньше было достаточно добавить новую технологию, подстроенную под каждый тип атаки, то сейчас такой подход не работает. Вредоносное ПО пятого поколения способно обойти все стандартные способы защиты. Программы быстро развиваются, гибридные и часто демонстрируют несколько совершенно разных функций.

Чтобы противостоять таким угрозам, нужна новая модель построения ИБ. Например, продвинутая система, которая равномерно предотвращает атаки на IT-инфраструктуру: с одним центром управления для администрирования, мониторинга и реагирования. В режиме реального времени она отслеживает и предотвращает известные и неизвестные угрозы пятого поколения.

Беседовала Анна Воробьева

БЕЗБУМАЖНЫЙ БАНК

ОБЗОР ТЕХНОЛОГИИ И ОСОБЕННОСТИ ЕЁ РЕАЛИЗАЦИИ

Всего лишь несколько десятилетий назад идея создания такого банка, в котором услуги клиенту предоставлялись бы без использования бумажных документов, казалась весьма утопичной. Однако неуклонное увеличение объёмов обрабатываемой информации и развитие информационных технологий заставляет отбросить стереотипы и превратить, казалось бы, фантастические идеи в реальные работающие схемы обслуживания клиентов.

Сбербанк — одна из первых российских компаний, которая взялась внедрить юридически значимый электронный документооборот между банком и клиентом, перенимая мировой опыт ведущих иностранных компаний. Причём в Сбербанке этим начали заниматься задолго до того, как диджитализация стала мейнстримом отечественной экономики. Сейчас масштабы ежегодного роста доли электронных документов в России в различных сферах бизнеса поражают воображение: если пару лет назад речь шла об оборотах, исчисляющихся в миллионах электронных документов в год, то сейчас это миллиарды. Именно поэтому Сбербанк «не верит в бумагу» и делает всё для цифровизации своего бизнеса и развития цифровой экономики.

Несомненный факт, что удержание лидирующих позиций в современном цифровом мире требует быстрой реакции на происходящие изменения среды: постоянного контроля потребностей клиента и разработки новых продуктов и сервисов, актуализации существующих бизнес-моделей, автоматизации и упрощения бизнес-процессов. Для решения этих задач банкам необходима трансформация из классического финансового института с кипой бумаг в цифровую организацию, деятельность которой строится на основе использования современных решений. Одним из таких решений стала технология безбумажного фронт-офиса (БФО), работа над которой началась в 2014 году и продолжается до сих пор в рамках проекта с говорящим названием «Безбумажный мир».

ТЕХНОЛОГИЯ БФО И ЭФФЕКТ ОТ ВНЕДРЕНИЯ

БФО представляет собой технологию электронного взаимодействия банка и клиента, основанную на максимальном сокращении бумажного документооборота между ними за счёт предоставления клиенту удобного и безопасного спо-

соба оформления операций. Внедрение этой технологии позволяет сократить издержки, оптимизировать трудозатраты и минимизировать операционные риски при исполнении поручений, а клиенту, в свою очередь, получить более гибкий, защищённый и быстрый способ получения банковских услуг.

Электронные документы имеют ряд преимуществ перед бумажными аналогами. Во-первых, это экономический эффект — уменьшение расхода бумаги и затрат на закупку и обслуживание печатной техники, транспортировку документов, аренду и (или) покупку значительных площадей для их хранения.

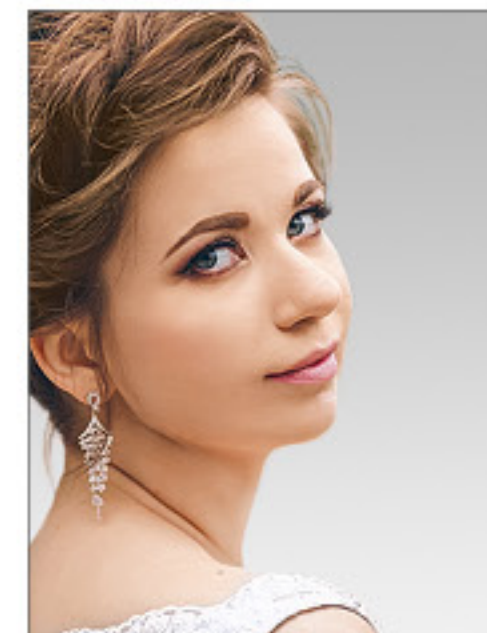
Во-вторых, эффективный контроль — возможность быстро отследить путь и статус документа от момента его создания до уничтожения. Природа электронного документа такова, что его обработка формирует цифровой след в информационном пространстве. Цифровой след содержит подробную информацию не только о самом электронном документе, но и действиях пользователей, связанных с его обработкой на протяжении всего жизненного цикла. С момента начала крупномасштабного перевода документооборота в цифровой формат эффективность контроля увеличилась по сравнению с бумажным документооборотом более чем в два раза, а факты утраты или неспособности найти нужный клиентский документ свелись к нулю.

В-третьих, удобство поиска и хранения — электронный архив позволяет найти необходимый документ даже пятилетней давности за считанные минуты, не требуя при этом больших трудозатрат со стороны сотрудника.

В-четвёртых, повышение скорости работы — высокая скорость создания, обработки и передачи документов способствует повышению скорости обслуживания клиентов. В частности, эффект только от внедрения технологии БФО при обслуживании клиентов в офисах Сбербанка привёл к росту скорости совершения клиентской операции на 30%.

В-пятых, расширение границ ведения бизнеса — отсутствует необходимость физического присутствия клиента в офисах обслуживания, что даёт возможность вести бизнес удалённо или в любом удобном для клиента месте.

В настоящее время доля электронных документов в офисах обслуживания клиентов Сбербанка превышает 85%. Динамика роста доли



Диана КНЯЗЕВА
главный инженер
Управления
экспертизы
кибербезопасности
Сбербанка

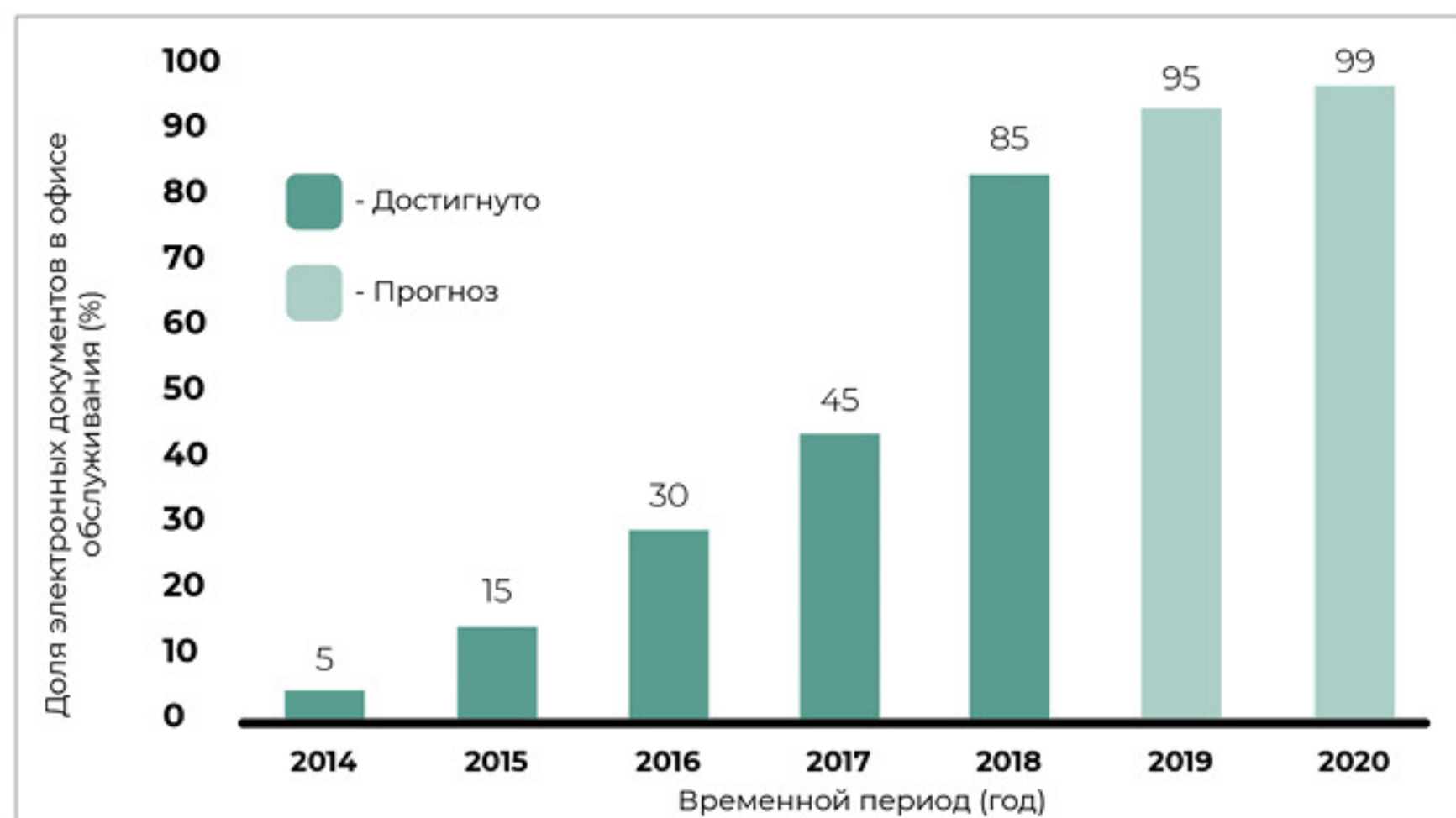


Рисунок 1. Динамика роста доли безбумажного документооборота в офисах обслуживания

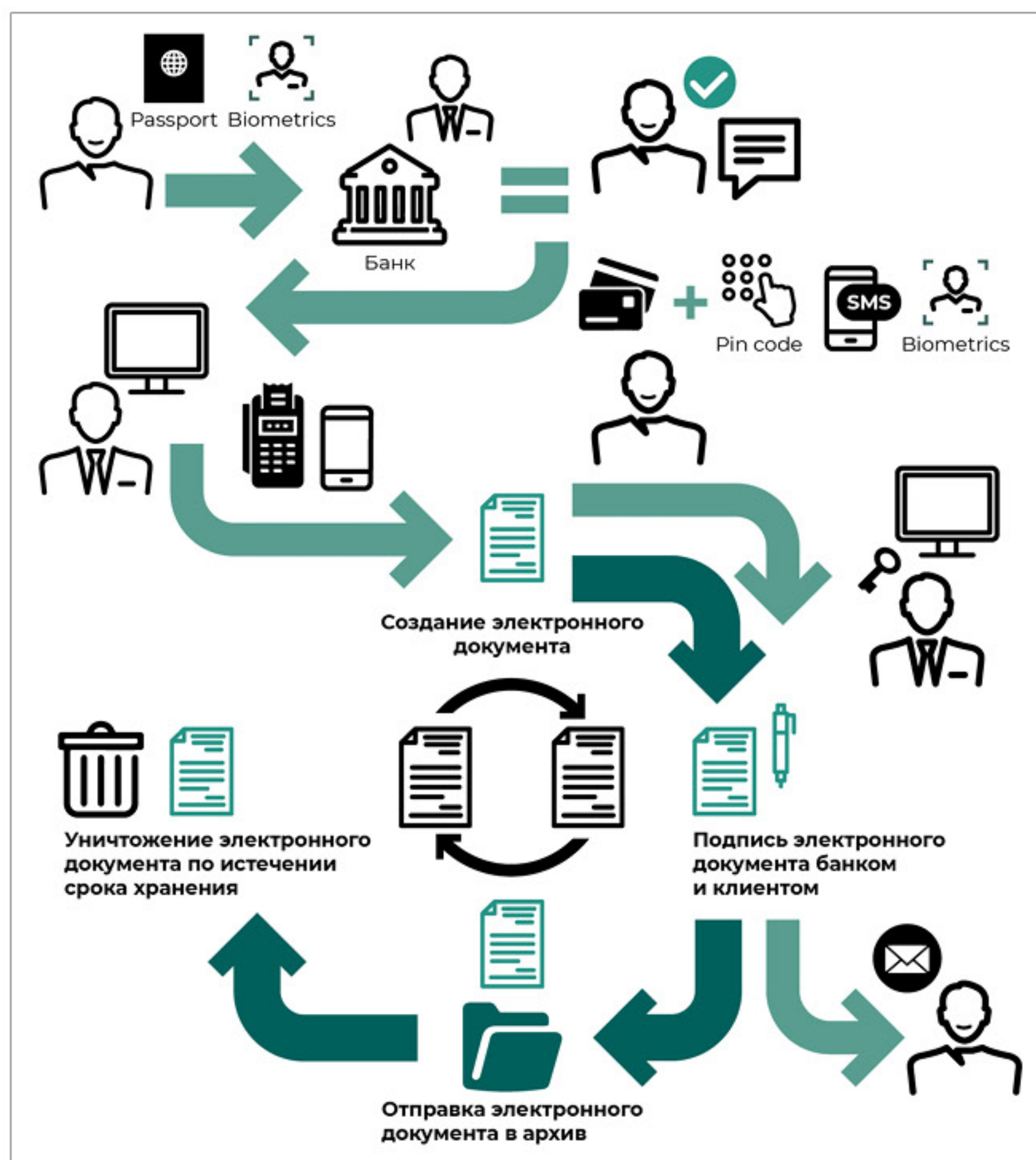


Рисунок 2. Жизненный цикл электронного документа

безбумажного документооборота, в том числе и прогнозируемая, приведена на графике (рис.1).

В Сбербанке технология БФО встроена в процессы обслуживания по вкладам, счетам и картам, при предоставлении услуг аренды индивидуальных сейфов, переводов и платежей в пользу поставщиков услуг. Ведутся работы по переходу на безбумажное обслуживание кли-

ента в более консервативных процессах, таких как оформление кредитных продуктов и банковских доверенностей. К примеру, уже сейчас в таком сложном продукте, как ипотечное кредитование с электронной регистрацией сделки в Росреестре, число бумажных документов сведено до одного — это заявление на выпуск электронной подписи, полстранички текста на каждого участника даже сложных альтернативных сделок. Все остальные документы, начиная от договора купли-продажи и вплоть до выписки из ЕГРП, приходят участникам сделки по электронной почте, а очное взаимодействие покупателя, продавца и сотрудника банка сведено до одной встречи, которая по продолжительности не превышает двух часов. Но здесь заслуга не только банка, но и государственных ведомств, которые синхронно переводят свои услуги в электронный формат, что делает возможным удалённое получение государственных услуг.

МЕСТО БФО В БИЗНЕС-ПРОЦЕССЕ

Типовой жизненный цикл электронного документа, сформированного по технологии БФО, и его место в бизнес-процессах представлены на рис. 2.

Клиент обращается в банк за услугой, а банк, в свою очередь, устанавливает личность клиента, определяет его потребность, формирует черновик операции и соответствующий электронный документ на основании введённых в систему данных. Сформированный документ отображается клиенту на экране электронного устройства. Цифровая природа документа позволяет использовать для одного и того же документа разные стили форматирования в зависимости от особенностей канала и устройства вывода. Можно подчеркнуть основные реквизиты и суть подтверждаемой операции, а вторичные параметры «убрать под кат», чтобы не распылять внимание клиента.

Далее клиент принимает решение о подтверждении операции и нажимает кнопку «подтвердить» на устройстве вывода электронного документа. На этапе подтверждения дополнительно осуществляется аутентификация одним из выбранных клиентом способов: считывание карты и ввод ПИН-кода (PIN) или ввод кода, полученного в SMS-сообщении, или биометрическая аутентификация. В случае успешной аутентификации формируется блок данных, который составляет простую электронную подпись (ЭП) клиента и помещается в электронный документ в поля, предназначенные для собственноручной подписи клиента.

Сформированный электронный документ отображается сотруднику банка для ознакомления

и подписания усиленной ЭП. Подписанный документ передаётся на хранение в электронный архив. По истечении срока хранения он удаляется из архива. Электронный документ, подписанный всеми участниками, может быть направлен клиенту по цифровым каналам связи. Кроме того, клиенту по его желанию может быть предоставлена распечатанная бумажная копия электронного документа.

Описанный выше способ применения технологии БФО универсален и может быть использован в различных каналах. Однако при выборе инструментов и методов реализации необходимо учитывать специфичные для электронных документов риски.

ПОТЕНЦИАЛЬНЫЕ РИСКИ

Ознакомиться с потенциальными рисками, специфичными для электронных документов, а значит, и рисками внедрения технологии БФО, можно на рис. 3.

Правовой риск — несоблюдение требований законодательства Российской Федерации при формировании юридически значимого электронного документа. В отличие от «классических» бумажных документов здесь есть проблема с неопределённой и (или) отсутствующей практикой обеспечения неотказуемости факта совершения сделки между участниками электронного взаимодействия. При использовании простой ЭП авторство и целостность документа доказываются по косвенным данным (логи, журналы аудита, выгрузки смежных АС) и результаты экспертизы могут существенно отличаться в зависимости от персоны конкретного эксперта.

Риск несанкционированного доступа (НСД) — получение доступа к документу в результате нарушения правил разграничения доступа или их отсутствия. В отличие от бумажного носителя цифровые имеют свойство множиться с неконтролируемой скоростью. По сути, каждая передача документа из точки в точку порождает его копию. Поэтому необходимо особое внимание уделять надёжности каналов передачи данных и процедур аутентификации участников электронного взаимодействия на всех этапах бизнес-процесса.

Риск недоступности — невозможность предоставления документа с юридической силой по запросу клиента и (или) органов государственной власти. Банальный технический сбой может в один миг уничтожить весь архив. Поэтому отдельный фокус внимания направлен на обеспечение безопасности электронного архива, систем резервного копирования и восстановления данных. Но здесь есть и обратная сторона — избыточное копирование плодит дополнительные точки компрометации.



Рисунок 3. Риски, специфичные для электронных документов

Риск утечки — следствие реализации риска несанкционированного доступа. Если из физического архива незаметно вынести можно только несколько папок, то из цифрового хранилища — всё.

Риск модификации или подмены — несанкционированное изменение документа или его подмена в результате отсутствия процедур контроля целостности документа на каждом этапе жизненного цикла документа.

Многие организации, переходящие или планирующие переход на электронный документооборот с частным клиентом, слишком концентрируются на вопросах НСД, пренебрегая юридическими аспектами. Однако задача обеспечения кибербезопасности цифрового документа ничем не отличается от задачи защиты любого другого цифрового актива. Когда организация не ощущает уверенности, что их, к примеру, расчётная или биллинговая система достаточно безопасна, то переход на цифровой документооборот либо преждевременен, либо переоценён по эффективности. Недооценка же правовых рисков, в свою очередь, может в какой-то момент перечеркнуть все усилия по обеспечению целостности и конфиденциальности во всех системах компании. Описанный ниже практический опыт поможет минимизировать вышеизложенные риски и избежать основных ошибок при реализации безбумажной технологии за счёт соблюдения как требований регуляторов, так и требований кибербезопасности.

ПРО ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

При предоставлении клиенту сервиса безбумажного оформления операций необходимо руководствоваться положениями следующих нормативных документов: Гражданский кодекс

Российской Федерации (ГК РФ) и Федеральный закон N 63-ФЗ «Об электронной подписи» от 06.04.2011 (63-ФЗ).

В соответствии с п. 2 ст. 160 ГК РФ при совершении сделок, помимо собственноручной подписи, допускается использование электронной подписи. Регулирование отношений в области использования электронных подписей при совершении гражданско-правовых сделок и иных юридически значимых действий осуществляет 63-ФЗ.

Согласно этим нормативно-правовым актам, перед тем как предложить клиенту формирование документов по технологии БФО, необходимо убедиться, что между организацией и клиентом заключён специальный договор (соглашение), определяющий условия и порядок электронного взаимодействия между ними. При этом нужно понимать, что клиент может расторгнуть данное соглашение в любой момент времени, что вызывает необходимость проверки актуальности такого соглашения при каждом обращении клиента.

В Сбербанке таким якорным документом является договор банковского обслуживания (ДБО). В целевой картине это единственный документ, который хранится в бумажном виде и подписывается собственноручной подписью. Однако если заглянуть за горизонт, то развитие государственных сервисов по идентификации частных лиц даёт все предпосылки к тому, что и ДБО станет электронным документом. В качестве собственноручной подписи клиента в таком случае будет использоваться облачная подпись, выданная государством данному гражданину после прохождения им аутентификации через общегосударственные сервисы Единой системы идентификации и аутентификации и (или) Единой биометрической системы.

В соответствии с 63-ФЗ участники электронного взаимодействия вправе использовать электронную подпись любого вида по своему усмотрению, если иное не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами, либо соглашением между участниками электронного взаимодействия. Существует два вида ЭП: простая и усиленная (которая, в свою очередь, делится на квалифицированную и неквалифицированную).

Формально законодательство не устанавливает требований к составу простой ЭП, поэтому она может представлять собой любой блок данных и быть интегрирована в электронный документ по любым событиям, о которых банк заранее договорится с клиентом (в нашем слу-

чае — ДБО). Однако при формировании такого блока данных необходимо учитывать, что содержащаяся в нём информация должна обеспечить доказуемость того факта, что «событие» действительно наступило, и не быть при этом избыточной. Допускается использовать как бизнес-параметры операции, так и технические.

Сбербанк в своей практике придерживается минимально достаточного набора данных, который позволяет точно определить клиента, дату и время операции, факт аутентификации клиента, способ подтверждения операции. Для определения лица, подписавшего документ согласно ст. 9. 63-ФЗ, набор данных составляющих простую ЭП должен быть интегрирован в электронный документ в поля, предназначенные для собственноручной подписи клиента.

При реализации безбумажной технологии взаимодействия с клиентом необходимо предусмотреть возможность ознакомления всех сторон с подписываемыми электронными документами перед непосредственной процедурой подписания и визуализации результатов проверки ЭП всех подписантов согласно 63-ФЗ. Законодательство не устанавливает ограничений на типы электронных устройств отображения документов, поэтому Сбербанк использует в офисах обслуживания наиболее удобные и привычные для клиента устройства — POS-терминал или планшет, а для сотрудника средством вывода дополнительно может служить экран монитора рабочего места.

ГК РФ не устанавливает обязанности сторон использовать при электронном взаимодействии какие-либо конкретные информационные технологии и (или) технические устройства. Аналогичное правило содержится, например, в п. 2 ст. 463-ФЗ, согласно которому одним из принципов использования электронной подписи является возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования, установленные для конкретных видов электронных подписей.

Всё вышесказанное необходимо учитывать при выборе способов реализации технологии электронного взаимодействия с клиентом, однако юридические аспекты реализации — это только половина пути при движении в сторону цифровой трансформации бизнеса. Вторая половина — обеспечение кибербезопасности.

(Окончание в следующем номере)

ТЕХНОЛОГИЯ ЗАЩИТЫ ОТ УГРОЗЫ ПОДМЕНЫ БИОМЕТРИЧЕСКОГО СКАНЕРА

ЧАСТЬ 3. ВОЗМОЖНЫЕ РИСКИ И МЕХАНИЗМЫ ЗАЩИТЫ СХЕМЫ АУТЕНТИФИКАЦИИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ¹



Максим ФЕДОТЕНКО
руководитель направления Центра внутри-корпоративного взаимодействия Сбербанка

В любом процессе распределения аутентификаторов, также, как и в описанной схеме аутентификации мобильного приложения, есть свои проблемы кибербезопасности, связанные с внешними субъектами, а иногда и внутренними злоумышленниками. Рассмотрим выявленные нами угрозы и поговорим о возможностях защиты от них. Сразу отметим, что все риски рассматриваются в общем случае, когда

аутентификация пользователя в мобильном приложении не осуществляется или происходит только при помощи биометрии. При иллюстрации на рисунках жёлтым цветом подсвечиваются легитимные артефакты, похищенные злоумышленником, а красным — артефакты, сгенерированные злоумышленником и выдаваемые им за легитимные.¹

¹ Окончание. Начало в № № 1, 2 / 2019

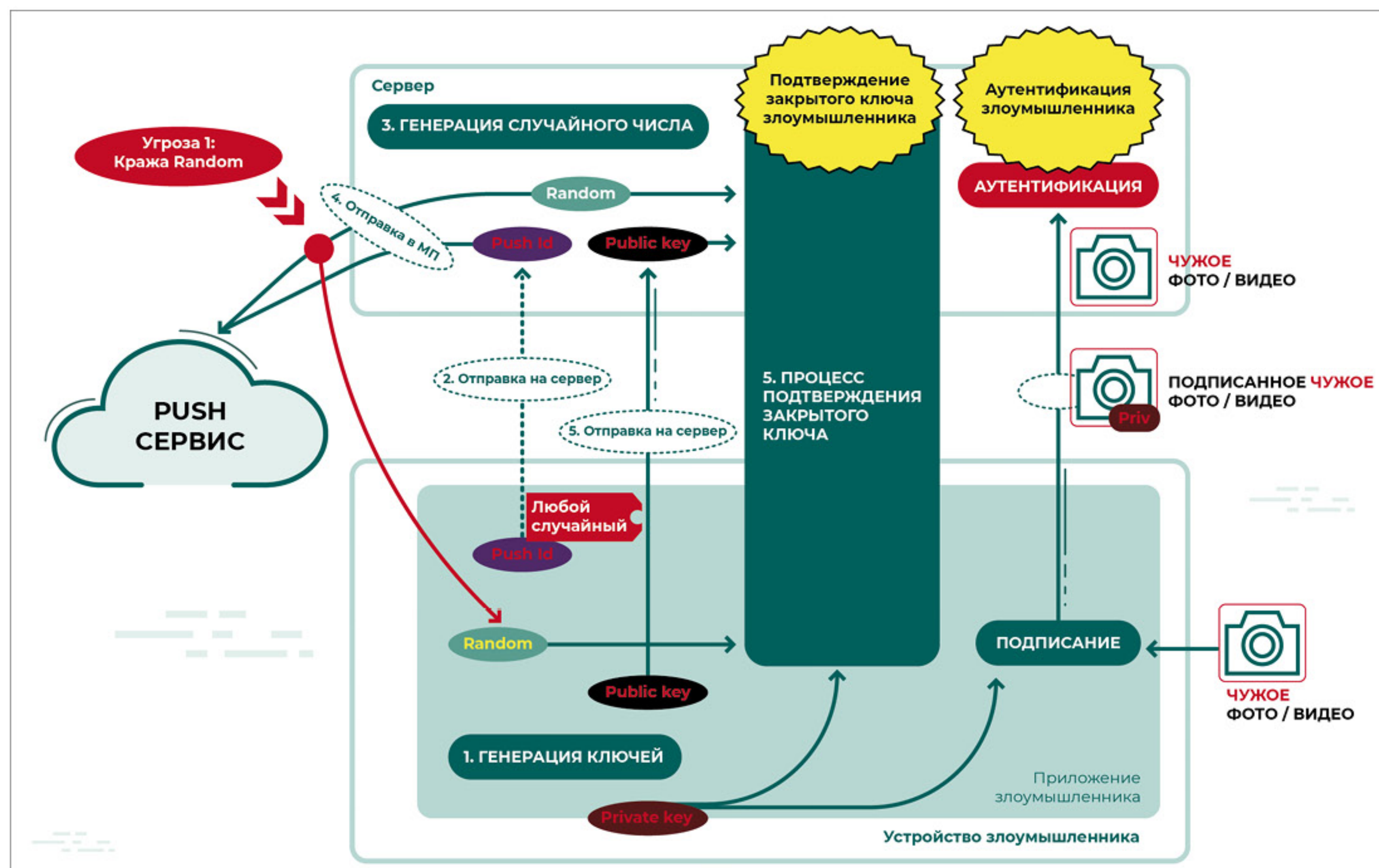


Рисунок 1. Угроза кражи случайного числа на серверной части или в push-сервисе

УГРОЗА 1: КРАЖА СЛУЧАЙНОГО ЧИСЛА

Значение случайного числа, передаваемого через push-уведомление, неизвестно злоумышленнику — на этом постулате основана вся схема создания аутентификатора для мобильного приложения. В случае перехвата его на сервере или в push-сервисе защита рухнет, и злоумышленник сможет акцептовать собственное мобильное приложение (рисунок 1).

Действительно, в данном случае злоумышленнику уже неинтересно, дойдёт ли push-уведомление до какого-нибудь мобильного приложения — ему вообще не нужно использовать официальное мобильное приложение. Злоумышленник отправляет любой случайный push-идентификатор, получает сгенерированное случайное число на серверной части, передаёт его в своё приложение, подписывает на собственном закрытом ключе и отправляет на сервер, где подтверждается закрытый ключ злоумышленника. Хотя такая кража маловероятна, но в случае Сбербанка перед отправкой push-уведомление проходит большое количество внутренних систем перед тем, как попасть в push-сервис производителя операционной системы. Поэтому защитные меры необходимы. Шифро-

вание здесь не поможет, так как мы можем зашифровать сообщение только в адрес того же самого злоумышленника, и он его легко расшифрует. Защититься от угрозы можно только при помощи организационных мер и end-to-end защитой канала от сервера к push-сервису. Это стандартные меры защиты, поэтому останавливаться на них мы не будем.

УГРОЗА 2: КРАЖА PUSH-ИДЕНТИФИКАТОРА И СЛУЧАЙНОГО ЧИСЛА НА УСТРОЙСТВЕ

Следующая угроза — перехват злоумышленником push-идентификатора и случайного числа на своём мобильном устройстве с установленным легитимным приложением (рисунок 2).

Вначале злоумышленнику нужно будет получить push-идентификатор и передать в собственное приложение для регистрации возможности отправки push-уведомлений и собственного открытого ключа, а затем уже перехватить случайное число, чтобы зарегистрировать свой закрытый ключ. После этого злоумышленник сможет использовать этот закрытый ключ для подписи любых фотографий.

Например, в случае Android и сервиса Firebase Cloud Messaging перехватить push-идентификатор можно следующим образом:

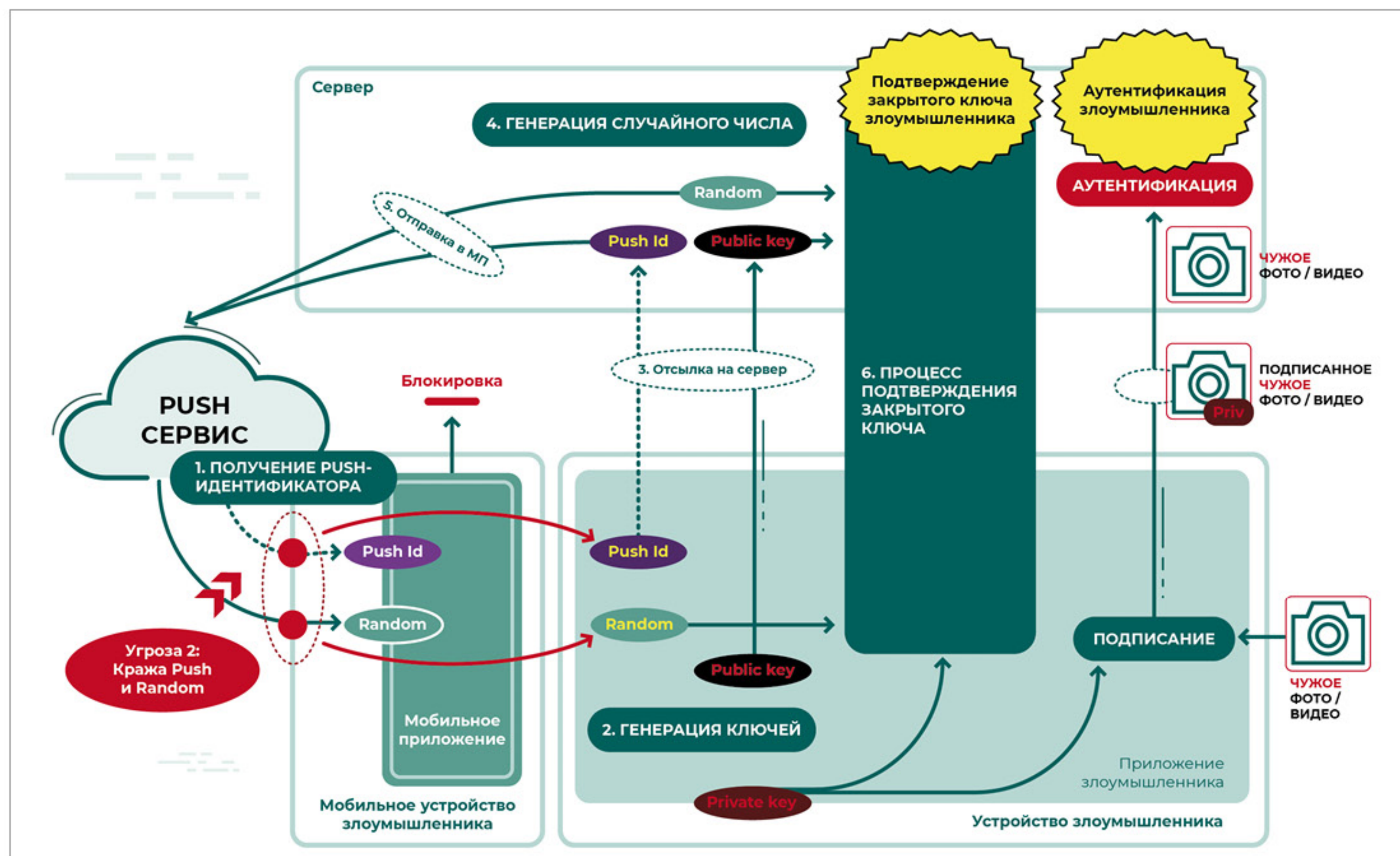


Рисунок 2. Угроза кражи push-идентификатора и случайного числа при использовании злоумышленником легитимного мобильного приложения


```
<service android:name=".MyNotificationListener" android:label="@string/app_name"
android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter>
        <action
            android:name="android.service.notification.NotificationListenerService" />
        </intent-filter>
    </service>
```

фикатор можно при помощи простого прокси-сервера (например, Burp Suite) с подменой TLS-сертификатов, так как Android при обращении к этому облачному сервису не осуществляет TLS-пининг. Поэтому достаточно установить в хранилище доверенных сертификатов мобильного устройства сертификат прокси-сервера и найти push-идентификатор в расшифрованном трафике.

Запрос будет выглядеть примерно следующим образом (здесь он сильно сокращён).

```
POST /c2dm/register3 HTTP/1.1
app: ru.mfedotenko.push
Host: android.clients.google.com
X-subtype=...&X-X-subscription=
...&sender=1136792233789&X-X-subtype=
...&X-app_ver=1&...&X-sig=...&X-cliv=
...&X-gmsv=...&X-pub2=...&X-X-kid...&X-appid=
...&X-scope=*&X-subscription=
...&X-gmp_app_id=1%3A1036791400789%3
Aandroid%3A7e3a9140abe14d85&X-app_ver_
name=...&app=ru.mfedotenko.push&device=
...&cert=...&app_ver=1&info=...&gcm_ver=...
```

А ответ будет содержать push-идентификатор:

```
HTTP/1.1 200 OK
Server: GSE
token=|ID|1|: cFX2BI99kfk: APA91bG-
cxC7DKH1b1abcFZXvREYhonhoy-
BR50cAFS1pZrf6hcsQtot160PmyoSaoth-
klhFa6R-AB--FkVe07YYvTlP1KKpvAVEAv-
aid6vaaIU13thvNN081sC-K6-LWmZfXAnT-
VS75RzcwNwiwiX5r7j9ivJrq0VbQ
```

Далее злоумышленнику необходимо получить отправленное на легитимное мобильное приложение случайное число. Для этого можно воспользоваться приложением из Google Play (например, Notification Blocker, Notification History и т.п.) или разработать собственное². Суть работы этих приложений в том, что они подключаются к системной службе Notification Listener, которая отслеживает все уведомления на устройстве. Естественно, для подключения к службе нужны соответствующие права доступа, которые нужно запросить с использованием файла манифеста (пример см. на врезке в начале страницы).

² Описание одной реализации можно увидеть по ссылке <https://habr.com/post/249167/> или найти примеры на Github (например, <https://github.com/opayen/android-notification-access-sample>)

При запуске такой программы от пользователя потребуется разрешить ей доступ к уведомлениям. После этого в ней можно будет просматривать уведомления, приходящие в наше мобильное приложение.

Как бы производители мобильных устройств ни старались, пользователи имеют возможность получить на своём устройстве полные права администратора. Если в случае со средой Apple iOS можно говорить, что Apple активно борется с jailbreak, хотя и не всегда удачно³, то многие китайские смартфоны с Android продаются уже рутованными.

Однако на уровне мобильного приложения можно реализовывать определение, работает ли оно на jailbreak/root-устройстве. Существует достаточно много как нативных методов (используемых в SDK различных вендоров), так и общедоступных алгоритмов проверки⁴. В мобильных приложениях Сбербанка такие проверки давно реализованы и постоянно совершенствуются, это одна из основных мер их защиты. Однако нужно понимать, насколько эффективно эти методы могут распознать взлом устройства. К сожалению, стопроцентного способа проверки jailbreak/root не существует.

УГРОЗА 3: ПЕРЕХВАТ PUSH-ИДЕНТИФИКАТОРА И СЛУЧАЙНОГО ЧИСЛА В КАНАЛЕ

Следующая угроза — кража с блокировкой отправки push-идентификатора и подписанного случайного числа при передаче из официального мобильного приложения на сервер (рисунок 3).

В этом случае злоумышленник может отослать перехваченные данные на сервер от имени своего приложения и пройти подтверждение его закрытого ключа. Для этого вначале перехватывается сам push-идентификатор и отправляется вместе с открытым ключом приложения злоумышленника, а затем и случайное число, которое пересылается приложением злоумышленника, подписанным на его закрытом ключе.

³ <https://4pda.ru/forum/index.php?showtopic=403138>, <https://www.reddit.com/r/jailbreak/wiki/escapeplan/guides/jailbreakcharts>

⁴ Примеры — в статьях «Как защитить свою iOS-программу от взлома» (<http://pshenichny.livejournal.com/36316.html>) и «Распознавание крякнутой версии (Anti-Piracy)» (<http://ilya2606.ru/?p=13>)

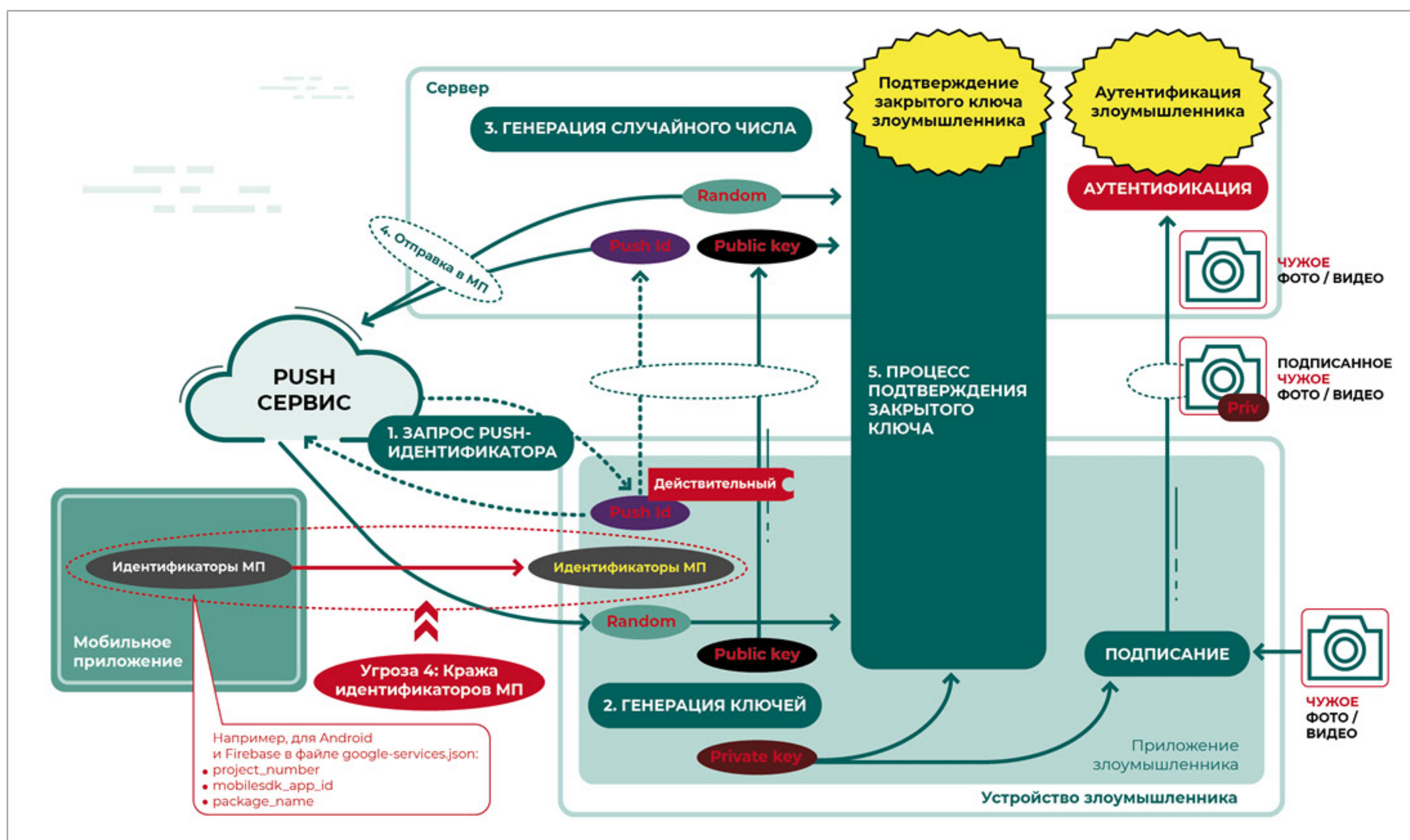


Рисунок 4. Угроза кражи идентификаторов мобильного приложения

бильного приложения, так что оно всё равно будет получать push-уведомления. Другими словами, он сможет создать свой аутентификатор и этим закрытым ключом будет подписывать биометрические данные, но при этом, например, в нём будут отключены механизмы liveness detection.

Защита от реверс-инжиниринга мобильного приложения — крайне сложная задача, которая не может быть выполнена на 100 %. В этом случае необходимо производить обфускацию кода⁷ или шифрование публикуемого в магазине приложения, а также заложить в мобильное приложение методы защиты от манипуляций со средой выполнения (runtime) при помощи отладчика. Для платформы Apple iOS шифрование производится автоматически средствами App Store с использованием DRM-технологии FairPlay⁸, а для платформы Android имеет смысл воспользоваться обфускатором (например, бесплатным обфускатором ProGuard⁹, распространяющимся с Android Studio).

⁷ Запутывание исходного кода с целью защиты от реверс-инжиниринга

⁸ Обход этой технологии также возможен (см. <https://habrahabr.ru/post/199128/>)

⁹ <https://www.guardsquare.com/en/proguard>, https://github.com/codepath/android_guides/wiki/Configuring-ProGuard

УГРОЗА 5: КРАЖА ЗАКРЫТОГО КЛЮЧА

Угроза связана с получением собственно аутентификатора (закрытого ключа) мобильного приложения. Злоумышленнику достаточно получить закрытый ключ и использовать его в дальнейшем для подтверждения биометрических данных со своего нелегитимного приложения, которое, например, всегда отправляет одну и ту же фотографию и не использует методы защиты типа liveness detection. Причём получить закрытый ключ он должен на своём мобильном устройстве с использованием официального мобильного приложения, а использовать потом может в любом приложении на любой платформе, в том числе немобильной (рисунок 5).

Получить закрытый ключ можно разными путями: например, при помощи резервной копии. При создании резервной копии iOS с ис-

google-services.json	strings.xml	AndroidManifest.xml
project_number	gcm_defaultSenderId	—
mobilesdk_app_id	google_app_id	—
package_name	—	package

Таблица 1. Названия идентификаторов для платформы Android

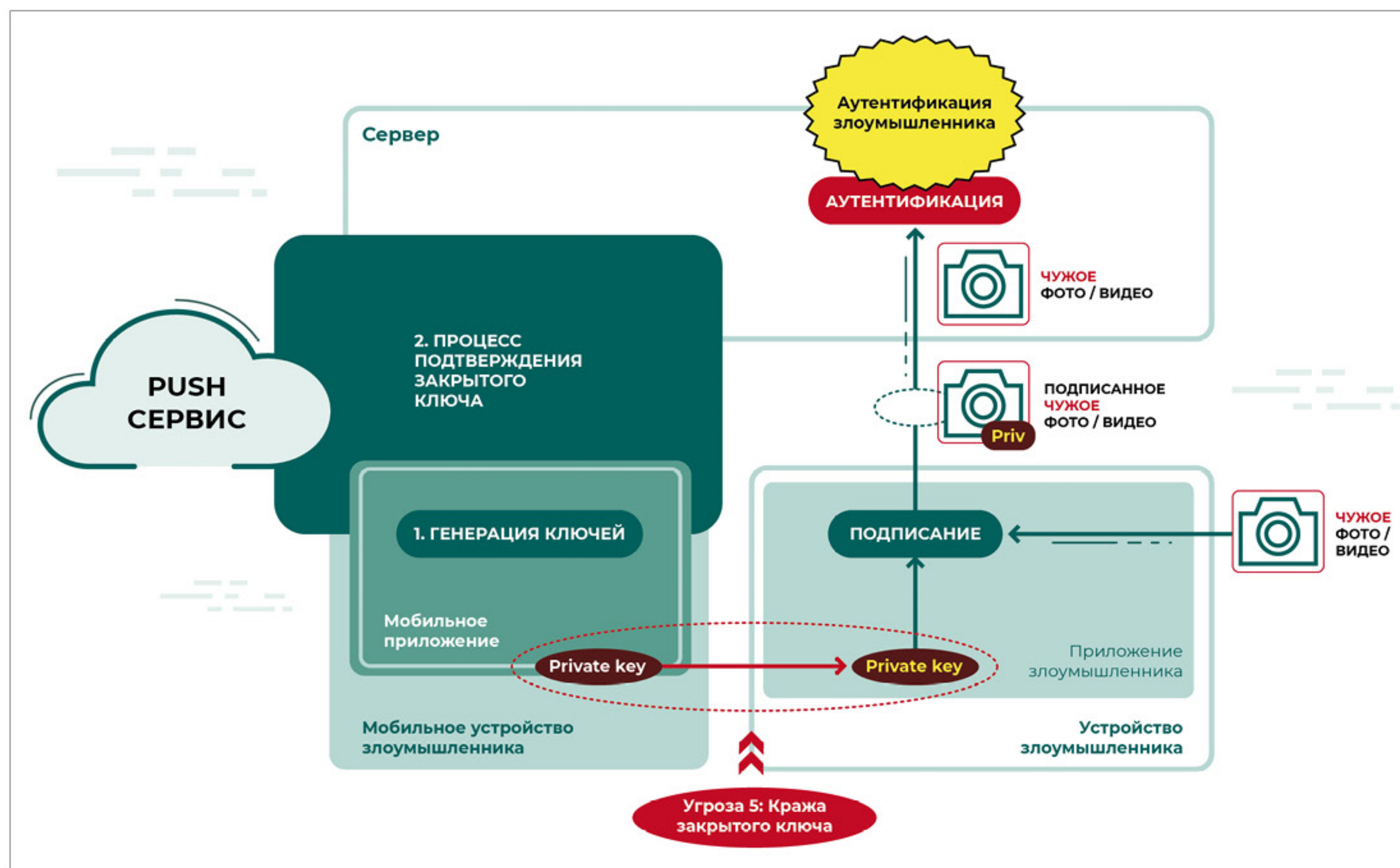


Рисунок 5. Угроза кражи закрытого ключа мобильного приложения

пользованием iTunes, если использовать защиту резервной копии при помощи пароля, то все данные, в том числе данные keychain¹⁰, шифруются на этом ключе и могут быть легко расшифрованы злоумышленником (который сам и вводил пароль на резервную копию). Поэтому для защиты keychain от резервного копирования необходимо применять специальные атрибуты при его создании:

- ♦ Атрибут kSecAttrSynchronizable, отвечающий за возможность синхронизации keychain с другими устройствами, в том числе в рамках резервного копирования, необходимо установить в значение kCFBooleanFalse, то есть запретить синхронизацию.

- ♦ Атрибут kSecAttrAccessible, отвечающий за доступ в программе к keychain, необходимо установить в любое значение, оканчивающееся на ThisDeviceOnly (kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly, kSecAttrAccessibleWhenUnlockedThisDeviceOnly, kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly, kSecAttrAccessibleAlwaysThisDeviceOnly). Выбор константы определяется логикой работы приложения. Описание этих констант можно посмотреть на портале

¹⁰ <https://developer.apple.com/library/content/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html>

разработчика Apple¹¹, они определяют различные условия доступа к keychain на устройстве, но без возможности переноса на другие устройства.

Ещё один вариант — это атака, связанная с получением полных прав (jailbreak/root) на своём устройстве. А в старых версиях Android, например, данные в keychain сохранялись зашифрованными на PIN-коде разблокировки устройства, а в случае его отсутствия — в открытом виде. О мерах защиты в этом случае мы говорили, когда разбирали угрозу 2.

Иногда предпочтительнее не сохранять закрытый ключ в хранилище ключей (keychain), предоставляемом соответствующей мобильной операционной системой, так как злоумышленник на собственном мобильном устройстве может получить к ним доступ. В этом случае предлагается использовать нативные средства мобильного приложения для хранения и защиты закрытого ключа. Общих рекомендаций по такому хранению нет, каждый разработчик осуществляет его по-своему. Однако в этом случае также необходимо производить обфускацию кода приложения.

¹¹ <https://developer.apple.com/documentation/security/ksecattraccessible>

УГРОЗА 6: УГРОЗА КРАЖИ ПОДПИСАННОГО ФОТО/ВИДЕО И ЕГО ПЕРЕИСПОЛЬЗОВАНИЕ

Мы подошли к последнему шагу процесса — аутентификации пользователя (или подтверждения операции) при помощи биометрии. На нём возможен перехват подписанных биометрических признаков (выше были показаны возможности такого перехвата) и их повторного использования для аутентификации (рисунок 6).

Возможности защиты от такого вида угроз показаны на рисунке 7.

Во-первых, для того чтобы нельзя было перехватить подписанную фотографию, необходимо использовать зашифрованный TLS-канал с проверкой сертификата сервера по прикрепленному сертификату, о чем мы говорили выше. Во-вторых, можно подписывать не просто фотографию, а некоторый пакет данных, включающий в себя дополнительную информацию о текущей аутентификации. Например, можно использовать алгоритмы генерации одноразовых паролей на основе счётчика (RFC 4226. HOTP: An HMAC-Based One-Time Password Algorithm) и/или времени (RFC 6238. TOTP: Time-Based

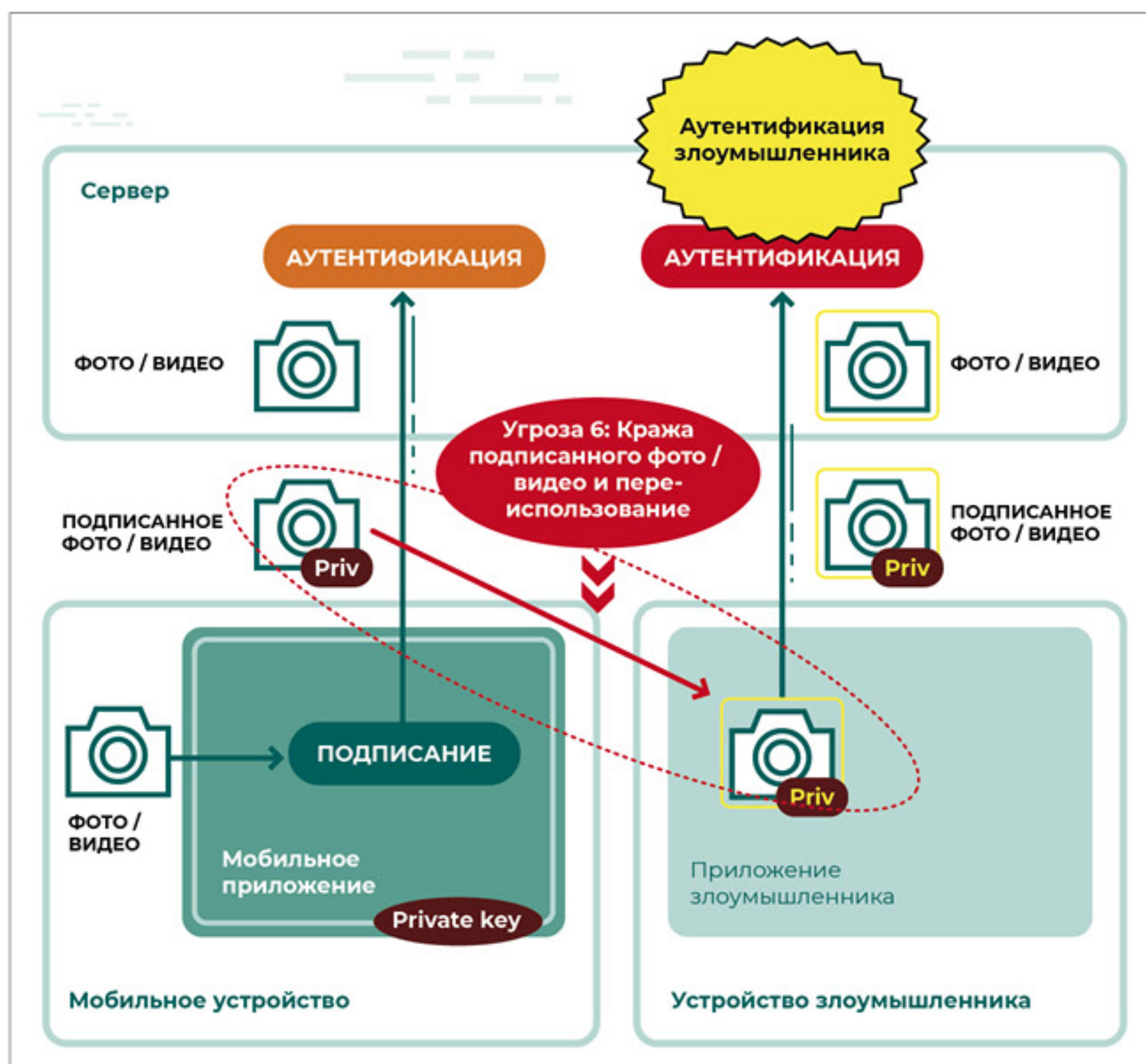


Рисунок 6. Угроза кражи подписанного фото/видео и переиспользование

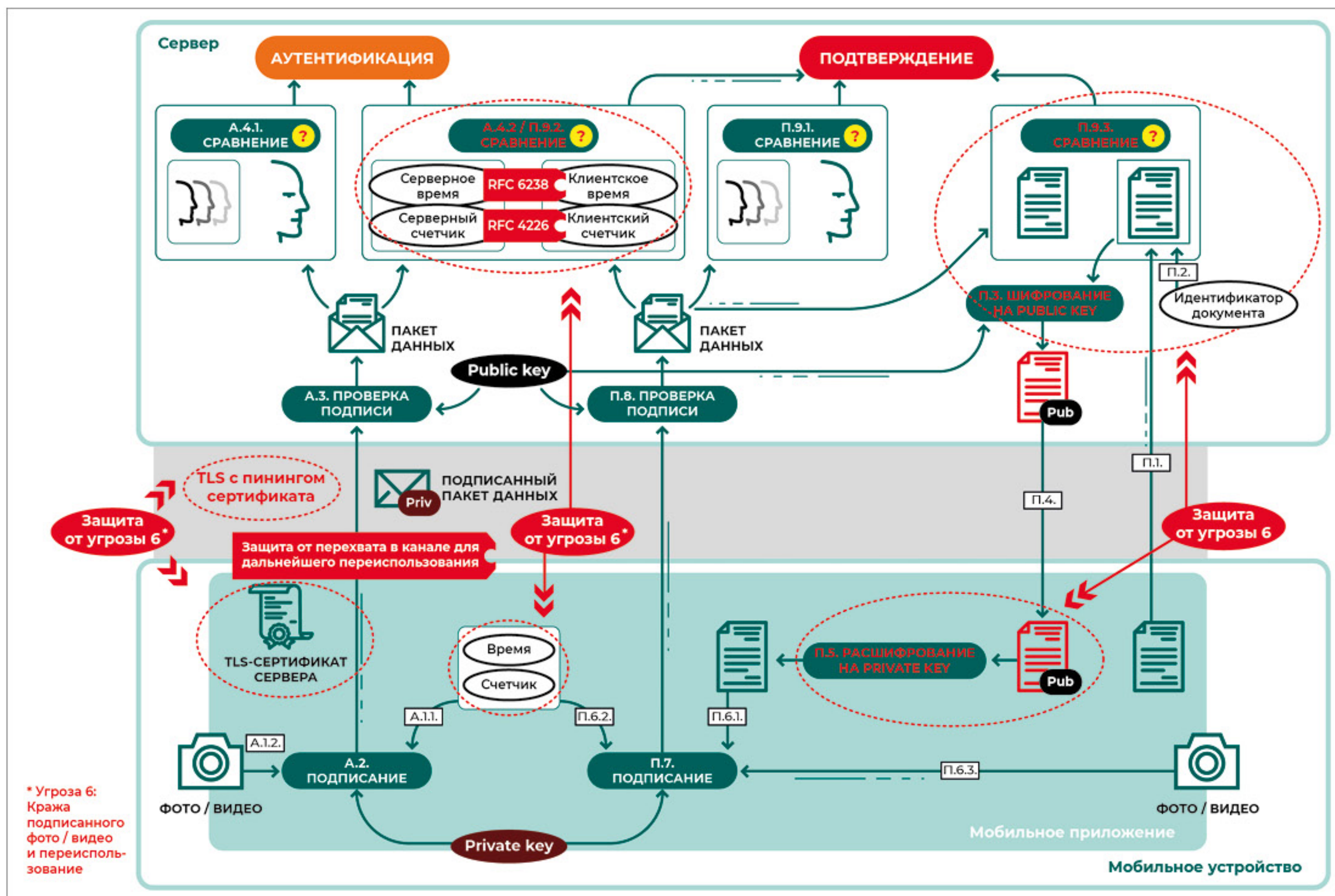


Рисунок 7. Методы защиты от угрозы переиспользования

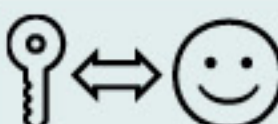
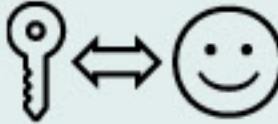
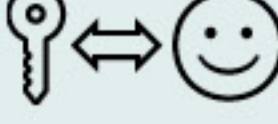
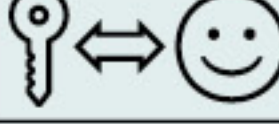
УГРОЗА	ТЕХНОЛОГИЯ ЗАЩИТЫ	АТАКА			
		Целенаправленная		Фишинг	
		Остаточный риск	Актуальность	Остаточный риск	Актуальность
Угроза 1: Кража случайного числа		Нивелируется	Нет	Нивелируется	Нет
Угроза 2: Кража push-идентификатора и случайного числа на устройстве		Снижается	Да	Снижается	Нет
		Не меняется		Нивелируется	
Угроза 3: Перехват push-идентификатора и случайного числа в канале		Нивелируется	Нет	Нивелируется	Нет
Угроза 4: Кража идентификаторов МП		Снижается	Да	Снижается	Нет
		Не меняется		Нивелируется	
Угроза 5: Кража закрытого ключа		Снижается	Да	Снижается	Нет
		Не меняется		Нивелируется	
Атака 6: Кража подписанного фото/видео и переиспользование		Нивелируется	Нет		Нет
Символ	Описание				
	Технические меры				
	Контроль соответствия аутентификатора мобильного приложения и аутентифицируемой по биометрии личности				

Таблица 2. Анализ рисков

One-Time Password Algorithm). Однако нужно не забывать, что клиентские и серверные значения счётчика и времени должны быть синхронизированы, что бывает затруднительно выполнить.

Если биометрические признаки используются для подтверждения документа или транзакции, защититься от повторного использования можно формированием окончательного документа на стороне сервера с включением в него уникального номера документа. После этого сервер шифрует документ на открытом ключе мобильного приложения и отправляет его в приложение. Соответственно, расшифровать документ может только мобильное приложение, обладающее закрытым ключом. При этом сервер должен единожды принять подписанный документ с данным номером и приложенными к нему биометрическими признаками.

АНАЛИЗ РИСКОВ

Выше мы рассмотрели некоторые угрозы, применимые к предложенному методу аутентификации мобильного приложения с использованием открытого API. Теперь же необходимо понять, насколько они актуальны в преломлении тех атак, которые мы затронули во второй части статьи (№ 2/2019), — целенаправленной атаки и фишинга (таблица 2).

Кража случайного числа на серверной части (угроза 1) позволяет зарегистрировать любое приложение сколько угодно раз, что даёт возможность использовать его как для целенаправленной атаки, так и в целях фишинга. Однако организационные меры и end-to-end защита канала с push-сервисом позволяют нивелировать эти риски.

Кража push-идентификатора и случайного числа на устройстве (угроза 2) и их перехват в

канале (угроза 3), а также кража закрытого ключа (угроза 5) в связи с необходимостью использования оригинального приложения для целей фишинга достаточно затруднительны, если на сервере осуществлять контроль соответствия аутентификатора (открытого ключа) мобильного приложения и аутентифицированного при помощи биометрии пользователя. Поэтому злоумышленнику придется каждый раз использовать новое мобильное устройство. В случае канала связи защититься от целенаправленной атаки можно соответствующими настройками TLS. В первом и третьем случаях технические меры не могут стать панацеей, и приходится констатировать, что угроза актуальна при целенаправленной атаке.

В случае кражи идентификаторов мобильного приложения (угроза 4) злоумышленник имеет возможность создать приложение-клон, которое может распространяться в случае Android просто установочным файлом. В официальном магазине опубликовать такое приложение не получится, так как его наименование будет совпадать с официальным. По этой же причине невозможно на одном устройстве установить официальное приложение и его клон. Уменьшить риск централизованного фишинга можно при помощи контроля соответствия аутентификатора мобильного приложения и пользователя. Злоумышленнику будет проблематично заставить пользователей установить нелегитимное приложение в массовом порядке. В случае же целенаправленной атаки любые предлагаемые меры неэффективны. Такие рода угрозы мы сможем отслеживать только стохастическими средствами, такими как антифрод.

С кражей и переиспользованием подписанных биометрических данных (угроза 6) легко бороться при помощи технических средств, таких как добавление номеров посылок и/или времени, а также идентификаторов документов в случае подтверждения.

Итак, актуальными угрозами можно считать:

- ♦ кражу push-идентификатора и случайного числа на устройстве и кражу закрытого ключа, которые ведут к возможности злоумышленником зарегистрировать собственное приложение, обладая доступом к официальному;

- ♦ кражу идентификаторов мобильного приложения, которое позволяет злоумышленнику создать собственное мобильное приложение и распространять его.

Очевидно, чтобы защититься от целенаправленных атак, реализуемых на основе актуальных угроз, необходимо использовать многофакторную аутентификацию, которая включает в себя не только аутентификацию по биометрическим признакам, но и основанную на знании

(knowledge base). Например, в случае Сбербанка Онлайн регистрация мобильного приложения только при помощи биометрии — рискованное занятие. Другое дело — в уже зарегистрированном по стандартному процессу при помощи одноразового пароля, отправляемого в SMS-сообщении, мобильном приложении использовать дополнительную аутентификацию и подтверждение операций в случае подозрения на мошенничество.

Хотя предлагаемая схема защиты может нивелировать риски фишинга, помимо использования стохастических методов необходимо проводить разъяснительную работу среди клиентов, убеждая их не устанавливать мобильные приложения из неофициальных магазинов.

ЗАКЛЮЧЕНИЕ

В статье освещена общая модель киберугроз для процесса биометрической аутентификации в целом, а также на примере лицевой модальности и мобильного канала. Были рассмотрены различные модели биометрического процесса, а также выделена характерная угроза для биометрического процесса в мобильном канале — подмена биометрического сканера (мобильного приложения) и/или биометрических данных, отсылаемых на сервер для целей аутентификации, а также метод защиты от этой угрозы.

В качестве метода защиты предложена схема создания аутентификатора (закрытого ключа) мобильного приложения и подтверждения им используемых биометрических данных. Метод создания аутентификатора предполагает использование нативной push-нотификации, предлагаемой мобильными операционными системами Apple iOS и Google Android, и применяет средства асимметричной криптографии — шифрование и электронную подпись. Были рассмотрены возможные атаки на такую схему подтверждения и меры защиты от них.

К сожалению, предложенная схема аутентификации не может в полной мере противостоять целенаправленным атакам, однако является достаточно эффективным инструментом аутентификации мобильного приложения, использующего открытые интерфейсы взаимодействия с серверными приложениями. В сочетании с такими вероятностными инструментами, как адаптивная аутентификация и антифрод, а также методами двухфакторной аутентификации, основанной на знании (knowledge base), можно получить хорошую защиту биометрических процессов в мобильном приложении. Предложенные в статье механизмы внедряются в Сбербанк в биометрических процессах мобильного канала как одна из мер защиты.



**Александр
БАРАНОВ**

заведующий
кафедрой ИБ НИУ
ВШЭ, доктор физико-
математических наук,
академик Академии
криптографии РФ

ГЛАВНОЕ — ВЫБРАТЬ НАПРАВЛЕНИЕ УДАРА

А ПРИМЕРЫ ИЛОНА МАСКА И ДИФФИ —
ХЕЛЛМАНА ПОМОГУТ НАНЕСТИ УДАР

В конце мая в НИУ ВШЭ состоялась VII Международная научно-практическая конференция «Управление информационной безопасностью в современном обществе». BIS Journal по горячим следам попросил рассказать о ней главного организатора Александра Баранова. Разговор очень быстро повернул в сторону импортозамещения.

— Александр Павлович, судя по пленарному заседанию, проблемы информационной безопасности по-прежнему решаются весьма сложно и имеют два классических направления — технологическое и юридическое. О чём больше говорили?

— Было пять секций. На одной из них рассматривали юридические проблемы — полтора десятка докладов. Речь шла о необходимости корректировки законов — о персональных данных, об электронной подписи, обсуждались возможные направления корректировок, конкретные предложения и т.д.

Остальные четыре секции были посвящены техническим проблемам. Собственно тон задавал доклад профессора А. В. Шмидта, он назывался так: «Достижение цифрового суверенитета РФ как необходимое условие развития российского этноса». Соответственно тема импортозамещения сквозила непрерывно и обсуждалась с разных сторон. Например, президент госкорпорации «Эшелон» Алексей Марков поднял основные проблемы в области анализозащищённости информационных систем, методов анализа, возможностей и пределов этого анализа. Его выступление и послужило затравкой к круглому столу.

— В этом году традиционный круглый стол сосредоточился на проблемах создания и аттестации безопасного прикладного ПО. А что было на прошлой конференции?

— Тогда мы рассматривали вопросы безопасных отечественных или импортозамещённых операционных систем и баз данных. И спустя год, мы констатировали: существенное продвижение в этой области есть. Вопрос из принципиально идеологического состояния перешёл в технологическое. Имеется несколько стабильных операционных систем, как полностью отечественных, так и сделанных на базе Linux.

— А конкретнее?

— Продолжает развиваться криптософтовая QR ОС — очень выгодная, потому что многие приложения, сделанные для Microsoft и Windows, могут работать на этой системе. Главное, что она живёт и развивается — пензенский «КриптоСофт» представил в этом году ряд новых приложений. Если в импортозамещении смотреть несколько веток, то вот эта — полностью отечественная.

Следующая ветвь — это клоны Linux, проверенные и аттестованные по ИБ, — Альт Linux и Астра Linux. И вот на том, как они развиваются, какие прикладные продукты к ним создаются, мы и сосредоточились на конференции. Потому что вся ценность компьютерных систем во все не в операционках, и даже не в их безопасности, а именно в прикладном продукте. Если прикладных задач нет, сама по себе операционка и не нужна.

Другое направление, которое обсуждалось, — отечественные гипервизоры. Какие задачи на их базе можно решать, какие прикладные системы можно строить, на какие уровни безопасности можно выйти. Отмечалось, что гипервизор и платформа «Горизонт», кстати, полностью отечественная, — своеобразный аналог криптософтовой QR ОС. Эта московская разработка тоже очень успешная, аттестованная. Платформа рассчитана на разные операционки и соответственно на много разных прикладных продуктов.

Заодно затронули и положение с базами данных. Констатировали, что фирма Постгресс представила достаточно развитый продукт, под которым появилось много прикладных продуктов. То есть определённый прогресс наблюдается, но по большому счёту ситуация с базами данных по-прежнему тяжёлая. В потреблении и эффективности преобладают Oracle, Microsoft SQL, и вот они-то 90% рынка и определяют.

— Этим вопросам был посвящён круглый стол. Их активно обсуждали представители восьми предприятий-разработчиков защищённых компьютерных систем. Их список сам по себе интересен: «Базальт СПО», «ИЦ «Баррикады», «КриптоСофт», «Открытая мобиль-

ная платформа», «НПО РусБИТех», «Постгрес профессиональный», «НППКТ». А дальше?

— Затем пошли пленарные заседания. Первый вопрос — национальная сим-карта. Представитель компании «Национальная сим-карта» Владимир Олегович Дрелихов помог нам разобраться, что происходит в этом направлении. Как мы поняли, речь идёт об отечественном крипто-кошельке, который будет работать либо через вай-фай, либо через GSM. Конечно, отмечалось, что есть проблема с российской элементной базой, что симку пока удаётся реализовать только на самсунговском типе. Но есть надежда, что «Микрон» сделает нам чип, и симка получится полностью отечественная. По крайней мере, отработка технологии создания крипто-кошелька движется бодро. В прошлый раз нам рассказывали только общую схему и общие представления об этой организации.

Дальше мы обсудили ряд вопросов, связанных с облачными сервисами и методами оценки аутентификации граждан. Тут принципиального прорыва пока не случилось, но доклады были хорошие, глубокие.

— Два доклада были посвящены проблемам развития отечественной элементной базы. В частности, для суперкомпьютеров...

— Да, два доклада. Что мы из них поняли? Что есть некоторый прогресс в понимании возможностей применения импортных чипов для построения отечественных суперкомпьютеров. Всё-таки ещё пока импортных. Безусловно, есть надежда на чипы «Эльбруса», но там ещё не все технологические проблемы решены. В общем, дело движется, но приходится констатировать, что число суперкомпьютеров и решаемых на них задач у нас (по сравнению с другими ведущими странами) крайне мало. То есть, меньше на порядки. Это, конечно, печально, потому что когда-то мы были второй державой по суперкомпьютерам в мире. И это — результат нашего отставания в первую очередь в элементной базе.

— Александр Павлович, скажите, пожалуйста, своё мнение по поводу импортозамещения на сегодняшний день. Какие главные проблемы в этой сфере?

— Главная проблема импортозамещения состоит в отсутствии технического квалифицированного единого руководства этой отрасли. Не выделены основные направления, решающие первоочередные задачи импортозамещения. Пока что всё размазывается тонким слоем по огромной площади. И даже программа «Цифровая экономика РФ» составлена таким образом, что финансирование ведётся по принципу «всем сестрам по серьгам» — всем понемногу, тонким слоем, так сказать.

Если, конечно, считать цифровизацию регионов главной проблемой импортозамещения, то тогда это и есть импортозамещение, но какое-то странное, при котором цифровизация осуществляется на импортном оборудовании.

— А как, по-вашему, надо?

— А надо выделить основные, наиболее острые задачи. Ведь для чего оно — импортозамещение? В первую очередь для информационной безопасности. А какие проблемы информационной безопасности сейчас самые острые? Самая острая — это возможность выключения интернета, учитывая то положение, которое он занял в жизни общества, страны. И этот интернет может быть выключен, и не надо питать по этому поводу иллюзий. Он может быть выключен в результате того, что чипы, которые там используются, плохо сертифицированы, допускаются разные ошибки, уязвимости... И когда эти ошибки-уязвимости найдут, то возьмут и выключат. Все думают, что если выключат, то сразу во всём мире — ничего подобного. Могут и сегментарно, уж я не говорю о происках, так сказать, недоброжелателей.

И никто такую проблему не хочет понимать. Все думают, что отключение интернета — это отключение Яндекса. Ничего подобного. Интернет — это всеобщая транспортная сеть теперь, или мобильные телефоны... Телефоны отключатся мгновенно, потому что все провайдеры пользуются для связи между вышками именно интернетом, и ничем больше. И вся эта система рухнет. Потому что все сидят на изделиях а-ля Huawei, а-ля Cisco, а-ля прочее-прочее, которые сертифицированы без нас, в лучшем случае. А, может быть, и не сертифицированы вообще. Ну, по крайней мере, нами не проверены. Нам их проверять не дают, и они не аттестовываются по надлежащим уровням безопасности. И эта проблема не решается никак.

Вместо этого говорится, что будут строиться отечественные коммутаторы или маршрутизаторы. Вопрос: на каких принципах они будут строиться? Можно строить на принципах обеспечения защиты верхнего слоя управления. А это, на самом деле, ничего не даст против выключения интернета. А можно строить так, как надо строить — на принципе защиты нижнего слоя реализации соединений. Но для этого нужно разрабатывать и реализовывать свои микросхемы, так называемые айсики.

Не такая уж это непосильная задача. По некоторым оценкам, это всего два миллиарда рублей, и в течение двух лет можно получить циски, вернее построить аналоги цисок в районах 2.000–5.000-й серии. Для более мощных цисок нужны другие разработки. Но и так возможно. Где эта задача обозначена? Нигде. А она главнейшая, на самом деле.

Нужно выделять основные направления, и именно на них сосредотачивать усилия и финансы. Тогда будут и прорывы в науке, и отечественная электроника, и безопасный интернет

Недавно кто-то в Госдуме посчитал, что если интернет выключат, то потери составят 20 миллиардов рублей в день. Безумная сумма. Высочайшие риски. Вот что такое импортозамещение! Но ни в самой программе импортозамещения, ни в программе «Цифровая экономика РФ» мы такого приоритета не найдём.

В принципе, персональный компьютер можно составить из импортных компонентов, если он отвечает определённым условиям размещения. Но в данном случае, учитывая всеобщность и глобальность доступа в интернет, этого делать никак нельзя.

— А что делать?

— Без вложения средств и целенаправленной политики, выделения ответственных организаций, которые бы целевым образом осуществляли развитие и финансирование, ничего не получится. Посмотрите, как у американцев. Илон Маск, он что, на свои деньги запустил этот самый Фолькон-9? Да, он его сделал — синхронизовал работу 9 двигателей, а потом и 28 двигателей, что и является главным принципиальным новшеством. Но не на свои деньги, вернее, не только на свои. У него же госзаказ колоссальный! Он вложил туда свою сотню миллионов на сотню миллионов государственных. За точность цифр не отвечаю, но соотношение примерно такое.

Почему мы так не делаем? Надо перенимать капиталистические методы хозяйствования, методы стимулирования науки. Не просто грантами, в которых очень трудно определиться. Вот, например, как был создан знаменитый открытый ключ Диффи — Хеллмана, по сути, революционный прорыв в криптографии? Очень поучительная история, мне её рассказал Диффи лично. В Википедии вы об этом не прочитаете.

Агентство национальной безопасности поставило тупиковую на тот момент задачу. Можно ли осуществлять секретную связь, не распределяя предварительно ключей? Потому что главная проблема — предварительные ключи. И все отказывались, а Диффи и Хеллман согласились. Для нас интересны условия, на которые они согласились. Им дали на эту работу — на командировки и зарплату — на год где-то 30–50 тысяч долларов. Цифры точно уже не помню, но порядок такой. С учётом, что шёл 1975 год,

это было не мало, но и не много. По истечении года заказчик принимает работу. Если агентство посчитает, что эта работа нужна государству, то государство забирает себе все права на неё, за что выплачивает авторам миллион или два, точно не помню.

По словам Диффи, АНБ рассмотрело их работу и признало, что она выполнена, деньги потрачены правильно, но... работу у ребят агентство не возьмёт и миллионов им не даст. Зато они могут распоряжаться этим интеллектуальным продуктом по своему усмотрению.

Диффи и Хеллман не стали патентовать это дело, кому-то продавать, предлагать, они просто опубликовали статью и стали всемирно известными. Монетизировал ли Диффи эту работу? Думаю, да, учитывая, что в последний раз я беседовал с ним как с вице-президентом Sun Microsystems, где его годовая зарплата явно превышала тот самый миллион, который ему не заплатили в АНБ. Но важно не это, а то, как было организовано это изобретение, как стимулировано и мотивировано.

Совершенно необычно — не так, как у нас. У нас либо все берут, либо все не берут, а у них — вариативность. И это продуктивный метод, ведь открытый ключ Диффи и Хеллмана — это фундаментальное открытие, как ни крути.

Это я снова к тому, что нужно выделять основные направления, и именно на них сосредотачивать усилия и финансы. Тогда будут и прорывы в науке, и отечественная электроника, и безопасный интернет.

Нечего разбрасывать деньги. Конечно, фирмы, которые работают на этом рынке, хотят заработать. Но нам-то сейчас — в условиях обостряющейся внешнеполитической обстановки — нужны наиболее быстрые, наиболее эффективные результаты. Мы же видим, что обстановка, как ни крути, обостряется. Значит, надо сосредотачиваться, собирать силы в кулак.

Может ли это сделать ФАНО? Вряд ли, это юридическая организация. А я глубоко убеждён, что юрист не может управлять техническими исследованиями. Сколько бы мне ни говорили, что современный менеджер может управлять чем угодно, хоть баней, хоть тракторным заводом, я считаю, что это не так. Я убеждён, что управленец высшего звена должен быть специалистом в своей области. Не может учитель истории управлять IT-технологиями и развивать их эффективно. Хоть кол мне на голове чеши, не может! И лингвист не может руководить физическими исследованиями...

Нам говорят, что, мол, сейчас Курчатовых нет. Есть! Есть, у нас тут — на конференции были такие ребята.

ТЕХНОЛОГИЧЕСКАЯ НЕЗАВИСИМОСТЬ В ИТ

ЗАКЛАДКА ФУНДАМЕНТА¹

Обеспечение технологической независимости российских предприятий и организаций в сфере ИТ перешло из разряда дискуссий в практическую плоскость. Интерес к отечественным программным продуктам и аппаратным средствам активно проявляют не только госведомства и госкорпорации, действия которых регламентируются нормативной базой, но и организации, не подпадающие под эти требования. ТЭК, финансовые структуры, транспортная отрасль, образование, медицина и другие отрасли просчитывают риски, связанные с использованием зарубежных программно-аппаратных средств, и приступают к формированию планов по переводу ИТ-инфраструктур на отечественные суверенные технологии. Эту тенденцию отражает аналитическая статья Карла Сумманена, опубликованная в BIS Journal № 2/2019.1

Однако на поднявшейся волне интереса к отечественным технологиям нам всем — государству, заказчикам, разработчикам ПО — важно не совершить ошибку, которая повлечёт за собой многомиллионные потери. Нельзя автоматически присваивать знак качества отечественному софту просто по факту его происхождения.

Какие характеристики фирмы-разработчика и самого программного продукта могут служить гарантией его качества?

«МАЯКИ» КАЧЕСТВА

Собственный «завод» по производству ПО. Важнейший ориентир — наличие у вендора собственной инфраструктуры разработки, которая позволяет ему обеспечивать полный и долгосрочный жизненный цикл программных продуктов. Жизненный цикл включает в себя создание продукта, его систематическую модификацию в соответствии с требованиями регуляторов, появлением новых и совершенствованием существующих технологий, изменяющимися потребностями пользователей и т.п., а также обеспечение техподдержки. Собственная инфраструктура разработки обеспечивает возможность вносить в программный

продукт существенные изменения в соответствии с потребностями заказчиков, устранять уязвимости и другие ошибки.

Наличие собственной «фабрики» обеспечивает технологическую независимость программных продуктов, в состав которых включены компоненты, созданные международными проектами разработки свободного ПО. «Базальт СПО» в 2000 году создала и развивает отечественный репозиторий «Сизиф», на основе которого выпускает линейку операционных систем «Альт». Фактически, репозиторий — это «фабрика» программного обеспечения, в которой средствами производства служит инфраструктура разработки ПО (программные инструменты и аппаратная база), есть хранилище «сырья» — база программных пакетов и хранилище готовой продукции — дистрибутивов операционных систем. В роли персонала выступают как разработчики «Базальт СПО», так и сообщество разработчиков свободного ПО. Управление репозиторием осуществляет «Базальт СПО».

В репозитории есть все необходимые средства для разработки его самого и продуктов на его базе: сложные программные системы обеспечивают автоматизацию процессов разработки и целостность репозитория, контроль зависимостей хранящихся в нём программных пакетов. Основные инструменты созданы силами «Базальт СПО» (hasher, gear, геросор и др.).

Интеграция в международные проекты разработки. Сегодня ни одна компания, даже такие мировые и отечественные гиганты как Google, Facebook, Яндекс и др., не способна в одиночку справиться с разработкой крупных систем. Поэтому разработка программных продуктов на базе свободного софта стало общей практикой. За несколько последних десятилетий созданы фундаментальные наработки под свободными лицензиями — операционные системы, базы данных, библиотеки, средства разработки. Порой разработчики пользуются доступностью свободного ПО, и выводят на рынок минимально модифицированные плоды трудов международных проектов. Это экономит затраты на разработку, но не имеет ничего общего с трансфером технологий. По сути, мы усиливаем в технологическую зависимость, маскируя её под суверенность.



Алексей СМЕРНОВ
генеральный
директор
«Базальт СПО»

¹ Начало полемики в BIS Journal № 2/2019 (Карл Сумманен, «ИТ-импортозамещение в России. Пути дальнейшего совершенствования», стр. 42–49)

Для обеспечения реальной независимости российского ПО крайне важно, чтобы его разработчики были реальными участниками ключевых международных проектов разработки свободных программ. Такой подход позволяет играть не пассивную роль потребителей высоких технологий, а активную роль их производителей, занять сильную позицию в международном разделении труда. В качестве примера можно привести созданные сотрудниками «Базальт СПО» значимые патчи, включённые в международное ядро Linux (около 2 тысяч строк кода в 2018 году, в том числе и криптокомпоненты, соответствующие российским стандартам). Компания входит в тройку лидеров по обнаружению ошибок и предоставлению их исправлений в офисный пакет LibreOffice; сотрудники участвуют в международных проектах, в том числе — в проектах glibc, libssl в роли мейнтейнеров, ответственных за выпуск версий. Спектр подобного участия очень широк, и мы постоянно его расширяем, обеспечивая двунаправленный трансфер технологий.

Ориентация на стандарты. Задача формализации требований к инфраструктуре разработки, о которой упоминает в своей статье Карл Сумманен, в определённой мере уже решена российской нормативной базой. Прежде всего, ГОСТом 54593–2011 «Информационные технологии (ИТ). Свободное программное обеспечение. Общие положения», в котором, помимо определения ПО под свободными лицензиями, подробно описаны требования к инфраструктуре разработки и поддержки. Эти требования стоит взять за основу построения инфраструктуры разработки программ всех классов.

Совместимость с аппаратными платформами и прикладным ПО. Основа технологической независимости — наличие единого комплекса, состоящего из аппаратных платформ, системного ПО (в первую очередь, операционных систем) и средств разработки. Ключевым связующим звеном любого ПАК, объединяющим «железо» и софт, служат операционные системы (ОС). Крайне важно, чтобы ОС была способна работать на максимально широком спектре аппаратных платформ: на российских, и на наиболее популярных зарубежных, а также на набирающих силу открытых международных платформах. Например, в ОС «Альт» помимо традиционных архитектур Intel и AMD, поддерживаются отечественные компьютеры на процессорах Эльбрус, Байкал, YADRO, ЭЛВИС, и на перспективных зарубежных платформах Open Power, MIPS. Это позволяет заказчикам выбирать программно-аппаратные платформы, адекватные стоящим перед ними задачам.

Одновременно операционная система должна обеспечивать работу широкого прицельного спектра прикладного ПО разного назначения, причём важна не только совместимость прикладных программ с операционной системой, но и наличие целых программных комплексов, позволяющих решать определённые классы задач. Примерами таких комплексов служат стеки для создания типового рабочего места офисного сотрудника (в составе — ОС «Альт», СЭД «Дело», офисный пакет «МойОфис», система видеоконференцсвязи «ВидеоМост», пакет для поддержки корпоративных коммуникаций CommuniGate, правовая система «Гарант»), стек для сложных вычислений и решения задач аэрогидродинамики (в составе компьютеры на базе процессоров Эльбрус с ОС «Альт», СУБД PostgresPro и инженерная система FlowVision), стек для мониторинга атомных электростанций на базе ОС Альт, созданный совместно с ООО «Московский завод «Физприбор», и другие. Необходимо, чтобы вендор на регулярной основе сотрудничал с разработчиками прикладных программ по систематическому тестированию продуктов на совместимость и её обеспечению для новых версий.

Таким образом, в распоряжение заказчиков предоставляются стеки ПО, которые позволяют решать целые группы задач предприятий и организаций, формировать рабочие места определённого типа. Объединением усилий российских разработчиков программ занимается комитет по интеграции АРПП «Отечественный софт», в работе которого активное участие принимает «Базальт СПО». Надо отметить, что фактически сформировалась и постоянно растёт экосистема, включающая не только разработчиков программ и «железа», но организации, которые осуществляют внедрение, техническую поддержку и обучение.

Технологии перехода от унаследованного программного обеспечения к отечественному. ИТ-инфраструктура подавляющего большинства российских организаций сегодня построена на зарубежном ПО, но уже начался переход на российские решения. Это долгий, многоступенчатый процесс, и на время переходного периода необходимо обеспечить устойчивую, надёжную, бесконфликтную работу гетерогенной сети, одновременно включающей зарубежные и отечественные компоненты. Поэтому особую важность приобретает наличие у вендора технологий для решения этой задачи. Например, домен-контроллера SAMBA DC, способного встраиваться в систему доменов Microsoft Active Directory, постепенно заменяя её.

Единый реестр российских программ. Формальным критерием «отечественности» программного продукта, влияющим на возможность его участия в процедуре госзакупок, служит присутствие в Едином реестре российских программ. Существование реестра прописано в законе «Об информации, информационных технологиях и защите информации» и регулируется Постановлением Правительства РФ № 1236.

Реестр — это государственная информационная система, которая не только регулирует госзакупки, но и служит базой для реализации других инициатив, связанных с развитием отечественных технологий.

ПРОБЛЕМЫ РЕЕСТРА ПОРОЖДАЮТ ПРОБЛЕМЫ У ЗАКАЗЧИКА И РАЗРАБОТЧИКОВ

Реестр играет заметную, важную роль в процессах импортозамещения программного обеспечения. Но, как любая развивающаяся система, он не лишён недостатков. Первая проблема, присущая ему с момента создания, заключается в том, что при определении отечественности программ используются, в основном, экономико-правовые критерии (собственник, место регистрации фирмы, конечный бенефициар и т.д.). Эти требования совершенно не отражают компетенции разработчика ПО. Как следствие, в реестр попадают программные продукты-однодневки, в том числе представляющие собой русифицированную кальку готового продукта на основе СПО. Формально у правообладателя есть на него соответствующие права, но отсутствуют реальные компетенции и техническая возможность поддерживать и модифицировать продукт. Вряд ли такие включения в реестр можно считать обоснованными. Необходимо добавить критерии отбора ПО, напрямую связанные с компетентностью и наличием реального, а не имитированного процесса обеспечения жизненного цикла ПО. Например, от разработчиков операционных систем на базе ядра Linux можно требовать, чтобы они продемонстрировали не менее сотни патчей, принятых в основное ядро ОС. Такие компетенции можно доказать только уже сделанной работой, и именно они служат для заказчиков гарантией качества программного продукта.

В другом случае Постановление Правительства № 325 о дополнительных требованиях к офисному софту в федеральных органах решили применить ко всему реестру. Начали возникать казусные ситуации: например, офисная программа, написанная отечественным разра-

Начали возникать казусные ситуации: например, офисная программа, написанная отечественным разработчиком для отечественного процессора Байкал, не может быть включена в реестр

ботчиком для отечественного процессора Байкал, не может быть включена в реестр, так как, согласно текущим условиям, офисная программа должна работать под двумя ОС из реестра и под Windows, а версии этой зарубежной ОС для процессора Байкал не существует. И в целом, такой подход вызывает недоумение: почему № 325 ПП выдвигает требования только к отечественному офисному ПО, не предъявляя аналогичных требований к зарубежному?

Сомнения в целесообразности вызывают и попытки централизовать закупку отечественного софта. Зарубежные продукты организация имеет право приобрести самостоятельно, а для закупки отечественных необходимо пройти через сложные бюрократические процедуры (обосновывать необходимость выбранного продукта и т.п.). Намного более естественной была бы процедура закупки, которая позволяет ведомствам без ограничений покупать отечественные программы, а необходимость в зарубежном ПО — обосновывать.

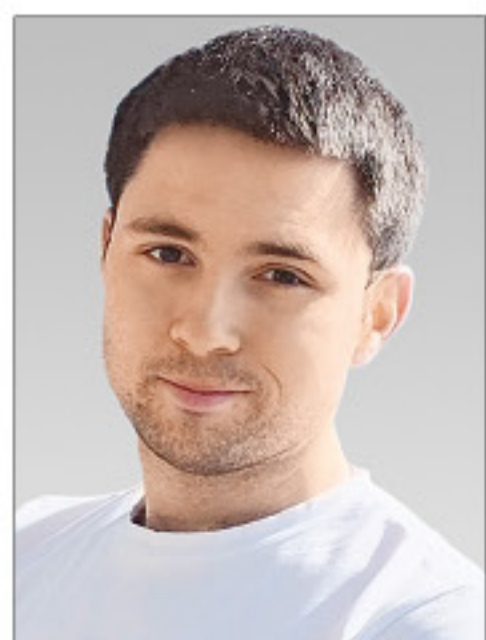
«НЕТ НИЧЕГО ВАЖНЕЕ МЕЛОЧЕЙ»

Этот девиз Шерлока Холмса стоит взять на вооружение при формировании критериев выбора отечественного программного обеспечения. Хотя ряд описанных в статье требований к выбору программных средств ещё не вошёл в нормативные документы, заказчик, которому важна надёжная и долгосрочная работа его инфраструктуры, должен самостоятельно обращать на них внимание. В России уже существует качественное ПО, которое служит полноценной альтернативой операционной системе Windows, системообразующим инфраструктурным продуктам Microsoft и разнообразному прикладному софту. Такой софт позволяет организациям и предприятиям успешно реализовывать программу импортозамещения и строить на отечественной технологической платформе качественную ИТ-инфраструктуру с длительным жизненным циклом, заменять программное и аппаратное обеспечение зарубежного производства на отечественные высокотехнологичные решения мирового уровня.

ОТЕЧЕСТВЕННАЯ КРИПТОГРАФИЯ В РУНЕТЕ



Дмитрий ГОРЕЛОВ
управляющий партнёр
компании «Актив»,
директор ассоциации
«РусКрипто»



Станислав СМЫШЛЯЕВ
директор
по информационной
безопасности
компании
«КРИПТО-ПРО»,
кандидат физико-
математических наук

Приближается тот момент, когда защищённый доступ к российским веб-ресурсам с использованием российской криптографии прекратит быть экзотикой, а изображение двуглавого орла в адресной строке браузера станет столь же привычным, как зелёный замочек. Государство и разработчики криптографических решений ведут активную работу.

ВВЕДЕНИЕ И ХРОНОЛОГИЯ СОБЫТИЙ

На конференциях РусКрипто'2018 и РусКрипто'2019 прошли круглые столы «Российская криптография в российском сегменте Интернет» и «Переход на TLS с ГОСТ: дорожные карты и реальные перспективы», посвящённые данной тематике.

Поводом для круглого стола в 2018 году стало утверждение плана мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика РФ». Он предусматривает разработку дорожной карты по переводу российского сегмента интернет на отечественную криптографию. Обсуждались как задачи информационной безопасности, требующие использования российской криптографии в TLS-соединениях, так и проблемы, решение которых необходимо для данного перехода.

Эксперт круглого стола Дмитрий Малинкин («Спутник») рассказал, что перевод сайтов госорганов на TLS с ГОСТ необходим для выполнения Поручения Президента от 16 июля 2016 года № Пр-1380 «Об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования». Дмитрий Гусев («ИнфоТеКС») отметил, что массовое применение уязвимых реализаций зарубежного SSL/TLS во множестве существующих пользовательских и бизнес-систем делает переход в них на отечественные проверенные реализации TLS с ГОСТ не просто ответом на политику импортозамещения, но и реальной необходимостью с точки зрения практической безопасности.

Руслан Гилязов (МГУ имени М.В. Ломоносова) добавил, что безопасность российских криптонаборов подтверждается и тем, что даже для столь ответственной задачи, как передача

данных, собираемых системами СОРМ, планируется защита с помощью российских алгоритмов.

Говоря о существующих препятствиях, Игорь Устинов («Криптоком») и Станислав Смышляев («КриптоПро») отметили принципиальную важность задачи регистрации идентификаторов российских криптонаборов TLS в реестре международной организации IANA (Internet Assigned Numbers Authority), управляющей идентификаторами и параметрами протоколов сети Интернет. Как отметили тогда эксперты, без наличия международно признаваемых криптонаборов существовала опасность блокировки TLS с ГОСТ из-за захвата номеров криптонаборами третьих стран, а внесение поддержки российских криптонаборов в свободном ПО было крайне затруднено.

Кроме того, Дмитрий Горелов («Актив») отметил, что в отношении клиентского и серверного ПО с поддержкой TLS с ГОСТ существует «проблема курицы и яйца»: пользователи не переходят на браузеры с поддержкой ГОСТ из-за практического отсутствия сайтов с его поддержкой, а владельцы серверов не внедряют отечественную криптографию, справедливо опасаясь слишком малого распространения поддерживающих российские алгоритмы браузеров. В связи с этим в качестве одного из итогов круглого стола был выдвинут следующий тезис: наиболее правильным путём является плавный переход на российские алгоритмы, с помощью добавления опциональной возможности подключения по ГОСТ, без запрета работы по зарубежной криптографии — однако для этого требовались сертифицированные СКЗИ для серверной стороны, поддерживающие, кроме российской криптографии, ещё и зарубежную.

ОБ ИТОГАХ ПРОШЕДШЕГО ГОДА

За прошедший год удалось успешно решить две наиболее важных задачи. 7 февраля 2019 года организация IANA зарегистрировала в своём реестре все три действующих российских криптонабора TLS и сопутствующие параметры, в соответствии со спецификациями документа «GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.2».

В части второй задачи — создания сертифицированных решений, поддерживающих зарубежные криптоалгоритмы наравне с оте-



чественными — как минимум один продукт с такими возможностями уже появился благодаря сертификации в ФСБ России решения «КриптоПро NGate».

Для пилотирования мягкого перехода на российские алгоритмы одновременная поддержка зарубежной и российской криптографии в 2018 году была внедрена и продолжает успешно использоваться на веб-ресурсах компаний, представленных сразу несколькими участниками круглого стола: RU-CENTER, КриптоПро и Спутник.

Поддержка TLS с российскими криптоалгоритмами была добавлена с сохранением возможности использования зарубежных криптонаборов TLS: при отсутствии установленного российского СКЗИ клиенты спокойно продолжают использовать эти сайты с защитой зарубежными алгоритмами, а при его наличии с помощью браузеров Internet Explorer, Edge, «Спутник» или Яндекс.Браузер имеют надёжно защищённое Г О С Т о м соединение.

В рамках проекта «Информационная безопасность» национальной программы «Цифровая экономика» планируется создание Национального удостоверяющего центра (НУЦ) для выдачи российских TLS-сертификатов. Важной целью такого центра является формирование

единого пространства доверия узлам национальной доменной зоны (.RU, .РФ), функционирующего в соответствии с российским законодательством и российскими стандартами.

ФГБУ НИИ «Восход» в 2018 году приступил к созданию Национального удостоверяющего центра и выполнил первый этап: проектирование. На 2019 год запланированы работы по созданию программно-аппаратного комплекса Национального удостоверяющего центра с последующей сертификацией и запуском в промышленную эксплуатацию в 2020 году.

По части стандартизации необходимых для развития данного направления протокольных решений за прошедший год также были существенные продвижения. Так, Росстандартом утверждён и введён с 1 февраля 2019 года в действие TLS 1.2 с новыми алгоритмами шифрования, завершается разработка российских криптонаборов TLS 1.3.

ПРОТОКОЛ TLS: КРАТКАЯ СПРАВКА

TLS (Transport Layer Security) — протокол сеансового уровня согласно модели ISO/OSI, который обеспечивает безопасность передаваемых данных в сети Интернет. Протоколы уровня приложений (HTTP, FTP, SMTP и т.д.) используют TLS для защиты передаваемой информации.

TLS реализует три компонента защиты данных: это аутентификация между клиентом и сервером, шифрование и имитозащита (обеспечение неизменности) данных.

Шифрование и имитозащита пакетов данных позволяют защитить передаваемую информацию от злоумышленников. Для шифрования используются симметричные алгоритмы, поэтому после аутентификации клиент и сервер обмениваются симметричными ключами. Для установления безопасного соединения в современных криптонаборах используются схема Диффи-Хелмана и эфемерные (одноразовые) ключи.

Использование TLS с российскими криптоалгоритмами определяется двумя документами, утверждёнными в техническом комитете № 26 по стандартизации «Криптографическая защита информации». За ТК 26 закреплены объекты стандартизации, относящиеся к методам шифрования (криптографического преобразования) информации, способам их реализации, а также методам обеспечения безопасности информационных технологий с использованием криптографического преобразования информации.

В настоящее время все основные реализации опираются на методические рекомендации МР 26.2.001–2013 «Использование наборов алгоритмов шифрования на основе ГОСТ 28147–89 для протокола безопасности транспортного уровня (TLS)», а с начала этого года начался переход на использование новых рекомендаций по стандартизации Р 1323565.1.020–2018 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)». Не вдаваясь в детали, эти документы определяют криптонаборы с российскими алгоритмами хэширования, шифрования и электронной подписи, используя их в соответствии с наиболее современными и безопасными практиками использования криптоалгоритмов. Получение в начале этого года идентификаторов в реестре IANA на описанные в двух упомянутых документах криптонаборы обеспечивает возможность полноценного использования российской криптографии в TLS наравне с зарубежной.

TLS С ГОСТ: НЕОБХОДИМАЯ ИНФРАСТРУКТУРА

Необходимым условием функционирования протокола TLS является наличие доверия к сертификату открытого ключа серверной стороны. Для этого требуется собственно наличие пространства доверия, обеспечиваемое удостоверяющими центрами.

Одним из ключевых элементов, необходимых для обеспечения применения российских

криптоалгоритмов при организации взаимодействия рядовых пользователей с информационными ресурсами в интернете, может стать НУЦ.

Единое пространство доверия предполагается обеспечить посредством создания иерархической структуры, состоящей из Национального удостоверяющего центра (корневой удостоверяющий центр, подчинённый удостоверяющий центр, портал Национального удостоверяющего центра) и подчинённых аккредитованных удостоверяющих центров, отличных от текущих аккредитованных УЦ для выдачи квалифицированных сертификатов.

Корневой удостоверяющий центр будет предназначен для организации иерархической структуры: создания корневого самоподписанного сертификата (корня доверия) и выдачи сертификатов подчинённым удостоверяющим центрам в рамках иерархии. Доверенное распространение корневого сертификата Национального удостоверяющего центра будет обеспечено за счет его включения в сертифицированные средства криптографической защиты информации, распространяемые лицензиатами ФСБ России.

Подчинённый удостоверяющий центр будет предназначен для выдачи ГОСТ-TLS-сертификатов (или траст-сертификатов) владельцам веб-ресурсов, включая органы государственной власти, органы местного самоуправления, организаторов распространения информации.

Портал НУЦ обеспечит взаимодействие с владельцами веб-ресурсов в части выдачи TLS-сертификатов и обеспечения сопровождения жизненного цикла TLS-сертификатов.

Предполагается, что аккредитованные удостоверяющие центры по выдаче TLS-сертификатов будут обеспечивать TLS-сертификатами физических и юридических лиц, не относящихся к органам государственной власти и местного самоуправления, а также к организаторам распространения информации.

Наряду с существованием самой иерархии удостоверяющих центров для стабильной работы TLS-инфраструктуры необходимо проверять статус сертификатов — не через громоздкий механизм непосредственной работы со списками отзыва, а через запрос к доверенному OCSP-серверу, возвращающему подписанные ответы о статусе любого серверного сертификата. Средства, реализующие такие протоколы, уже существуют и эксплуатируются в других проектах (для работы с так называемой «усовершенствованной электронной подписью»).

Иначе обстоят дела с механизмом, обеспечивающим повышенную защиту от поддельных серверных сертификатов, так называемым «certificate transparency». Он нацелен на решение

проблемы ошибочной выдачи сайтам сертификатов — по причине взлома или ошибки сотрудника УЦ. В рамках соответствующей рабочей группы IETF разработано решение, состоящее в формировании набора доверенных серверов с журналами (работа с которыми разрешена по принципу «только на добавление») выданных каждому конкретному имени сертификатов, а также автоматических средств отслеживания ошибочных или потенциально опасных ситуаций по данным журналам. В пилотном режиме за рубежом подобные доверенные сервера (в настоящий момент на мощностях компании Google) уже начали функционировать.

Чтобы TLS с ГОСТ мог стать по-настоящему массовым, требуется также предоставить возможность владельцам рядовых сайтов в сети Интернет быстро и просто получать ГОСТовые сертификаты на свои сайты — с помощью механизмов автоматического получения сертификатов с пониженным уровнем доверия, таких как протоколы Automatic Certificate Management Environment (ACME), описанные в RFC 8555. Создание таких механизмов уже обсуждается в профессиональном сообществе российских разработчиков средств криптографической защиты информации.

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ TLS С ГОСТ

Как оператор информационной системы может перевести свой веб-ресурс на поддержку российской криптографии? Первое, что необходимо отметить, говоря о переходе на TLS с ГОСТ: браузеры, поддерживающие российскую криптографию (Яндекс.Браузер, «Спутник», Chromium+GOST или Internet Explorer от Microsoft с установленным российским криптопровайдером), есть сейчас не у всех пользователей, а кардинально ограничивать доступ к своему ресурсу ни одна организация не захочет. Разумным видится переход веб-сервера не на исключительную поддержку ГОСТ (при котором соединение по https вовсе не поднимется, если у пользователя нет браузера с отечественной криптографией), а на решение, позволяющее одновременно поддерживать как российские криптосборы, так и зарубежные. В этом случае любой пользователь сможет успешно войти на веб-страницу: обладатели браузеров с российской криптографией получат https на TLS с ГОСТ (при этом, по желанию владельца ресурса, им можно, например, предоставлять расширенный перечень действий в личном кабинете), а соединения всех остальных, как и раньше, будут работать с использованием зарубежной криптографии.

Разумным видится переход веб-сервера не на исключительную поддержку ГОСТ, а на решение, позволяющее одновременно поддерживать как российские криптосборы, так и зарубежные

Решения, обладающие таким функционалом, уже существуют и прошли сертификацию. Они имеют ряд существенных преимуществ по сравнению с вариантом встраивания криптографических библиотек в веб-сервер. Решения устанавливаются перед веб-сервером и обеспечивают работу с шифрованным трафиком, позволяя тем самым решить две важных задачи: с веб-сервера снимается излишняя нагрузка, что весьма важно в высоконагруженных системах, и отсутствует необходимость проведения оценки влияния в части корректности вызова прикладной частью веб-сервера криптографических функций.

Кроме этого, некоторые существующие решения позволяют не только прозрачно предоставлять доступ к веб-ресурсам с ПК, планшетов и мобильных устройств, но и при необходимости разграничивать его на основе различных методов аутентификации, предоставляя различным группам пользователей доступ к разным веб-ресурсам (например, при доступе администраторов к закрытым разделам сайтов для проведения регламентных работ) в зависимости от настроек политики безопасности.

Кроме обеспечения защищенного доступа к веб-ресурсам большим плюсом для подобных решений может являться наличие функционала по предоставлению защищенного доступа к произвольным ресурсам по протоколу TLS с ГОСТ (например, для удаленного подключения по RDP к серверам и рабочим станциям со стороны сотрудников Организации), а также поддержка технологий виртуализации.

При разворачивании серверного решения нужно будет как перенести серверный TLS-ключ от ранее полученного сертификата для веб-ресурса (это, как правило, RSA с длиной ключа 2048 или 4096), так и получить ГОСТовый сертификат (оба этих сертификата будут установлены на один сервер — пользовательское ПО сможет определить, с каким из них оно готово работать навстречу). До полноценного функционирования инфраструктуры Национального удостоверяющего центра это можно сделать, обратившись в удостоверяющий центр, сертификату которого заведомо доверяют все клиентские браузеры.



Виктор СЕРДЮК
генеральный директор
АО «ДиалогНаука»



Роман ВАНЕРКЕ
технический директор
АО «ДиалогНаука»

ЦИФРОВАЯ КИБЕРРАЗВЕДКА

ПЛАТФОРМА TIP ВЫЯВЛЯЕТ И РАССЛЕДУЕТ

Сейчас уже невозможно гарантировать, что внутри корпоративной сети всё благополучно. Даже если антивирусы молчат, межсетевые экраны отражают все нападения, а система установки обновлений работает быстро и оперативно, всё равно остаётся вероятность успешных целенаправленных атак злоумышленников, которые часто используют уязвимости «нулевого дня», ворованные учётные данные и методы социальной инженерии. При этом нарушители реализуют атаку в течение длительного временного промежутка, что также существенно затрудняет её обнаружение. Злоумышленники долго изучают защитные системы объекта атаки и наносят точные и стремительные удары в наиболее уязвимые места, вследствие чего средства защиты не всегда успевают их зафиксировать. Для выявления вредоносной активности нападающих необходимо ис-

пользовать комплекс мер и инструментов, которые выявляют признаки присутствия в системе злоумышленника. Одним из таких инструментов являются специализированные платформы для управления данными киберразведки (Threat Intelligence).

БАЗА TIP

Ключевым элементом платформы цифровой киберразведки (Threat Intelligence Platform, TIP) являются индикаторы компрометации или Indicators of compromise (IoC). Это набор признаков, по которым можно идентифицировать активность злоумышленников. В качестве таких признаков могут выступать хэши вредоносных файлов, IP-адреса и домены, связанные с преступной активностью. IoC может содержать, в том числе, и регулярные выражения для выявления записей в системных журналах, которые соответствуют действиям тех или иных хакерских группировок. Понятие IoC впервые было введено ком-

панией Mandiant (сейчас является частью FireEye), которая использовала их в процессе расследования инцидентов безопасности.

Чем IoC отличается от антивирусной сигнатуры? Индикатор компрометации содержит сведения о действиях программы, а не о её коде. Это позволяет описывать не только вредоносные программы, но и потенциально опасное проведение вполне легитимных программ и даже конкретных пользователей. Как правило, индикаторы компрометации составляют производители средств защиты информации — антивирусные лаборатории, разработчики межсетевых экранов, песочниц и др. Также в качестве поставщиков IoC могут выступать центры реагирования на инциденты, например, ФинЦЕРТ или ГосСОПКА в России или US-CERT в США. В частности, US-CERT начал публиковать индикаторы компрометации для хакерских группировок, атакующих ведомственные ресурсы США, в серии документов под названием Malware Analysis Report (MAR), то есть отчёты по анализу вредоносов.

Последовательности IoC из одного источника принято называть фидами — от английского слова feed, то есть подписка на серию IoC. Среди поставщиков фидов можно выделить такие компании, как Group-IB, Palo Alto, ESET, Kaspersky Lab, FireEye. Фиды бы-

IoC содержит сведения о действиях программы, а не о её коде. Это позволяет описывать не только вредоносные программы, но и потенциально опасное проведение вполне легитимных программ и даже конкретных пользователей

вают бесплатными, как в случае с MAR, так и платными — обычно такими продажами как раз и занимаются вендоры.

Платформы киберразведки предназначены для автоматического сбора, нормализации и хранения индикаторов компрометации (фидов). В состав поставки платформы Threat Intelligence, как правило, входит и набор фидов, как платных, так и бесплатных, которые в большой мере и определяют функциональные возможности платформы.

В состав платформы TIP также может входить модуль, который собирает информацию из различных системных журналов, средств защиты и операционных систем и анализирует их на наличие индикаторов компрометации, которые содержатся в платформе. В качестве источников таких исходных данных может выступать SIEM-система, которая уже содержит все необходимые события.

Если система находит тот или иной IoC в журналах аудита, то она выдаёт рекомендации по предотвращению вредоносной деятельности и проведению расследования. Качество рекомендаций сильно зависит от источника IoC — платные фиды могут содержать инструкции для конкретных межсетевых экранов или антивирусов, в то время как с рекомендациями от бесплатных придётся разбираться самостоятельно, что потребует дополнительных расходов на зарплату соответствующего компетентного персонала.

Таким образом, платформа TIP может использоваться как для выявления новых, так и для расследования уже случившихся инцидентов. Расследование потребует анализа с помощью платформы данных истории (действий/событий), которые должны быть собраны. В качестве источника таких данных также может выступать SIEM-система. По этим данным с помощью индикаторов компрометации можно обнаружить, где и когда произошла атака, которая впоследствии привела к расследуемому инциденту. Эти сведения помогают обнаружить виновных и выяснить реальный ход событий, что и является основной целью расследования. Если корпоративная сеть является распределённой, то поиск срабатывания IoC по данным истории (действий/событий) по всем филиалам позволяет оценить качество работы службы безопасности в них.

РЫНОК TIP

Одним из пионеров рынка платформ Threat Intelligence является компания Anomali, которая выпускает свои продукты с 2013 года. Возглавляет компанию Хью Ньеманзе (Hugh Njemanze), бывший соучредитель, СТО и исполнительный вице-президент по разработке производителя SIEM-инструмента ArcSight, который в июле 2014 года занимал пост генерального директора. Собственно, рынок TIP является продолжением SIEM, которые просто собирали и обрабатывали сведения из различных средств защиты.

В портфеле компании 3 продукта:

- ♦ Anomali STAXX — бесплатная платформа, позволяющая получать фиды в открытых стандартах обмена информацией о киберугрозах;

- ♦ Anomali ThreatStream — коммерческая платформа, осуществляющая сбор индикаторов компрометации более чем из 130 возможных источников в различных форматах;

- ♦ Anomali Enterprise — корпоративная платформа проактивного поиска угроз в сети, которая способна хранить события с глубиной поиска по архиву за последние 5 лет.

При этом в STAXX интеграция может быть организована только в открытых форматах STIX (Structured Threat Information eXpression) и TAXII (Trusted Automated Exchange of Intelligence Information), а с другими источниками взаимодействие не предусмотрено. В то же время Anomali ThreatStream интегрируется с другими системами защиты и позволяет реализовать весь цикл киберразведки. Anomali Enterprise позволяет осуществлять автоматический поиск индикаторов компрометации по всему архиву событий, что особенно важно для проведения расследований по данным истории (действий/событий) крупных корпоративных сетей.

Впрочем, есть и российские продукты для цифровой киберразведки. В частности, одним из них является платформа R-Vision Threat Intelligence Platform (RTIP), которая представляет собой специализированную платформу управления данными киберразведки. Она обеспечивает автоматический сбор, нормализацию и обогащение индикаторов компрометации, передачу

обработанных данных напрямую на внутренние средства защиты, а также поиск и обнаружение индикаторов во внутренней инфраструктуре организации с помощью сенсоров.

RTIP упрощает работу с индикаторами компрометации, осуществляя непрерывный сбор, нормализацию и хранение данных из различных источников в единой базе. Продукт облегчает выявление скрытых угроз, обеспечивая автоматический мониторинг релевантных индикаторов в сторонних SIEM, записях системных журналов syslog и DNS-запросах с помощью сенсоров. Собираемые сведения позволяют вовремя блокировать угрозы и минимизировать возможный ущерб благодаря автоматической выгрузке обработанных данных напрямую на внутренние средства защиты, такие как межсетевые экраны Cisco, PaloAlto Networks, Check Point и другие.

Есть разработки и с открытыми исходными кодами, лидером среди которых является Malware Information Sharing Platform (MISP). Платформа была выпущена более 6 лет назад и собрала вокруг себя множество профессионалов по всему миру. MISP интегрируется с IRP-системой TheHive, в связке, с которой способна реализовать гибкий механизм реагирования на инциденты ИБ, обнаруженные в рамках процесса киберразведки. Среди достоинств данной TIP можно отметить поддержку всех известных и используемых форматов импорта и экспорта индикаторов компрометации, обогащение и классификацию инцидентов, а также ежемесячные обновления и поддержку разработчиков.

Платформы киберразведки TIP в перспективе могут стать неотъемлемой частью ситуационных центров по информационной безопасности (SOC). Хотя платформа TIP сама по себе и не является средством защиты, но она позволяет оперативно обнаружить признаки начавшейся атаки и оперативно на неё среагировать. Кроме этого, платформа киберразведки может использоваться как эффективный инструмент для расследования инцидентов информационной безопасности.



Антон ТИХОНОВ
технический
менеджер ГК MONT

УВИДЕТЬ НЕВИДИМОЕ

КАК ЗАЩИТИТЬСЯ ОТ БЕСФАЙЛОВЫХ УГРОЗ

Восприятию мира мы полагаемся на зрение, а когда есть нечто, чего мы не видим, подключаются дополнительные органы чувств. Но что делать, когда мы не можем определить объект, опираясь на базовые чувства или если он намеренно маскируется для прохождения «под» органами чувств? Использование стелс-технологий в современном мире — явление довольно частое, в военном деле принята специальная терминология: Low-observation characteristics (LOC), техники снижения видимости личного состава, бронетехники, техники, ракетносителей, спутников для специальных средств обнаружения.

В сфере информационных технологий тоже нашлось место подобным техникам: это различные методы запутывания вредоносного кода с целью маскировки его от средств обнаружения,

различные методы туннелирования, использование т.н. эксплоитов — программных компонентов, позволяющих использовать известные или ещё не известные (0-day) уязвимости ОС и другого ПО на атакуемой системе, бесфайловые атаки — метод проведения атаки с помощью кода, располагающегося исключительно в оперативной памяти системы и использующей легитимные/доверенные инструменты для инициации и проведения злонамеренных действий. Хочется чуть подробнее остановиться именно на этом типе вредоносных техник и подробнее разобрать саму терминологию и протекание типовой атаки.

РЕЗОНАНСНЫЕ АТАКИ 2017\2018

Gold dragon — атака на ряд организаций, участвовавших в подготовке ОИ в Пхёнчхане. Атака распространялась через фишинговую рассылку и сохра-

нялась при помощи PS (powershell) implant «Gold dragon». Изначальной целью был сбор информации о скомпрометированных системах, с отправкой полученных данных в зашифрованном виде в командный центр. После исполнения начального PS скрипта он постоянно загружал полезную нагрузку, состоящую из различных PS скриптов, которые можно было использовать для будущих атак. Сама по себе атака довольно устойчивая, т.к. позволяла детектировать наличие средств борьбы с вредоносными объектами и могла их устранить.

Emotet banking trojan — атака, нацеленная на финансовый сектор. Всё также распространялась через массированные фишинг-рассылки, где с помощью социальной инженерии пользователя принуждали открыть прикрепленный Word документ и включить макро-контент. Само собой, после этого включения происходила загрузка PS скрипта, который, в свою очередь, догружал различную вредоносную полезную нагрузку, в качестве которой в разное время выступали различные виды вымогателей-шифровальщиков, банковские трояны Dridex, Trickbot, Pinkslipbot и др.

В целом направление развития данного типа угроз уже сейчас заметно и чаще всего в СМИ можно увидеть

Бесфайловые атаки — метод проведения атаки с помощью кода, располагающегося исключительно в оперативной памяти системы и использующей легитимные/доверенные инструменты для инициации и проведения злонамеренных действий

использование термина Fileless Malware или бесфайловый зловред. Но верен ли этот термин, ведь в отличие от первых зловредов данного типа, которые если и использовали техники восстановления себя в атакуемых системах, то сводились к тому, чтобы подвергнуть атаке уязвимую систему повторно, а современные угрозы используют более «приземлённые» методы: ключи в реестре, задачи в планировщике для перехода к следующему этапу атаки, программное обеспечение для сбора информации о системе. Всё это оставляет следы на жёстком диске системы, ввиду чего назвать бесфайловыми данные угрозы уже нельзя. В сети можно найти ещё несколько именовании для данных зловредных объектов:

- ♦ Bodiless — Сергей Голованов @kaspersky (<https://securelist.com/a-unique-bodiless-bot-attacks-news-site-visitors-3/32383/>)

- ♦ Non-malware attacks — Michael Visuso @carbonblack (<https://www.carbonblack.com/2017/02/10/non-malware-fileless-attack/>)

Хотелось бы отметить, что второй термин — non-malware attacks — очень близок к истине, т.к. данные угрозы используют легитимные инструменты Windows, такие как WMI (windows management instrumentation), в котором можно включать полезную нагрузку в репозитории. WMI, PowerShell довольно популярный инструмент для выполнения рутинных задач мониторинга и управления достаточно большого круга ИТ-специалистов, а с распространением этого инструмента ещё и на Linux-хосты и сетевое оборудование его ценность трудно переоценить. Однако это обоюдоострый инструмент, который удобен не только системным администраторам и ИТ-специалистам, но и злоумышленникам, ввиду его массового распространения в современных системах Windows.

Однако легитимные инструменты — это только часть целой атаки, и наряду с ними в качестве полезной нагрузки могут и используются «классические» зловреды. Получается, что остановиться на термине non-malware всё же нельзя, и больше подойдёт термин Fileless Attack или бесфайловые

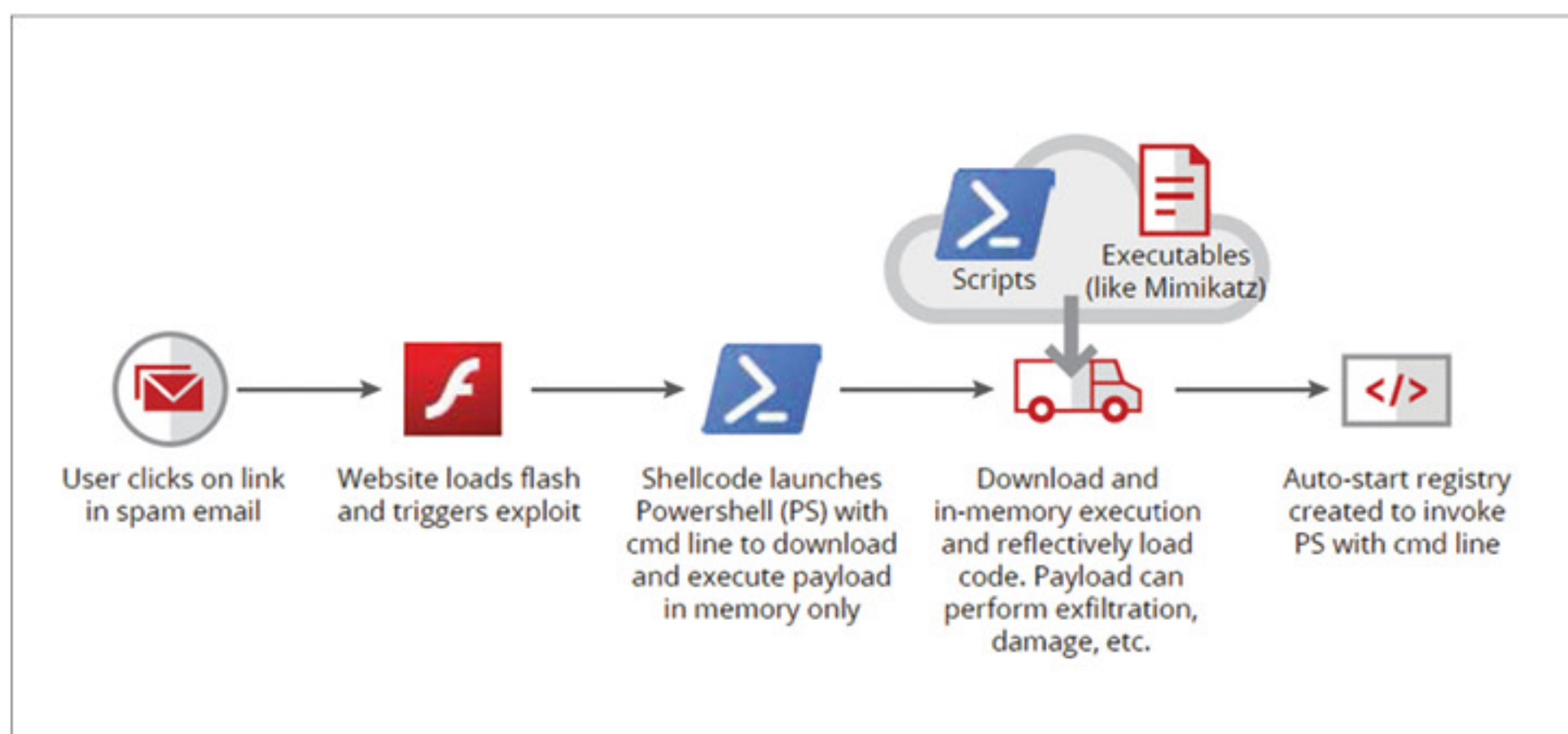


Рисунок 1. Fileless attack kill-chain

атаки (Рис. 1). Этот термин сочетает в себе и саму природу ряда техник, используемых часто для начальных этапов атаки, и более «классические» методы. Эту активность уже можно отнести к более широкому типу LOC атак, суть которых в данном контексте заключается в проведении скрытых действий с уклонением от обнаружения большинством средств безопасности и сложностью в последующем расследовании.

Как и большинство актуальных атак, для своего начала данный вид использует социальную инженерию, вынуждая пользователей щёлкнуть по ссылке или открыть вложение из полученного фишинг-письма. Довольно часто данные атаки используются для горизонтального распространения по сети компании, для сокрытия своей активности используются легитимные инструменты, которые часто включены в списки разрешённого к работе ПО (PowerShell, wscript.exe, cscript.exe) на корпоративных ПК.

Хотелось бы отметить, что в вышеописанном сценарии злоумышленнику не нужно выяснять, как проникнуть в систему, минуя барьер локальной системы защиты. Большая часть таких систем нечувствительна к исполняемым командам с использованием данных модулей. Для опытного аналитика ИБ идентификация подобных подозрительных активностей не является проблемой, но есть другая сложность — море информации, в котором нужно определить точное место поиска нужных индикаторов злонамеренной активности.

КАК ЗАЩИТИТЬСЯ?

В то время, как индустрия кибербезопасности становится всё более оперативной в устранении уязвимостей, срок жизни бесфайловых атак с каждым днём уменьшается. Самая очевидная техника по защите — поддержание актуального состояния, используемого ПО, использование пакета Microsoft Office 365, который включает продвинутые защитные техники. Компания Microsoft потратила много усилий для развития своего движка безопасности Windows Defender, предоставив ему возможность определения подозрительных нетипичных активностей в системе с использованием PowerShell.

Ключом к успешному противодействию атакам без файлов является комплексный подход, охватывающий весь жизненный цикл угрозы. Обладая многоуровневой защитой, вы получаете преимущество над злоумышленниками, имея возможность исследовать каждый этап злонамеренной кампании до, во время и после атаки.

Особенно важны две вещи:

- ♦ Возможность видеть и оценивать происходящее: обнаруживать методы, используемые атакой, отслеживать действия с использованием инструментов управления, как например, PowerShell или любых других языков автоматизации, иметь доступ к общему потоку данных по текущим атакам, потенциальным угрозам и действиям пользователей.

- ♦ Возможность контроля состояния целевой системы: остановка произвольных процессов, восстановление процессов, являющихся частью атаки, и изоляция заражённых устройств.

MSAFEE ПРЕДЛАГАЕТ РАСШИРЕННУЮ ЗАЩИТУ ДЛЯ САМЫХ СЛОЖНЫХ АТАК

McAfee предоставляет решения безопасности, которые защищают данные и предотвращают угрозы от конечной точки до облачных инфраструктур (device to cloud), используя открытый, проактивный и интеллектуальный подход. Последняя версия McAfee Endpoint Security объединяет модули предотвращения угроз, веб-защиты и хостовый МСЭ, модуль, использующий технологию машинного обучения для проведения поведенческого анализа ПО (Real Protect) и предотвращения вредоносной активности, а также модуль динамической изоляции и устранения угроз (Dynamic Application Containment), чтобы остановить распространение как классических, так и бесфайловых атак.

McAfee помогает клиентам строить гибкую архитектуру безопасности, которая оборудована для защиты от бесфайловых атак и включает в себя:

- ♦ Укрепление конечных точек (endpoint hardening): поскольку бесфайловые атаки направлены непосредственно на конечные точки, важно иметь продвинутое решение для их защиты, такое как McAfee Endpoint Security, которое обеспечивает контроль и оценку уязвимостей, защиту от эксплойтов, защиту памяти, хостовый МСЭ и контроль Web-доступа.

- ♦ Машинное обучение: McAfee применяет аналитические решения в области безопасности, использующие передовые, адаптивные и самые современные методы машинного обучения, глубокого обучения и искусственного интеллекта.

- ♦ Контроль приложений: McAfee Application Control — это решение для составления и контроля белого списка, позволяющее блокировать неавторизованный запуск приложений и кода на серверах, настольных компьютерах и других устройствах, не входящих в этот список.

- ♦ Мониторинг поведения. Понимание аналитики поведения пользователей (UBA) помогает идентифицировать угрозы, скрытые в ваших данных, что позволяет повысить точность команды мониторинга и реагирования

на инциденты ИБ и сократить время, требуемое на проведение расследований. Вместо того, чтобы фокусироваться исключительно на пользователях или объектах, McAfee Enterprise Security Manager использует комбинацию обнаружения аномалий и настраиваемых правил вместе с другими интеллектуальными и продвинутыми корреляционными моделями.

- ♦ Интерактивный поиск угроз: McAfee Active Response предлагает инструмент обнаружения и реагирования (EDR), который проводит автоматический поиск и расследования нетипичного поведения на конечных точках, а также позволяет находить источники бесфайловых атак.

- ♦ Централизованное управление с одной консолью: McAfee ePolicy Orchestrator оптимизирует управление безопасностью с помощью единой платформы управления за решениями для защиты конечных точек, которая обеспечивает контроль, систему отчётности, наглядные панели мониторинга и наглядность управления системами в масштабах от сотен до десятков тысяч узлов.

- ♦ Интеграция с партнёрскими технологиями: McAfee Security Innovation Alliance (SIA) облегчает интеграцию с решениями других производителей, даже с теми, кто производит конкурирующие решения, ведь чем шире и скоординированней ваша экосистема безопасности в целом, тем выше способность противостоять бесфайловым атакам.

ХОТИТЕ ЗАЩИТИТЬСЯ ОТ ОПРЕДЕЛЁННЫХ ТИПОВ БЕСФАЙЛОВЫХ УГРОЗ?

Группы по исследованию угроз McAfee включают более 500 специалистов по компьютерной криминалистике по всему миру, которые анализируют подозрительные объекты и поведение на наличие вредоносных угроз и разрабатывают инструменты, позволяющие блокировать различные варианты бесфайловых атак. McAfee выпустила несколько сигнатур, блокирующих различные варианты бесфайловых атак:

- ♦ **Fileless threat: Reflective self injection**

Reflective loading refers to loading a portable executable (PE) from memory rather than from disk. A crafted function/script

can reflectively load portable executable without getting registered as a loaded module in the process and hence can perform actions without leaving footprints. PowerShell is one of the most widely used applications to execute these crafted scripts.

События данного типа указывают на факт использования PowerShell как компонента, использовавшегося для запуска бесфайловой атаки через внедрение PE в сам процесс PowerShell.

- ♦ **Fileless threat: Reflective EXE self**

Reflective loading refers to loading a PE from memory rather than from disk. A crafted function/script can reflectively load an executable (EXE) without getting registered as a loaded module in the process and hence can perform actions without leaving footprints. PowerShell is one of the most widely used applications to execute these crafted scripts.

События данного типа указывают на бесфайловую атаку, когда сценарий PowerShell пытается внедрить EXE-файл в сам процесс PowerShell.

- ♦ **Fileless threat: Reflective DLL remote injection**

Reflective loading refers to loading a PE from memory rather than from disk. A crafted function/script can reflectively load a DLL without getting registered as a loaded module in the process and hence can perform actions without leaving footprints. PowerShell is one of the most widely used applications to execute these crafted scripts.

События данного типа указывают на бесфайловую атаку с использованием сценария PowerShell для внедрения DLL в удалённый процесс.

- ♦ **Fileless threat: Malicious code execution using DotNetToJScript technique**

Это событие указывает на попытку выполнить вредоносный шелл-код, используя технику DotNetToJScript, которая используется распространёнными бесфайловыми атаками, такими как CACTUSTORCH. Векторы атаки DotNetToJScript позволяют загружать и выполнять вредоносную сборку.NET (DLL, EXE и т.д.) прямо из памяти с помощью библиотек.NET, предоставляемых через COM. Как и любой другой метод бесфайловой атаки, DotNetToJScript не помещает какую-либо часть библиотеки.NET, DLL или EXE на жёсткий диск компьютера.



**Дмитрий
НОВИКОВ**
генеральный
директор компании
ITP Services
(ГК «Инфозащита»)

НАШ БИЗНЕС — ПРЕДОСТАВЛЕНИЕ ЭФФЕКТИВНЫХ СЕРВИСОВ ДЛЯ ПРОТИВОСТОЯНИЯ КИБЕРУГРОЗАМ

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР КОМПАНИИ
ITP SERVICES (ГК «ИНФОЗАЩИТА»)

ДМИТРИЙ НОВИКОВ О СИТУАЦИИ В СЕГМЕНТЕ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

— С чем связаны структурные изменения в группе компаний «Инфозащита»?

— Внутренняя реструктуризация является логичным ответом на вызовы рынка, который требует от компаний, работающих в сегменте информационной безопасности, высоких показателей гибкости и управляемости. Мы провели ряд изменений, в том числе ребрендинг, в результате которых наша структура стала лучше соответствовать решаемым задачам. Основная задача осталась прежней — защита информационных систем корпоративных клиентов, — но за более чем десять лет, которые мы присутствуем на рынке, произошли значительные изменения в угрозах, бизнесах, законодательной базе, техническом оснащении и других компонентах. Компания ITP Services — это сервисная компания, создание которой нацелено на расширение и повышения качества услуг, оказываемых нашим клиентам.

— Новая сервисная компания открыта в этом году?

— Де-юре — да. Де-факто компания уже существовала в течение нескольких лет, но её направленность отличалась от текущей. Сейчас это команда квалифицированных специалистов по информационной безопасности, которая в сотрудничестве с поставщиками решений предоставляет услуги корпоративным клиентам и государственным структурам. Образно говоря, сейчас мы выполнили перестроение, что позволит нам стать более эффективными в работе с нашими клиентами.

— На что нацелен бизнес компании?

— Наш бизнес — предоставление эффективных сервисов для противостояния киберугрозам, которые могут создавать проблемы нашим клиентам. Мы, как я уже отмечал, занимаемся этим уже более десяти лет, придерживаясь концепции «безопасность как сервис».

— Планируете ли вы какие-то необычные проекты?

— Каждый проект по-своему необычен. Наши клиенты — компании среднего и крупного размера, работающие в разных сегментах экономики страны: телекоммуникации, нефть и газ, промышленность, банки и финансы, страхование, розничная торговля, ИТ, образование и т.д. В каждом сегменте есть свои особенности, информационная инфраструктура заказчика зависит не только от размеров его бизнеса, но и от размещения офисов, используемого прикладного и системного программного обеспечения и множества других факторов.

Также хочется отметить, что любой бизнес трансформируется, соответственно изменения будут происходить и в инфосистеме, что потребует пересмотра решений по безопасности. Изменяется также и киберпреступность: злоумышленники — люди изобретательные, их «аппетиты» растут, пропорционально увеличивается сложность и масштаб кибератак.

— Каковы планы компании на ближайшее будущее?

Развивать бизнес. Теперь, когда мы закончили реструктуризацию, можем направить все ресурсы на привлечение

новых клиентов, на совершенствование систем защиты у уже имеющих, на построение эффективных форматов взаимодействия с нашими партнёрами и, конечно, на обучение наших специалистов. Как я уже неоднократно отмечал, киберугрозы становятся всё более разнообразными и изощрёнными, для противостояния им наши сотрудники должны постоянно повышать собственную квалификацию, а компания в целом — наращивать экспертизу.

— Что вы хотели бы пожелать своим клиентам?

— Очень серьёзного отношения к теме информационной безопасности. Киберпреступники могут атаковать компанию в любую секунду из любой точки планеты. В случае успешной атаки, образно говоря, получив прибыли на копейку, киберпреступники могут нанести убытков на рубль, а то и на много большие суммы. А если речь идёт о промышленности, то размер ущерба, который может причинить кибератака, непредсказуем и может оказаться колоссальным.

Современный бизнес должен иметь многоуровневую эшелонированную защиту, настолько сложную в преодолении для злоумышленника, чтобы взлом утратил экономический смысл. Создавать, совершенствовать и развивать такую защиту может только слаженная высокопрофессиональная команда, содержать которую внутри непрофильной компании экономически нерентабельно. Поэтому лучшее решение — приобретать безопасность как услугу. Это позволит оптимизировать затраты и при этом получить полноценную и высоконадёжную защиту информации.



Екатерина СТЕПАНОВА
ведущий консультант ДИБ
АМТ-ГРУП, кандидат
технических наук



Анастасия ПЕТЛЯКОВА
консультант ДИБ АМТ-ГРУП

КУДА? КОМУ? КАК?

В ВАШЕЙ СЕТИ¹

Регулярно в своей работе мы сталкиваемся с, казалось бы, таким простым, но таким важным процессом предоставления сетевого доступа. При незначительных масштабах компании управление доступом серьёзных проблем не вызывает, но, когда число пользователей, систем и узлов исчисляется тысячами, расширяется «зоопарк» устройств, а топология сети становится слишком запутанной, процедура настройки сетевого взаимодействия занимает значительно больше усилий и времени, чем предполагалось.

¹ Начало темы в BIS Journal № 2/2019, с. 63–65. Статья М. Ксенофонтова «Что? Где? Куда? в вашей сети».

Это может привести к ситуации, когда на момент предоставления доступа потребности в нём уже нет, что неминуемо повысит уровень недовольства конечных пользователей и вполне вероятно окажет влияние на бизнес в целом.

Осознание проблемы и стремление найти её решение приводит к пониманию необходимости автоматизации процесса. На рисунке 1 приведена упрощённая модель процессов предоставления услуг, связанных с управлением сетевым доступом.

В настоящий момент на рынке представлено несколько решений, позволяющих автоматизировать процесс управления сетевым доступом. С некоторыми

сценариями использования систем данного класса можно ознакомиться в статье М. Ксенофонтова «Что? Где? Куда? в вашей сети» (BIS Journal № 2/2019).

Стоит отметить, что, как и в любом проекте по внедрению программного продукта, путь от идеи до успешного функционирования достаточно долг и тернист. Все прекрасно знают, какие стадии проходит такой проект:

- ♦ предпроектное обследование и актуализация процессов;
- ♦ составление технического задания;
- ♦ внедрение системы и её сопровождение.

Однако специфика проекта по внедрению систем управления доступом такова, что нельзя недооценивать важность первого этапа: после изучения особенностей бизнес-процессов компании и проведения интервью с ключевыми сотрудниками заказчика необходимо выявить области для улучшения или формализации, а также идентифицировать справочники (например, CMDB) и правила, которыми руководствуются исполнители, и смежные процессы, в рамках которых предъявляются требования к рассматриваемому. Это позволит быть уверенным, что на выходе будет получен не стихийный процесс или автоматизированный хаос, а гибкое и качественное решение. Схема актуализации приведена на рисунке 2.

К примеру, если рассматривать процесс управления сетевым доступом более детально, то недостаточная проработка на одном из начальных этапов — этапе оценки допустимости запроса и опасности маршрута прохождения трафика с учётом действующих



Рисунок 1. Укрупнённая модель процессов предоставления услуг, связанных с управлением сетевым доступом



Рисунок 2. Актуализация процесса управления сетевым доступом

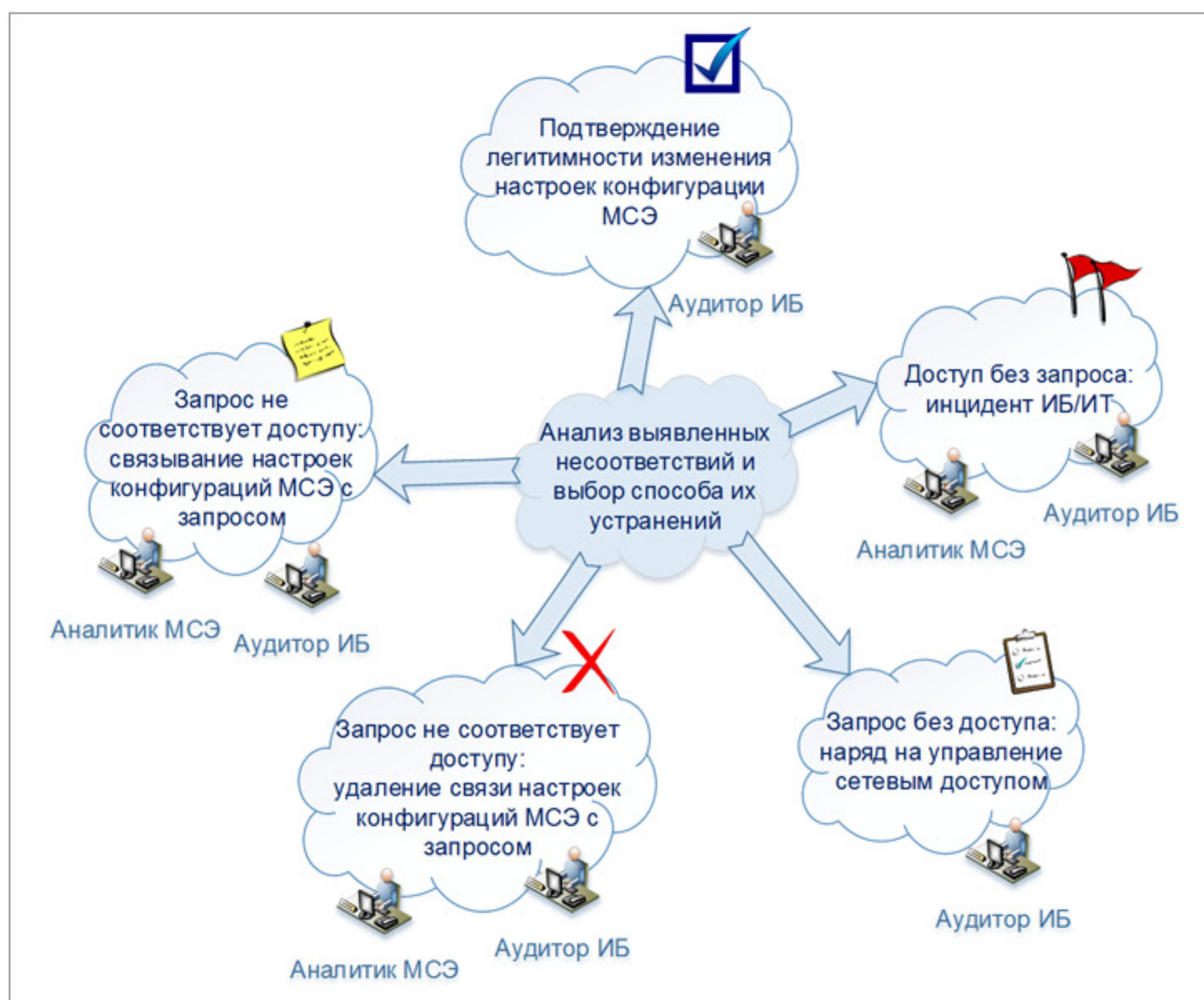


Рисунок 3. Устранение несоответствий фактических настроек и базы запросов на изменение

в компании правил информационного взаимодействия сетевых сегментов и «лучших практик» — может привести к снижению уровня защищённости сети в целом, в то время как качественный анализ требует методической базы, учёта большого числа параметров и, соответственно, может привести к задержке в предоставлении услуги.

К тому же, ввиду того, что предоставление доступа находится на стыке информационной безопасности (ИБ) и информационных технологий (ИТ), возникает необходимость разграничения ответственности между исполнителями, определения их функциональности и закрепления её в инструкциях

для каждой бизнес-роли рассматриваемого процесса.

Что же даёт актуализация процесса управления сетевым доступом?

- ♦ понимание сфер ответственности исполнителей;
- ♦ структурированность и порядок в предоставлении сетевого доступа;
- ♦ обеспечение прозрачности процесса и высокой скорости настройки сетевого доступа;
- ♦ снижение рутинной нагрузки на специалистов.

После того, как процесс отлажен и автоматизирован, чётко регламентировано, чем руководствоваться исполнителю, трудностей не возникает — мини-

мизируется вероятность и количество ошибок и уязвимостей, а также появляется возможность, а главное — ресурсы для реализации процедур, повышающих безопасность и надёжность сети, внедрение которых ранее было невозможно из-за трудоёмкости ручного сбора и анализа данных для обработки запроса на сетевой доступ.

Другим примером функции, которую позволяют осуществлять детальная проработка процесса предоставления доступа и применение систем управления доступом, является функция контроля сетевых доступов с точки зрения их избыточности и несоответствия бизнес-процессам компании — аудит настроек межсетевых экранов (МСЭ).

На рисунке 3 схематично изображена процедура устранения несоответствий в ходе проверки легитимности внесённых изменений в настройки МСЭ.

Проведение регулярного аудита вручную затруднительно ввиду ограниченности человеческих ресурсов, ведь аудитор ИБ необходимо сопоставлять изменения конфигураций МСЭ и базы запросов на изменение. С другой стороны, важность проведения систематических проверок заключается в том, что процессы контроля способствуют повышению уровня безопасности компании. И только внедрив соответствующее потребностям средство автоматизации, будь то AlgoSec, Tufin или Skybox, можно системно и качественно решить задачу аудита сетевого доступа.

Подробное описание данного процесса, подготовка методики устранения несоответствий, разграничение зон ответственности позволяют работать качественно, быстро и безопасно.

Таким образом, для полноценного функционирования систем управления сетевым доступом их внедрение должно сопровождаться интеграцией в другие системы компании не только в технической части, но и в процессной. Такой комплексный подход позволит реализовать гибкие сценарии работы и более зрело решать возникающие проблемы, снизит нагрузку на ИТ- и ИБ-специалистов компании и даст прогнозируемые сроки для решения задач, а также уверенность в успешном результате проекта.



**Дмитрий
КАНДЫБОВИЧ**
генеральный
директор компании
StaffCorp (ООО «Атом
Безопасность»)

СИСТЕМА ОСОБОГО НАЗНАЧЕНИЯ

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ
ГОСТ Р 57580.1-2017 С ПОМОЩЬЮ
ПРОГРАММНОГО КОМПЛЕКСА STAFFCORP

Один из залогов благополучия банка в долгосрочной перспективе — это комплаенс, то есть соответствие требованиям законодательства. Ожидается, что в 2020 году выполнение ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» станет обязательным для банков. Как можно подготовиться к этому событию?

ИСТОЧНИК РИСКА

ГОСТ предписывает ряд процессов, цель которых — стандартизировать защиту информации в финансовых организациях. Этот нормативный документ предусматривает организационные, технические и программные меры, с помощью которых будут защищены все информационные аспекты банковской деятельности. Остановимся на блоке требований к системе защиты.

Источник рисков внутренней информационной безопасности — в первую очередь сотрудники, так как они непосредственно имеют доступ к информационным активам и персональным данным. Разнообразные риски, связанные с сотрудниками (ошибки, недобросовестное выполнение обязанностей, злоупотребления и противоправные действия), с некоторых пор преобладают в статистике, и эффективная борьба с ними возможна только комплексными мерами.

STAFFCORP ПОЗВОЛЯЕТ...

Для соответствия банка требованиям ГОСТ Р 57580.1-2017 в области вну-

тренней информационной безопасности используется программный комплекс StaffCorp Enterprise, обеспечивающий мониторинг действий пользователей и событий внутренней информационной системы финансовой организации. Система StaffCorp позволяет контролировать движение информации в организации и за ее пределы, фиксировать события информационной безопасности, расследовать инциденты и вести учет рабочего времени сотрудников.

КОНТРОЛЬ ДОСТУПА

В частности, контроль доступа осуществляется несколькими способами. Во-первых, StaffCorp дополняет штатную СКУД, отслеживая использование учетных записей уволенных сотрудников или сотрудников, находящихся на больничном, в командировке или в отпуске. Во-вторых, на особо ответственных рабочих местах можно процесс внесения логина и пароля сопровождать снимками веб-камер, что позволит видеть, кто именно набирал учетные данные. В-третьих, система может дать сигнал в случае подбора пароля. И, наконец, удаленное подключение к любому рабочему столу даст возможность перехватить управление в случае некорректных или опасных действий сотрудника и заблокировать учетную запись до выяснения обстоятельств дела.

СЕТЕВОЙ КОНТРОЛЬ

Модуль сетевого контроля StaffCorp позволяет полностью контролировать выход сотрудников в сеть, сайты, к которым они обращаются, время, проведенное на них, отправку почты с почтовых серверов, сохранение информации в обла-

ко, переписку в мессенджерах. Имеется возможность сформировать «белые» и «черные» списки сайтов и осуществлять блокировку в соответствии с ними. Также система позволяет маркировать сайты как продуктивные, непродуктивные и нейтральные, что позволяет контролировать использование сотрудниками рабочего времени.

КОНТРОЛЬ ПО НАСТРОЙКАМ

StaffCorp позволяет контролировать защищенность организации в соответствии с настройками политики безопасности и сигнализировать в случаях возникновения угроз: пересечения важным документом контура безопасности, появления в переписке слов из сигнального списка, запись больших массивов информации на USB-носитель, сигналы детектора аномалий.

Детектор аномалий — это функция, позволяющая фиксировать отклонения от среднестатистического поведения конкретного пользователя. Например, если сотрудник распечатывает обычно 50–100 документов, и вдруг распечатал 1000 — это сигнал к тому, чтобы поинтересоваться, чем именно занят сотрудник, какие документы распечатывает, не готовится ли он к увольнению или передаче информации злоумышленнику за пределами организации.

ДОПОЛНЕНИЕ К АНТИВИРУСУ

StaffCorp является дополнительным уровнем защиты от вредоносного кода в дополнение к антивирусу. Например, фиксируется запуск вредоносных и других программ, и можно определить список нелегитимного ПО. В StaffCorp

возможна реализация так называемой «песочницы», которая позволяет протестировать новое ПО на скрытые функции в контролируемой цифровой среде до начала эксплуатации.

ПРОТИВ УТЕЧЕК

Предотвращение утечек — одна из ключевых функций любой системы информационной безопасности. Для эффективного противодействия утечкам следует провести аудит внутренней информационной безопасности, чтобы понимать, какие каналы утечек характерны для вашей организации. Система StaffCop позволяет провести аудит своими силами уже в рамках бесплатного тестового периода.

После того как наиболее актуальные каналы утечек обнаружены, создаются внутренние регламентирующие документы, в которых фиксируются политики безопасности. В соответствии с ними настраивается конфигурация агентов StaffCop. Предотвращение утечек возможно несколькими способами: блокировкой каналов (например, съемных носителей,

сайтов, использования онлайн-почты) и блокировкой файлов по меткам. Второй способ реализуется таким образом: на особо важную информацию устанавливается цифровая метка, которая позволяет производить с файлами только разрешенные действия разрешенным пользователям. Можно ограничить использование файла только определенными приложениями и пользователями.

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

Программный комплекс StaffCop позволяет осуществлять качественное управление инцидентами. Во-первых, осуществляется полный контроль действий пользователей, особенно из группы риска, так, что любое действие можно рассмотреть в контексте, на основе чего можно делать выводы о сути инцидента. Во-вторых, аналитические инструменты позволяют выгрузить информацию в максимально наглядном виде.

И ПРОЧИЕ ПРЕЛЕСТИ

Для удобной и быстрой работы с отчетами в системе StaffCop используются

базы данных PostgreSQL и ClickHouse, а также технология многомерных OLAP-кубов, позволяющая структурировать большие массивы данных по многомерному принципу. Следует отметить, что в системе не используются программные продукты, требующие постоянных оплат лицензий и увеличивающие стоимость владения. StaffCop Enterprise реализован в логике импортозамещения и имеет крайне умеренные требования к базовому оборудованию.

Программный комплекс StaffCop Enterprise включен в единый реестр российских программ Минсвязи РФ за № 3337. Проходит сертификацию ФСТЭК на отсутствие НДВ по 4 уровню контроля и соответствию НПА по съемным машинным носителям информации по 4 классу защиты. По итогам 2010 и 2016 года StaffCop стал лучшим решением по мониторингу сотрудников по версии журнала PC Magazine / Russian Edition, по итогам 2017-го вошел в ТОП-8 программных решений контроля сотрудников в мире (по версии PCMag.com).



Программный комплекс для контроля информации, действий сотрудников и событий системы на ПК

МОНИТОРИНГ. АНАЛИЗ.
ОПОВЕЩЕНИЕ. БЛОКИРОВКА





Выявление инсайдеров, кардеров и нелояльных сотрудников



Контроль информационных потоков внутри банка



Централизованный контроль филиальных сетей



Полный контроль действий сотрудников за компьютерами



Учет рабочего времени и удаленное администрирование



Подробнее для банков и финансового сектора

✓

Мощная аналитика!

✓

Скорость работы на больших данных

✓

Низкая стоимость внедрения и эксплуатации



Единый реестр российских программ Минсвязи РФ №3337

Попробуйте бесплатно!

Подробная информация: www.staffcop.ru / +7 (499) 653-71-52

СТСРЮПТ 2019

VIII СИМПОЗИУМ «СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В КРИПТОГРАФИИ» ЗАВЕРШИЛСЯ ЗАХВАТЫВАЮЩИМ КРИПТОГРАФИЧЕСКИМ КВЕСТОМ

В Светлогорске Калининградской области 4–7 июня состоялся VIII симпозиум «Современные тенденции в криптографии» (СТСрЮпт'19), участие в котором приняли более 140 исследователей в области криптографии из 7 стран мира. Организаторами симпозиума выступили Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), Академия криптографии РФ и Математический институт им. В.А. Стеклова РАН.

Симпозиум СТСрЮпт проводится в сотрудничестве с Международной ассоциацией криптологических исследований (IACR) и при поддержке Фонда содействия развитию безопасных информационных технологий (ФСРБИТ). Организационную поддержку мероприятию оказала Медиа Группа «Авангард».

СТСрЮпт 2019 стал весьма показательным международным научным событием в России, посвященным те-

оретическим и практическим аспектам криптографии. Для участия в научной программе симпозиума было представлено 37 работ, что почти в два раза больше, чем в прошлом году. Возросшее число докладов свидетельствует о понимании научным сообществом важности вопросов обеспечения информационной безопасности, в том числе, в контексте взятого руководством страны курса на цифровизацию всех сфер жизни и деятельности в государстве.

Отбор рецензентов прошли 22 доклада. Их тематика оказалась очень обширной. Особенный интерес вызвали вопросы синтеза и анализа как классических блочных и поточных криптографических алгоритмов, так и широко обсуждаемых в последнее время постквантовых криптографических механизмов, способных противостоять криптографическим атакам с использованием квантовых вычислителей.

Отличительной чертой симпозиума СТСрЮпт является включение в научную программу приглашенных докладов ведущих отечественных и зарубежных специалистов. В этом году таких докладов было три. Первый подготовили Андрей Пичкур и Алексей Тарасов, посвятив его памяти действительного члена Академии криптографии Российской Федерации, профессора Михаила Михайловича Глухова — одного из основателей российской алгебраической криптографической школы. Второй доклад прочитал ведущий специалист в области постквантовой криптографии на основе эллиптических кривых Лука де Фео, и третий, посвященный новой версии протокола TLS, — профессор Швейцарской высшей технической школы Цюриха Кеннет Патерсон.

В рамках симпозиума также проходили два круглых стола. Первый был посвящен впервые создаваемому в Рос-



Андрей Пичкур, председатель ФУМО ИБ



Андрей Зубков (МИАН), Игорь Качалин, Дмитрий Матюхин (ТК 26)

сии музеем криптографии, а второй — деятельности лаборатории проблем стандартизации в области криптографии и безопасности информационных технологий, созданной в Академии криптографии РФ в рамках национальной программы «Цифровая экономика РФ».

Также во время симпозиума был проведён своего рода эксперимент. Впервые научную программу дополнили популярными лекциями по криптографии для специалистов в области защиты информации и школьников старших классов. В первом случае в роли лекторов выступили ведущие специалисты компаний-разработчиков средств криптографической защиты и эксперты технического комитета по стандартизации ТК 26 «Криптографическая защита информации». Соответственно были сформулированы и темы лекций: «Всё, что вы хотели знать про TLS, IPsec и CMS, но стеснялись спросить», «Что плохого можно сделать, неправильно используя криптоалгоритмы», «Блокчейн — трезвый взгляд, реальные применения и текущие проблемы», «Постквантовая криптография: вызов брошен» и др.

А для калининградских школьников при поддержке ФСРБИТ преподаватели ведущего вуза страны, осуществляющего подготовку специалистов-криптографов, устроили увлекательные выездные занятия, завершившиеся захватывающим криптографическим квестом.

Генеральным партнёром СТСгрупп 2019 стала компания «ИнфоТеКС», официальным партнёром — ООО «КРИПТОПРО». Партнёрами симпозиума выступили компании «Код Безопасности» и «Актив».

Широкий перечень рассмотренных вопросов, глубина научной проработки проблем и высокий профессионализм участников подтвердили статус симпозиума СТСгрупп как ведущего российского научного мероприятия в области криптографии. По решению Руководящего комитета летом 2020 года состоится следующий — IX симпозиум «Современные тенденции в криптографии».



С приглашенным докладом выступил Лука де Фео (Франция)



В Симпозиуме участвовали криптографы из семи стран



Криптографический квест для калининградских школьников

SBERBANK ICC 2019

ЦИФРОВОЙ ХАОС ИЛИ «ДУРАКИ И ДОРОГИ» ЦИФРОВОЙ ЭКОНОМИКИ

В царской России, как считалось, было две беды — дураки и дороги. Бедой цифровой экономики является, похоже, цифровой хаос. Этот термин можно считать своеобразным открытием Международного конгресса по кибербезопасности. Он вошёл в название доклада руководителя службы кибербезопасности Сбербанка Сергея Лебеда и активно использовался им в выступлении.

ОСОЗНАТЬ И ПРИНЯТЬ... УЩЕРБНОСТЬ КОНТРОЛЯ

В научно-методическом контексте «цифровой хаос» — это обобщённая мера рисков управления ИТ-системой, проистекающих из осознанной ущербности контроля на основе современного подхода к управлению — риск-менеджмента, и отказа от «архаичного» управления ИТ и КИИ «по требованиям».

И первым из факторов, определяющих риски, в докладе г-на Лебеда были названы не хакеры, а сами по себе технологии и процессы их внедрения. Ока-

зывается, а нет оснований не верить руководителю службы кибербезопасности Сбербанка, инновации в ИТ или, скорее, инновации на основе ИТ, сегодня часто внедряются:

- ♦ в условиях внутреннего сопротивления персонала, не готового к инновациям;
- ♦ в условиях нехватки специалистов с квалификацией, позволяющей обслуживать новую инфраструктуру;
- ♦ в условиях, когда новая инфраструктура должна существовать в соседстве с тем оборудованием и/или приложениями, которые обозначаются иностранным словом «легаси», созданными, естественно, без учёта особенностей «инновационных» продуктов.

Ещё одним важным откровением в этом выступлении было упоминание о существовании «кирпичей» в современной ИТ-инфраструктуре. Речь о приложениях и оборудовании, которые вроде бы работают, но тонкости их функционирования остаются тайной за семью печатями как для пользователей, так и для эксплуатирующего персонала.

ИНЖЕНЕРНУЮ КУЛЬТУРУ — НА СВАЛКУ?

Уже содержание преамбулы доклада г-на Лебеда указывает на инженерную авантюристичность нынешней ситуации с внедрением новых цифровых «технологий» на основе анализа рисков. Да и лингвистический анализ указывает на то, что хорошее дело «хаосом» не назовут.

Технологии и принципы внедрения инфраструктуры «индустрии 4.0» ломают сложившуюся и хорошо зарекомендовавшую себя инженерную культуру. В результате оказывается, что киберпокалипсис вполне достижим и без усилий лиц, обосновавшихся в «даркнете».

В ЗЕРКАЛЕ АНЕКДОТА

Краткое, но образное изложение коренных различий старой и новой культур содержится в анекдоте. Его суть в том, что при поломке автомобиля, в котором едут бизнесмен, инженер и «айтишник», лишь инженер предлагает изучить документацию и, проанализировав поломку, устранить её.

Бизнесмен же предлагает протереть зеркало заднего вида и проверить давление в шинах, а «айтишник» — выйти из машины и зайти в неё снова. И сегодня бизнесмен и «айтишник» зачастую оказываются союзниками в их стремлении к минималистичной операционной «эффективности».

В ЗЕРКАЛЕ ЖИЗНИ

Один из итогов наступления новой эры «индустрии 4.0.» — две резонансные катастрофы с «киберфизическими» боингами и ещё ряд катастроф авиатехники, менее резонансных, но с той же природой произошедшего. А природа — в точности как в докладе г-на Лебеда: технологии-«кирпичи» в современной авионике и отсутствие понимания того, какова должна быть квалификация лётного состава «киберфизических» самолётов.

И уже есть примеры активного сопротивления лётчиков пересаживанию их на «кирпичи» с крыльями.



Доклад руководителя службы кибербезопасности Сбербанка Сергея Лебеда.
Фото: icc.moscow

КТО ОТВЕТИТ? ВОТ В ЧЁМ ВОПРОС

Автоматизированный блиц-опрос, инициированный модератором самой первой панельной дискуссии на ICC 2019 показал, что 17% аудитории считает, что ответственность за обеспечение кибербезопасности лежит на государстве, 42% полагают, что за это должны отвечать поставщики услуг, а 41% возложил ответственность на пользователей.

При этом министр цифрового развития Константин Носков оказался многолик: «Как министр я выбрал первый вариант — государство, как частное лицо — третий, то есть пользователь».

Т.е. цифры, пусть и полученные «на вскидку», указывают на то, что сегодня в нашей стране отсутствует распределение ответственности — по сути организационной основы для решения проблем кибербезопасности.

В этих обстоятельствах заслуживает внимания мнение президента Совета по кибербезопасности Германии Ханса-Вильгельма Дюна, что ответственность за кибербезопасность оборудования и услуг (которая должна быть «встроенной») должны нести вендоры, а регуляторы и надзорные органы должны иметь полную информацию о тонкостях работы предлагаемого для «инду-

стрии 4.0» оборудования и приложений. И никаких «кирпичей»!

«ОЧКОВ С ПОЛДЮЖИНЫ СЕБЕ ДОСТАЛА...»

На фоне конкретики высказываний президента Совета по кибербезопасности Германии диссонансом звучат высказывания отечественных ЛПРов, в которых слышится лишь тасуемый набор терминов, но отсутствует связующая их мысль и осознание реалий жизни.

«...сквозные технологии, обладание которыми будет определять преимущества и глобальное неравенство.

«БЕЗОПАСНЫЙ МИР — БУДУЩЕЕ ИЛИ УТОПИЯ?»

ТЕЗИСЫ УЧАСТНИКОВ ПЛЕНАРНОЙ СЕССИИ

Дмитрий Медведев, Председатель Правительства РФ:

— Проблема киберпреступности входит в пятёрку глобальных рисков в рейтинге Всемирного экономического форума. Международное экспертное сообщество зачастую ставит её выше всяких других угроз, даже таких опасных и страшных, как терроризм, глобальные экологические проблемы. Потери мировой экономики от киберпреступности оцениваются в этом году в \$2,5 трлн, что сравнимо с совокупным ВВП всех африканских стран.

Необходимо выработать общемировые стандарты противодействия киберугрозам. Но одними государственными усилиями проблему киберугроз не решить. К этому процессу должны подключиться все, в том числе представители бизнеса.

Эльвира Набиуллина, председатель Центрального банка РФ:

— Руководители компаний и банков часто думают: да, меня пронесло сегодня. Я назначу человека ответственного,

который будет отвечать за кибербезопасность, и он все решит. Но я согласна с коллегами: это не техническая проблема, а проблема управления киберрисками. Мы не научились управлять киберрисками. Руководители компаний, в том числе финансового сектора, не понимают масштаб угроз.

С прошлого года Центральный банк как регулятор имеет полномочия осуществлять надзор за финансовыми институтами с точки зрения того, как они выполняют требования по кибербезопасности. В прошлом году мы проверили 58 банков, в этом году 75 и во всех были найдены проблемы, нарушения. Выявленные недостатки нельзя назвать критическими, но они могут стать серьезными, если финансовые институты не будут придавать им значение. Основные причины этого: бизнес-процессы пока не включают в себя управление киберрисками, даже если есть компетентный человек, он не сможет ничего сделать, и второе — не хватает компетентных людей. Необходимо чтобы организации обучали своих со-

трудников и встраивали в бизнес-процессы вопросы кибербезопасности.

Все действуют в конкурентной среде и часто экономят на кибербезопасности. Но защищенность от киберрисков и уровень кибербезопасности скоро станут конкурентным преимуществом компаний, потому что люди будут обращаться в те организации, где будут уверены, что там обеспечен высокий уровень кибербезопасности.

В Банке России создан новый департамент, функциями которого является, в том числе сбор информации о кибератаках. У организаций есть желание скрыть информацию об инцидентах. Руководители финансовых организаций считают, что это может подорвать доверие клиентов. Поэтому добровольный обмен информацией мы будем сочетать с надзором. Это чрезвычайно важно для защиты прав клиентов.

Герман Греф, президент, председатель правления Сбербанка:

— Когда ты начинаешь понимать, насколько сложно защитить все элемен-

Они нам хорошо известны: это искусственный интеллект, это индустрия сетей беспроводной связи, это сети связи пятого поколения, сети, которые обеспечивают работу интернета вещей...»

Кто бы объяснил, в чём видится вице-премьеру РФ Максиму Акимову разница между индустрией сетей беспроводной связи, сетями связи пятого поколения, сетями, которые обеспечивают работу интернета вещей?

В то время, как президент Совета по кибербезопасности Германии высказывает озабоченность защитой в киберпространстве небольших семейных компаний своей страны, вице-премьер России озабочен мировыми проблемами: «...мы сосредоточены сейчас на проблемах, которые проистекают из того, что половина населения мира носит мобильные устройства с интернетом. А если каждого человека через 5 лет будет окружать около 20 мобильных устройств?»

Но вызывает сомнение, что в странах, где лишь считанные проценты населения обладают более, чем 90% богатств, «каждого человека через 5 лет будет окружать около 20 мобильных устройств». И проблема не в количестве мобильных устройств, окружающих простого человека, а в наличии встроенной и «прозрачной» для цифрового обывателя качественной киберзащиты хотя бы одного смартфона.

БЕЗОПАСНОСТЬ НЕ В СКОРОСТИ, А В ПРИНЦИПЕ

Более прагматично рассуждает на ICC 2019 руководитель службы кибербезопасности Сбербанка, но не странно ли, что дипломированный инженер и кандидат технических наук видит серьёзный риск для кибербезопасности при внедрении связи 5G в первую очередь в её скорости: «за секунду весь телефон улетит в облако — и всё?»

Следуя этой логике, серьёзный риск авиации в том, что аэропланы летают.

И не странно ли, что ответ на ситуацию «за секунду весь телефон улетит в облако — и всё» Сергей Лебедь видит в том, чтобы «повышать нашу скорость реагирования, обнаружения, защиты, реакции»? Сможет ли в реальной жизни «повышать нашу скорость реагирования, обнаружения, защиты, реакции» обладатель даже не 20, а одного-единственного мобильного устройства, если у него нет полноценной инструкции по эксплуатации этого «оборудования», а вендор фактически официально предлагает цифровому обывателю осваивать покупку методом проб и ошибок?

Может, например, в конкретной упомянутой ситуации стоит задуматься над тем, чтобы уж коли 5G будет внедрена в персональные устройства, то их конструкция должна отвечать требованиям, не позволяющим в принципе улететь в облако «всему телефону»?

НЕ ВСЕ ТАК БОГАТЫ

Руководитель службы кибербезопасности Сбербанка не видит больших проблем в реализации принципов риск-менеджмента при обеспечении кибербезопасности своей организации. Две-три «песочницы» в районе «периметра», быстрые технологии обнаружения угроз и быстрые же технологии для восстановления «упавших» приложений — вот «серебряные» пули для защиты от киберугроз крупной организации.

Но все ли «банки с базовой лицензией» и просто население нашей страны, вовлекаемое в процессы цифрового хаоса, обладают таким «боезапасом»?

Президент Совета по кибербезопасности Германии Ханс-Вильгельм Дюнн не забывает о том, что значительное количество бизнеса в Германии — семейные компании, предоставляющие качественные товары и услуги в рамках своих профессиональных компетенций, но не имеющие достаточного опыта и знаний в области обеспечения ИБ. И их интересы в этой сфере должны быть защищены в первую очередь ответственностью вендоров цифрового оборудования, а не «страховыми» технологиями. К такой постановке вопроса имеет смысл прислушиваться отечественным регуляторам. Управление «по требованиям» и риск-менеджмент не должны быть альтернативами, они должны работать совместно.

ты современных систем, ты понимаешь, что для этого нужно не только иметь очень мощную компетенцию внутри, но для этого нужна очень серьезная кооперация. Собственно говоря, мы с нашими партнёрами вместе выходим на этот форум с главной идеей — мы для себя какое-то количество лет назад сделали абсолютный вывод, что мы чувствуем себя уязвимыми и у нас есть страх перед будущим. Потому что мы видим, что самостоятельно эту проблему не решим. Всё больше и больше происходит процесс диджитализации, и экспоненциально растут риски кибербезопасности.

Два года назад мы ввели в действие SOC и были уверены, что достигли очередной планки соответствия, но сейчас понимаем, сколько нам еще нужно сделать.

Алоис Цвингги, руководитель Центра кибербезопасности Всемирного экономического форума:

— На Всемирном экономическом форуме мы пришли к необходимости создания центра кибербезопасности. Для руководителей крупных компаний проблема кибербезопасности — вопрос стратегии, вопрос обеспечения существования компании.

Кайрат Келимбетов, управляющий Международного финансового центра, Казахстан:

— Киберзлоумышленники работают в трансграничном масштабе, и ответ тоже должен быть трансграничным. Поэтому нам нужно двигаться в эту сторону вместе и понимать угрозы, которые стоят перед нами. Международный финансовый центр «Астана» совместно со Сбербанком также считают, что инициатива коалиционно выступать против угроз кибербезопасности должна расширяться на многие регионы, в том числе на регион Евразийского экономического союза.

«КОД ИБ» В МОСКВЕ 2019

ЭФФЕКТИВНЫЕ СБОРЫ В КЛУБНОМ ФОРМАТЕ

«Мой муж — гений! Он может делать всё, кроме денег». Эта фраза жены Эйнштейна вполне характеризует отношение бизнеса к ИБ. Но многое может измениться после доклада Рустема Хайретдинова «Как защитить бизнес-процесс» на конференции «Код ИБ». Докладчик поведал, как с помощью инструментов ИБ — приложений SIEM, UBA, DLP — выявлять отклонения в деловых процессах от задуманной линии реализации. Анализируя отклонения и предлагая корректирующие мероприятия, служба ИБ способна повысить эффективность бизнеса, демонстрируя свою полезность не только на ниве киберзащиты.

РАЗУМНО НЕБРЕЗГЛИВ

Московский этап конференции «Код ИБ» показал, что информационная безопасность сплачивает вокруг себя людей с особым, одновременно и критическим и креативным, взглядом на современный цифровой мир. Докладчики и ведущие мастер-классов, тренингов и круглых столов буквально заставили слушателей увидеть текущие проблемы ИБ под новыми, зачастую парадоксальными углами зрения.

Помимо уже упомянутого доклада Рустема Хайретдинова, впечатлило выступление Алексея Плешкова. Начальник управления режима ИБ Газпромбанка представил нетривиальный взгляд на «тёмный» Интернет. Алексей продемонстрировал, как инициативный «ибэшник» может извлечь пользу из информации, представленной в «даркнете». Погружение в эту часть Всемирной паутины позволяет не следовать за угрозами, а предсказывать и предупреждать кибератаки. Что касается моральных издержек, то «ибэшник», как и врач, должен быть разумно небрежлив и внимателен к гигиене. Рекомендации Алексея, безусловно, обогатили публику.

Полезными оказались и сообщения о контроле сотрудников в информационной среде компании (Дмитрий Кандыбович), о подводных камнях при организации антивирусной защиты в условиях интеллектуализации средств нападения на периметр (Вячеслав Медведев), о классификации подходов компаний к запросам на безопасность и возможным ответам на эти запросы (Дмитрий Блейзер). Эксперты актуализировали знания аудитории, пред-

ставив ряд новинок и сконцентрировав общее внимание на вопросах практики служб ИБ.

ЛОВИСЬ, РЫБКА!

Связующим звеном первых двух дней стала игра в командную работу служб ИБ, плавно перетёкшая в киберучения по фишингу под управлением Алексея Лукацкого. В итоге участники и зрители получили практически выверенный набор рекомендаций, реализация которых позволяет снизить эффективность «рыбалки» с нынешних 60–95 % (доля фишинга в общем количестве результативных кибератак) до неизбежных «клюнувших» (с позиций психологии) единиц процентов.

Сложные чувства вызвали результаты деловой игры по организации командной работы в ИБ. Интересна сама по себе попытка «сладить» команды за пару часов. И особенно любопытно было посмотреть на результаты этого — при постановке задач в форме, что называется, «fuzzy logic».

БЫЛО ВЕСЬМА КОМФОРТНО

Подводя итоги, можно констатировать, что конференция «Код ИБ» в Москве прошла в доверительной и познавательной клубной атмосфере. Нельзя не отметить весьма удачный «тайминг» докладов, количество перерывов, организацию деловых пространств конференции. Мероприятия не были избыточно утомительными, а их участники (проводить разделение на слушателей и «спикеров» тут не совсем уместно) выходили из залов с чувством лишь лёгкого «голода» по части незаданных вопросов. Но тут же могли удовлетворить свои потребности в продолжении общения уже в неформальной комфортной обстановке. Небольшая выставка, организованная рядом с залами, позволила познакомиться с представленными на ней новинками, а консультанты на стендах отвечали на вопросы с пониманием интересов участников конференции.



Код ИБ ПРОФИ Москва. Фото: vk.com/expolink_event

CISO ФОРУМ 2019

О ВНУТРЕННЕЙ КУХНЕ ИБ: ПРАКТИКА, БИЗНЕС,
ЗАКОНЫ И «ОБЛАКА»

С ISO Форум можно рассматривать как своеобразную отчётную конференцию в преддверии летнего затишья. Его гости встретились с более чем полусотней экспертов из банковской сферы, промышленности, торговли, из отечественных компаний и российских представительств компаний иностранных, с теми, кто «под санкциями», и с теми, кому ещё предстоит попасть в этот переплёт, с операторами персональных данных и с теми, кто таковыми себя не считают.

БОРЬБА ЗА БЮДЖЕТ

Российский рынок ИБ — это единицы процентов от зарубежного, что плохо для отечественных вендоров. Психология же бизнеса такова, что, по мнению Рустема Хайретдинова, угроза ИБ с вероятностью менее 100% рассматривается ЛПРом как угроза с вероятностью «орёл/решка», а значит «пока гром не грянет...». В результате в стране ИБ-проекты зачастую конкурируют за бюджет не между собой, а с бизнес-проектами. Поэтому одной из центральных тем на форуме стали технологии «успешных продаж» ИБ-проектов внутри компании. А также обсуждение, как вырастить в себе руководителя-«безопасника» и эффективно искать работу, в том числе за рубежом.

НА УРОВНЕ АНАЛОГА

Сухой остаток от услышанного и увиденного не слишком оптимистичен. Импортзамещение пробуксовывает, отечественные средства ИБ сырова-

ты, по-настоящему закрыться от киберугроз исключительно российским щитом не удаётся. Дмитрий Соломенцев из Банка ВТБ обозначил основную проблему для своего банка как отсутствие сквозных линеек по разным направлениям. Алексей Плешков из Газпромбанка высказался политически корректно: «Если отечественное решение соответствует требованиям или в целом на уровне зарубежного аналога, мы стараемся отдавать голоса нашему продукту».

ПРО КОРПОРАТИВНУЮ ПАРАНОЮ

А в дополнение к проблемам технологическим остаётся актуальной проблема «социальная» — сотрудники, чью тщательно взращиваемую корпоративную киберпаранойю успешно «лечат» рекламные посулы «цифровой экономики», призывающие работать «в один клик». «Безопасность — это не периметр. Всегда найдётся сотрудник, который откроет не ту ссылку», — отметил Илья Садовенко, Mary Kay. Меры для решения этой проблемы предлагаются зачастую самые радикальные. Сергей Вахонин, DeviceLock DLP, считает, что «нужно давать ровно столько возможностей, сколько человеку нужно для работы. Не больше. Для работы не нужны мессенджеры? Убрать. Не нужен цветной принтер? Ограничить доступ».

ПРО КОМПЛАЕНС

Центральной правовой темой стало обсуждение комплаенса в связи с 152-ФЗ, ведь каждая компания как минимум

имеет кадровую службу и интерактивный сайт. Мастер-класс Алексея Плешкова вылился в информативный обмен «премудростями» с аудиторией касательно реагирования на недомолвки законодательства о персональных данных.

ПРО ОБЛАКА

Темой, давно интересной, но не получившей на CISO 2019 внятной оценки со стороны потенциального потребителя, являются «облачные» технологии ведения бизнеса. Формально рассуждая, публичные и гибридные «облака» позволяют существенно повысить эффективность бизнеса. Однако, даже при наличии классического периметра, современная мобильность сотрудников и дистанционные технологии общения с клиентами доставляют безопасникам массу забот. А при использовании облаков масштабные мобильность и дистанционность — неизбежность.

На форуме тема «облаков» была затронута в контексте опыта компании Check Point, предлагающей платформу Check Point Infinity и сервисы Cloud-Guard для безопасного освоения «динамичных ИТ-сред». Но тут как бы за кадром осталась проблема импортозамещения. Есть ли сквозные отечественные решения для обеспечения ИБ в «облаке»? А это важно для бизнеса, который работает с оглядкой на санкционное творчество заокеанских партнёров и вовлечённых в эти игры партнёров с нашего континента. Для внедрения облачных технологий пора сформулировать внятную отечественную технологическую программу со сроками и ответственными.

Собственно, это пора сделать не только для «облаков», но и для направления ИБ в целом. Так считают многие участники форума.

Психология же бизнеса такова, что, по мнению Рустема Хайретдинова, угроза ИБ с вероятностью менее 100% рассматривается ЛПРом как угроза с вероятностью «орёл/решка», а значит «пока гром не грянет...»

THINK SUMMIT МОСКВА

КОНФЕРЕНЦИЯ IBM О БЕЗОПАСНОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ БИЗНЕСА

Проведённая в середине мая в Москве большая конференция IBM в России сконцентрировалась на обсуждении небольшого числа тем:

- ♦ Данные и ИИ;
- ♦ Облачные технологии и инфраструктура;
- ♦ ИБ и непрерывность бизнеса;
- ♦ Цифровые технологии в добывающих отраслях.

ГЕОЛОГИЧЕСКИЕ ПОДВИЖКИ

Открывая пленарное заседание, генеральный директор IBM в России и странах СНГ Ирис Джеба сосредоточилась на достоинствах применения IT для решения приземлённых и бытовых проблем в сельском хозяйстве и экологии, включая утилизацию отходов.

Технический директор, исполнительный вице-президент Сбербанка Давид Рафаловский рассказал о намерении Сбербанка превратиться в технологическую компанию. Фонетически он не озвучил чего-то нового, но на уровне эмоций возникло ощущение, что в России появилось теневое министерство цифровых технологий, которое решает проблемы финансирования своих проектов гораздо оперативнее и масштабнее, чем иные госведомства и частные структуры. Ключевые инструменты превращения Сбербанка в технологическую компанию сформулированы чётко и броско: Agile (Sbergile), производственный процесс разработки ПО (SberWorks), облачная инфраструктура (SberCloud), искусственный интеллект (AI First).

Гораздо более узко фокусировал своё выступление старший вице-президент «Норникеля» Сергей Батехин. Он рассказал о блокчейн-решении для поддержки сбыта металлов, в том числе редких и не торгуемых на бирже. Достоинства технологии — в возможности контроля происхождения металлов и их движения по цепочке продаж. О реальном «выхлопе» инициативы мы, возможно, скоро узнаём, но вклад в развитие IT-рынка есть

уже сегодня — поддержка металлургами блокчейн-платформы Hyperledger Fabric.

И СНОВА О БИЗНЕСЕ

Вице-президент IBM в странах Центральной и Восточной Европы Кирилл Корнильев представил доклад «Бизнес нового поколения: модели, подходы, технологии» на основе материалов аналитиков IBM. В качестве самых важных внешних факторов развития бизнеса на цифровых платформах названы рыночные факторы, технологические факторы и навыки персонала.

В своём выступлении К. Корнильев сосредоточился на положительной динамике, подкрепив её данными о том, как в лидеры выходят компании, использующие инновации (анализ больших данных на основе машинного обучения и облачные технологии). Завершилась пленарная сессия дискуссией «Бизнес нового поколения» с участием представителей ВТБ, МТС, «Мегафона», «ММК». Выступающие не раз подчеркнули важность анализа больших данных при выстраивании бизнес-процессов в своих компаниях.

И как оказалось, не один Сбербанк заглядывается на чужие «поляны». МТС, в частности, находится на пути перехода от бизнеса телеком-провайдера к созданию экосистемы бизнесов, эффективность которых будет обеспечиваться комплексными знаниями о клиентах компании, которые у оператора связи нарастают как снежный ком.

ПОДЪЁМ С ГЛУБИНЫ

Секция по информационной безопасности произвела приятное впечатление своей системностью и вдумчивым подходом к проблемам ИБ. После того, как руководитель подразделения ИБ IBM в России и странах СНГ Илья Кравцов заострил внимание слушателей на возможностях решения проблем безопасности с помощью экосистемы партнёров IBM, сессия предложила своим гостям путешествие по кругам... нет,

не ада, но горных серпантинов восхождения к совершенству системы ИБ.

Сначала Сергей Путин, директор по информационным технологиям ООО «УК «Росводоканал», рассказал, как крупный оператор в сфере ЖКХ пришёл к осознанию необходимости выстроить систему информационной безопасности и уже прошёл важнейшие стадии на этом пути. Далее управляющая компания розничной сети «Магнит» представила опыт перехода от самописных решений к использованию коммерческого продукта для построения SIEM-системы для крупнейшего ритейлера России.

А для тех, у кого нет ресурсов ЖКХ или розничной торговой сети, представитель компании BI.ZONE рассказал о перспективах рынка аутсорсинга ИБ в России, а потом, развивая тему, директор департамента операционных рисков «Московской Биржи» Сергей Демидов рассказал об опыте построения систем защиты данных в гибридных «облачных» средах.

ВЫШЕ ГОР

Справедливости ради отметим, что к вопросам ИБ на форуме следовало бы отнести и темы, обсуждавшиеся и на других секциях. В конце концов, ИБ — это не только анализ инцидентов, подготовка планов киберучений и поиск «дыр» в ПО, написанном под прессом пресловутого time-to-market. Безопаснее там, где код контролируется сообществом и его можно оперативно кастомизировать, там, где надёжная аппаратная инфраструктура... И об этих сильных сторонах IBM — активном участии в работе софтверной экосистемы Open Source и о предоставлении столь же открытому сообществу процессорной архитектуры Power — также шла речь.

* * *

Но «нельзя объять необъятное», как и присутствовать сразу на всех мероприятиях форума. Придётся читать документацию.

НАЛИЧНЫЕ В XXI ВЕКЕ

ЖАРКИЕ ДИСКУССИИ НА ПЯТОМ ОТРАСЛЕВОМ СОВЕЩАНИИ «АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ НАЛИЧНОГО ДЕНЕЖНОГО ОБРАЩЕНИЯ»

Слухи о «смерти» наличных денег оказались несколько преувеличенными. Прошедшее 29 мая совещание организаций сферы НДО и перевозки ценностей аргументировано это доказало. Причины сохранения наличных денег как минимум две: безопасность жизнедеятельности и консерватизм населения. Совещание показало, что цифровизация ритейла и банковской сферы не только не подразумевает тотальную виртуализацию денежных расчётов, но и позволяет сделать оплаты наличными более удобными и снизить издержки на их обеспечение.

ПРАГМАТИЗМ И ФУТУРИЗМ

Отказаться от наличных денег не даёт обычная осмотрительность — купюры и монеты в карманах позволяют

сгладить проблемы оплаты при сбоях в электроснабжении, работе интернета, при природных и техногенных катастрофах.

А когда инженерная инфраструктура и цифровые технологии работают нормально, законодательство, специальное оборудование и программные приложения могут позволить ритейлу повысить оборачиваемость наличных средств и даже зайти на новый для этой сферы рынок банковских услуг. Например, деньги, поступившие в кассы гипермаркетов и прочих магазинов, дистанционно учитываются банком и оперативно зачисляются на счета этих торговых организаций. При этом денежные купюры, собранные в кассах, автоматически закладываются в местные банкоматы и продолжают участвовать в обороте без промежуточной инкассации. Современное электронно- и электромехани-

ческое оборудование считает и сортирует наличные, отбраковывая ветхие купюры на порядок точнее и надёжнее человека.

Рассказанное — не домыслы и не плод футуристических фантазий. Владимир Изутин, заместитель председателя правления объединения «РОСИНКАС», в своём докладе «Общеввропейские тенденции на рынке НДО (по материалам конференции ESTA 2019 г.)» убедительно продемонстрировал, что население ряда европейских стран придерживается традиционных ценностей наличного денежного обращения, а лидером здесь является Австрия, где доля НДО не намного ниже 50%.

РОССИЙСКИЕ РЕАЛИИ

Что касается нашей страны, то хотя в прошлом году доля наличного денежного оборота в ритейле ушла ниже доли безналичных расчётов, абсолютный оборот наличных денег устойчиво увеличивается и в рублёвом эквиваленте и в «листах». Так что, по крайней мере, до 2028 года участникам рынка НДО безработицы опасаться не стоит. По прогнозам в этот год доля НДО в платежах ритейла пойдёт вниз и составит около 20%. Но следует помнить, что и эта величина в масштабах нашей страны не так уж мала. А прогнозы, как известно, не всегда сбываются.

В свете сказанного среди стратегических задач отрасли — планомерная борьба за безопасность НДО и «прозрачность» наличного денежного оборота, за рост эффективности работы ритейла и финансовых структур с «наличкой». Елена Меланич, первый заместитель председателя правления Ассоциации «НДО», отметила в своём докладе, что около 70% деятельности Ассоциации будет связано с обеспечением безопасности в сфере наличных расчётов и инкассации.



Директор департамента наличного денежного обращения Банка России Александр Лахтиков и председатель правления Ассоциации «НДО», президент-председатель правления Объединения «РОСИНКАС» Олег Крылов



Выступление члена комитета Совета Федерации по регламенту и организации парламентской деятельности Виктора Озерова



Образцы оборудования для НДО в демонстрационной зоне Отраслевого совещания

О том, какого уровня трудности преодолевают работники сферы инкассации, рассказал Дмитрий Коновалов, советник начальника ФГУП ГЦСС, в докладе «Особенности обслуживания клиентов в удалённых регионах России». В качестве примера был взят один регион — Дальний Восток. Но его размеры, «помноженные» на качество дорог и коммуникаций, плотность населения и климатические условия, позволили автору доклада выпукло продемонстрировать реально существующий «экстрим» при обслуживании НДО на просторах России.

КРЕАТИВ И ВОЛЬТЕРЬЯНСТВО

Инструментарий для обеспечения прозрачности и эффективности в наш «цифровой век», казалось бы, очевиден — автоматизация. Однако совещание собралось экспертов не только компетентных, но и креативных. Поэтому один из предложенных вариантов повышения эффективности был сформулирован как «Повышение эффективности инкассаторской деятельности через оптимизацию регуляторных требований». Присутствовавшие на Совещании представители регулятора отреагировали конструктивно, и предложения были приняты к анализу.

«Очевидная» автоматизация также не выпала из поля зрения Совещания: о её возможных направлениях и технологиях много говорили представители отечественных и зарубежных (скажем прямо — из Японии) вендоров оборудования. Идеи высказывались от банальных до откровенно футуристических, когда ритейл обретает банковские полномочия, получив оборудование «завтрашнего дня» (которое в Японии местами — уже «сегодня»).

Вольтерьянство вендоров получало мгновенную оценку банковского сообщества (ЦБ, Сбербанк, Банк ВТБ и др.) и сетевого ритейла («Магнит», «Фамилия» и др. торговые сети), представленного не одиночными экспертами, а мощными командами. Но отброшено не было, а было записано для более глубокой проработки в планы Ассоциации «НДО».

БУРНЫЙ ПОТОК ДИСКУССИЙ

Мощнейшим лидером и модератором дискуссий выступил Олег Крылов, председатель правления Ассоциации «НДО», президент-председатель правления Объединения «РОСИНАКАС». Ему достойно соаккомпанировали на технологических секциях Наталья Ракова, руководитель департамента стратегического маркетинга

«Гизеке & Девриент — ЛОМО, ЗАО» и Сергей Барсуков, президент «ПРОФИНДУСТРИИ-ЦЕНТР». А острые полемические дискуссии последнего с Михаилом Горфункелем, директором по специальным проектам GLO-RY RUS, украсили совещание как содержательно, так и примером ведения жарких схваток в рамках высших стандартов дипломатической корректности.

Ряд напутствий и рекомендаций экспертам отрасли дал сенатор Виктор Озеров, член комитета Совета Федерации по регламенту и организации парламентской деятельности, ранее более полутора десятков лет работавший председателем Комитета по безопасности и обороне и стоявший у истоков образования Ассоциации «НДО». Среди важнейших рекомендаций сенатора — начать 6-е совещание с ревизии итогов выполнения планов, намеченных на нынешнем заседании.

«Конференция прошла успешно! И так пятый раз!», — подвёл итоги Совещания Олег Крылов, и, похоже, лишь эти слова смогли остановить в 18:00 идущую по нарастающей дискуссию. Которая, впрочем, продуктивно продолжилась на фуршете.

CRITICAL COMMUNICATIONS RUSSIA 2019

МОБИЛЬНАЯ СВЯЗЬ ДЛЯ ОТВЕТСТВЕННЫХ ПРИМЕНЕНИЙ

Индустрия Critical Communications — это про системы связи, сохраняющие функциональные возможности до момента физического разрушения оборудования. Все прочие неблагоприятные факторы — температура, влага, электромагнитные помехи, число активных «абонентов», происки враждебных разведок и т.п. должны быть учтены при проектировании сети и нейтрализованы в случае проявления при реальной эксплуатации.

Некогда мобильные системы связи для ответственных применений были прерогативой спецслужб и железнодорожного транспорта, сегодня «простые» коммерческие предприятия, заботясь об информационной безопасности, обзаводятся корпоративной мобильной связью, недоступной для хакеров и независимой от произвола автоматизации коммерческих телеком-провайдеров. На конференции Critical Communications Russia 2019 обсуждались вопросы развития и внедрения профессиональной мобиль-

ной радиосвязи на основе стандарта LTE и создания на её основе интеллектуальных систем видеомониторинга, обеспечения общественной безопасности на крупных мероприятиях, передачи сигналов оповещения и экстренной информации при чрезвычайных ситуациях. Среди докладчиков конференции был убедительный пул представителей несломленной российской радиоэлектронной промышленности, готовой насытить рынок связи отечественной высокотехнологичной продукцией. И были

«У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН! — КТО ГОВОРИТ? — VIPNET QSS PHONE!»

Компания ИнфоТеКС и Центр Квантовых Технологий (ЦКТ) Физического факультета МГУ им. М. В. Ломоносова продемонстрировали журналистам работу первой в России линии голосовой телефонии с криптозащитой трафика на т.н. «квантовых ключах».

Демонстрация прошла в режиме телемоста между московским офисом компании ИнфоТеКС и расположенным в ЦКТ одним из узлов коммуникационной сети, защищённой на квантовых ключах. Видеопоток шифровался с помощью другой совместной разработки ИнфоТеКС и МГУ — комплекса квантово-криптографической защиты информации ViPNet Quandor, разработку и производство которого поддержало Министерство науки и высшего образования РФ.

Городские каналы связи были построены на оптоволоконной линии, предоставленной компанией «ЮЛ-ком».

К сожалению, не все журналисты поняли, что изюминка демонстрации — не банально обыденные телефонные аппараты, а пара «коробочек». Одна — та, для демонстрации которой авторы разработки сняли кожу заурядного корпуса, в котором с таким же успехом могла быть смонтирована начинка «обычного» компьютера. И ещё одна «коробочка»,

также не очень большая, а говоря языком техническим — выполненная в конструктиве формата 3U и смонтированная в стандартную серверную стойку.

Те из представителей СМИ и/или их читатели, которые не разобрались в том, где зарыта начинка квантового шифрования, решили, что заявленные траты в 700 млн рублей (140 млн из которых дало государство, а остальные 80 % суммы — частная компания ИнфоТеКС) пошли на закупку телефонных аппаратов, что является заблуждением.

Сотни миллионов денег были потрачены на то, что называется НИОКР — научно-исследовательская и опытно-конструкторская разработка, приведшая к тому, что макет устройства для распределения квантовых ключей, работающий в условиях сверхнизких температур, и занимающий солидный физический объём, превратился в компактное «железо» и дополнен всей необходимой связной «периферией».

В результате оказалось возможным обеспечивать не только голосовую, но и видеосвязь для организации совещаний и переговоров с потенциально неограниченным числом участников без опасности прослушивания. Ведь особенность квантовой технологии шифрования — невозможность расшифровки информации в канале защищённой связи, основанная

представители зарубежья, готовые подставить плечо этому российскому рынку продукцией локализованной.

Честь первых докладов устроители конференции предоставили иностранным гостям, которые рассказали о своих планах и шагах по конвергенции унаследованных технологий профессиональной мобильной связи с профессиональным исполнением технологии LTE. После чего российские докладчики раскованно и непринуждённо сообщили о своих успехах по адаптации технологии LTE на российскую целину корпоративных Critical Communications. Похоже, что эффект развития с отставанием сыграл свою положительную роль, и российские потребители систем связи для ответственных применений могут получить определённый гандикап, начав свои внедрения с действительно высоких технологий.

Помимо LTE в исполнении Critical Communications на конференции был представлен стандарт недорогих систем «цифрового радио» DMR. Сначала ита-

льянский гость представил стандарт этой технологии и достижения рабочей группы, занимающейся стандартизацией технологии, а потом слушатели познакомились с отечественным воплощением разработки DMR-оборудования на Саратовском электроприборостроительном заводе им. Серго Орджоникидзе, ведущим свою историю со времён первой индустриализации.

В качестве приложений, которые используют профессиональную мобильную связь (своеобразного антагониста сотовой связи потребительского уровня), на конференции были представлены доклады о системах мониторинга и дистанционного управления с использованием защищённых каналов связи; о системах интеллектуального видеонаблюдения и распознавания лиц (на примере Москвы); о защищённых решениях для спецслужб и служб быстрого реагирования.

Сухой остаток по итогам конференции можно сформулировать в виде вывода о хороших перспективах ис-

пользования технологии LTE на рынке систем мобильной связи для ответственных применений в аэропортах, на территории морских портов, на территориально распределённых объектах, предъявляющих особые требования к коммуникациям между сотрудниками, к M2M-коммуникациям в части доступности и криптозащиты. При этом имеется ряд отечественных компаний, обладающих высокими компетенциями и в части разработки соответствующих систем, и в части их развёртывания.

К сожалению, на конференции был представлен лишь один доклад, посвящённый диагностике систем связи для ответственных применений. Однако Денис Сладких (Viavi Solutions) смог, как видится, донести до аудитории важность этой компоненты индустрии Critical Communications. Он сопоставил расходы по этой статье в США (более 1 млрд долларов), Европе (около полумиллиарда евро) и России (менее 1 млрд рублей).

на фундаментальных физических принципах. Известные на сегодняшний день модели атак с использованием квантовых компьютеров бессильны, по утверждениям создателей нового уникального оборудования, в плане преодоления защиты системы телефонии ViPNet QSS Phone. Формируемые оборудованием «квантовые ключи шифрования» неизвестны даже администратору сети.

С организационной точки зрения, это событие — результат государственно-частного партнёрства или «решение общественно значимой задачи на основе взаимовыгодного сотрудничества государственных структур и частных компаний». Его общественная значимость определяется тем, что есть ситуации, когда нет времени держаться, когда денег нет. Например, обеспечение информационной безопасности нельзя отложить «на потом».

В ходе проведения пресс-конференции обсуждался и вопрос кадров, обладающих сбалансированной подготовкой в области квантовых технологий и общих инженерных дисциплин. Конечно, их не хватает. Физический факультет МГУ готов расширить приём студентов для этих целей на 50 че-

ловек. А вкуче со своими партнёрами по Квантовому консорциуму, среди которых — МВТУ им. Баумана и ряд вузов «северной столицы», ежегодная подготовка таких специалистов может быть доведена до нескольких сотен человек.

Дело за решением соответствующего министерства.



Демонстрация работы предсерийного образца первого в России «квантового» телефона ViPNet QSS Phone. Фото: infotecs.ru

**Сергей МЕЛЬНИКОВ**

заместитель генерального
директора ООО «Лингвистические
и информационные технологии»,
кандидат физико-математических наук

ЗАДАЧКА ПО БИОМЕТРИИ: КТО НАПИСАЛ ТХТ?

ОПРЕДЕЛЕНИЕ АВТОРСТВА ТЕКСТА В СИСТЕМЕ ИДЕНТИФИКАЦИИ

БИОМЕТРИЯ И ОПРЕДЕЛЕНИЕ АВТОРСТВА ТЕКСТА

Задача определения авторства принадлежит активно расширяющемуся в настоящее время кругу биометрических задач [1]. К ней можно отнести: определение авторства произнесённой речи по голосу [2], определение авторства по почерку [3], определение авторства по тексту.

Задача установления авторства текста решается с помощью выделения особенностей авторского стиля и сравнения этих особенностей с другими текстами, авторство которых известно. С начала XX века делались попытки формально определить стиль автора текстового произведения, хотя проблема спорного авторства появилась задолго до этого. Предпосылками для споров над авторством текстовых произведений были анонимные тексты, случаи плагиата, творчества под псевдонимами и др. Технологии определения авторства по тексту, использующие вычислительно-лингвистические подходы, активно развиваются последние тридцать-сорок лет. Авторский текст — один из самых сложных и, видимо, не слишком надёжных источников биометрических признаков. Однако востребованность использования его особенностей с точки зрения биометрии высока, что связано с гигантской популярностью систем обмена текстовыми сообще-

ниями (е-мейл, соцсети, смс, мессенджеры) и доступностью их материалов для анализа.

Среди инструментов автоматического анализа текстов, технологии определения авторства занимают сравнительно незначительную нишу. Рядом с этой нишей расположены такие технологии, как: идентификация языка/диалекта и тематики текста, выделение фактов из текста, установление зависимостей между текстами, выделение спама и др. Со всем родственными являются технологии определения плагиата, определения искусственного происхождения текста, оценки эмоциональной окрашенности, определения пола, возраста, профессии и психологических особенностей автора.

НА ПРАКТИКЕ

Практическое применение технологий определения авторства во многом связано с криминалистическими задачами. Известны случаи, когда анализ текстов сообщений с угрозами позволял экспертам однозначно определить автора среди группы подозреваемых или значительно сузить их круг. Актуальной, как показывает история с обвинением России во вмешательстве в американские выборы, является и задача установления авторства исходных кодов вредоносного программного обеспечения [4]. Перспективным является использование технологий определения авторства для анализа фейковых новостей.

КАК РАЗВИВАЛИСЬ ТЕХНОЛОГИИ ОПРЕДЕЛЕНИЯ АВТОРСТВА

Движителем прогресса в развитии методов определения авторства служили многочисленные литературоведческие дискуссии, связанные как с чисто научными интересами участников, так и, возможно, с юридическими или даже политическими. Классическим примером является многовековой спор об авторстве произведений, приписываемых Вильяму Шекспиру. В отечественном литературоведении аналогичная полемика долго велась (и ещё ведётся) по поводу авторства романа «Тихий Дон». Многие скептики приписывают авторство как минимум первого тома этого романа не М. А. Шолохову, а малоизвестному писателю из среды казачества Ф. Д. Крюкову. По мнению ряда экспертов, стиль текста первого тома романа «Тихий Дон» сильно отличается от стиля остальных трёх частей.

Первые продвижения в задаче определения авторства принадлежат лингвистам. Была предложена красивая идея авторского инварианта как набора значений текстовых характеристик, которые позволяют однозначно идентифицировать автора или группу авторов среди других авторов. В работе родителей академика А. Т. Фоменко [5] на материале художественных произведений 23 русскоязычных авторов XVIII–XX веков анализировалась различ-



тельная способность относительной частоты встречаемости определённых групп слов в задаче определения авторства. Был сделан качественный вывод, что хорошей различительной способностью для прозаических текстов обладают так называемые служебные слова (союзы, предлоги, частицы). В цитируемой работе авторы выделили 55 служебных слов. Другие группы слов и ряд структурных признаков текстов авторами признаны не подходящими для включения в авторский инвариант. Похожая картина наблюдается и для других языков, в частности, арабского [6].

В современной филологии в последние десятилетия разрабатывается т.н. лингвоперсонологическая теория и теория языковой личности [7], однако для решения практических задач удобнее пользоваться весьма развитыми статистическими методами и доступными ресурсами (текстовые корпуса, различные словари, ПО синтаксического, грамматического, морфологического анализа) из арсенала компьютерной лингвистики.

Одним из ведущих мировых форумов по задачам определения авторства текста сегодня является ежегодная конференция PAN (Uncovering Plagiarism, Authorship and Social Software Misuse, <https://pan.webis.de>). На этом форуме

доклаждаются результаты новых исследований в области идентификации авторства текста и близких задачах. Проводятся соревнования по точности определения авторства на представленных организаторами тестах. Все без исключения такие исследования базируются на современных методах вычислительной лингвистики, используют развитый математический аппарат и современные методы классификации (нейронные сети, машины опорных векторов и др.).

ТОЧКИ РОСТА ТЕХНОЛОГИЙ

Можно выделить несколько направлений, которые активно развиваются в последние годы:

1. Определение авторства коротких текстов (твиты, смс). Сложность этой задачи связана с неустойчивостью статистических характеристик текста на малых объёмах.
2. Кросс-жанровая задача установления авторства, то есть определение авторства текстов одного жанра, если в качестве образцов авторских коллекций представлены тексты другого жанра (например, e-мейлы и публицистические статьи).
3. Кросс-языковая задача установления авторства. Особенность задачи состоит в том, что в качестве образ-

цов авторских коллекций представлены тексты на одном языке, а задача определения авторства ставится по текстам на другом языке.

4. Изучение и локализация влияния редакторской правки на авторский стиль.
5. Выявление случаев, когда текст «склеен» из нескольких текстов разных авторов.
6. Разработка технологий автоматического обеспечения анонимности, то есть разработка методов противодействия известным подходам к определению авторства.

Помимо перечисленных направлений, повышенный интерес всегда вызывают новые подходы к определению авторства в т.н. открытой задаче, когда анализируемый текст может принадлежать одному из известных авторов, а может быть «чужим», то есть неизвестным системе. Определённые успехи здесь связаны с идеей привлечения для промежуточных вычислений большого количества заведомо чужих текстов, т.н. импосторов.

ТИПОВАЯ СТРУКТУРА АЛГОРИТМОВ ОПРЕДЕЛЕНИЯ АВТОРСТВА ТЕКСТА

Практически все методы определения авторства имеют двухэтапную структуру.

На первом этапе вычисляется представительный набор характеристик текста. Важно использовать характеристики, независимые от тематики текста, настроения автора, то есть такие особенности письма, которые проявляются на неосознанном самим автором уровне.

В этот набор для русскоязычных текстов могут входить [8]:

- ♦ словоформы, употреблённые в тексте (частоты их встречаемости),
- ♦ морфологические признаки (суффиксы, приставки, корни, окончания),
- ♦ грамматические признаки (часть речи, род, число, лицо, падеж, время, наклонение, спряжение, возвратность и проч.),
- ♦ особенности использования регистра букв (т.н. очертания слов, «shapes»), знаков препинания, сокращений и аббревиатур, цифр и числительных в тексте, эмодзи и других неалфавитных символов,
- ♦ характеристики длин слов, предложений, абзацев,
- ♦ особенности допущенных орфографических, синтаксических и грамматических ошибок,
- ♦ характеристики лексического разнообразия текста,
- ♦ и ряд других характеристик. Обычно такой набор содержит несколько тысяч числовых характеристик.

На втором этапе для сравнения анализируемого текста с текстами из авторских коллекций используется тот или иной классификатор (например, нейронная сеть). Классификатор сравнивает набор характеристик текстов из имеющихся авторских коллекций с характеристиками поступившего текста. В результате сравнения делается вывод о близости поступившего текста к той или иной авторской коллекции.

Казалось бы, чем большее количество характеристик текста использовать, тем точнее будет результат. Однако на практике существует определённый потолок числа входов у классификатора, при превышении которого эффективность снижается. Этот потолок зависит от самого классификатора, от числа проверяемых авторов, от размеров текстов для обучения и теста, от особенностей языка.

ПРАКТИЧЕСКАЯ ЭФФЕКТИВНОСТЬ СУЩЕСТВУЮЩИХ РЕШЕНИЙ

В русскоязычном сегменте интернет можно найти до десятка программ идентификации авторства текста. Эти программы предназначены для анализа объёмных литературных текстов. Все они решают закрытую задачу идентификации, то есть все возможные варианты авторов задаются своими текстами, и выбирается наиболее подходящий

из них. Требования к объёму текстовых данных для идентификации и обучения весьма высоки и вряд ли могут обеспечить практическую значимость.

С другой стороны, результаты, докладываемые на упомянутой выше конференции PAN, показывают, что практически эффективные алгоритмы идентификации авторства существуют по меньшей мере для нескольких европейских языков. Они позволяют работать с весьма небольшими текстами, обеспечивая приемлемый уровень ошибок идентификации.

Безусловно, распознавание авторства по тексту расширяет возможности в сфере идентификации личности. Для банковской биометрии этот инструмент, возможно, пока ещё несколько экзотичен, но это только пока. Функции биометрической идентификации и в банковской и в других сферах стабильно расширяются, усложняются и постепенно переходят от статического распознавания к динамическим расследованиям, требующим как комплексного подхода, так и разнообразного инструментария. На этом пути ожидается немало сенсаций. BIS Journal держит руку на пульсе.

ЛИТЕРАТУРА

1. Маршалко Г. Б. Угрозы безопасности биометрических систем // BIS Journal № 4(27). — 2017.
2. Ромашкин Ю. Н., Сорокин В. Н. Скажи «Пароль» // BIS Journal № 1(4). — 2012.
3. Брославский М. В., Мельников С. Ю. Сравнение эффективности классификаторов в задаче текстонезависимой идентификации автора русскоязычного рукописного текста // Обозрение прикладной и промышленной математики, т. 25, вып. 3, С. 234–235, 2018.
4. Стрёмухов В. Д. Модель и метод анализа схожести и определения авторства вредоносного кода: дисс. к.т.н.: 05.13.19. — СПб ИТМО. — Санкт-Петербург, 2013. — 95 с.
5. Фоменко В. П., Фоменко Т. Г. Авторский инвариант русских литературных текстов. Предисловие А. Т. Фоменко // Фоменко А. Т. Новая хронология Греции: Античность в средневековье. Т. 2. М.: Изд-во МГУ, 1996, с. 768–820.
6. Германович А. В., Мельников С. Ю., Хвостенко В. М. О выборе множества слов, характеризующих авторский стиль арабского текста // Обозрение прикладной и промышленной математики, т. 24, вып. 4, С. 324–325, 2017.
7. Лингвоперсонология: типы языковых личностей и личностно-ориентированное обучение: монография / Под редакцией Н. Д. Голева, Н. Б. Лебедевой, Н. В. Сайковой, Э. П. Хомич. — Барнаул, Кемерово: Изд-во БГПУ, 2006. — 435 с.
8. Романов А. С. Разработка и исследование математических моделей, методик и программных средств информационных процессов при идентификации автора текста / А. С. Романов, А. А. Шелупанов, Р. В. Мещеряков. — Томск: В-Спектр, 2011. — 188 с.



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

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

ИБ-ПСИХОЛОГА ВЫЗЫВАЛИ?

ГДЕ, ПОЧЕМУ И КАК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕ ОБОЙТИСЬ БЕЗ СОЦИАЛЬНОЙ ПСИХОЛОГИИ¹



Лев ПАЛЕЙ
эксперт ИБ

К каким образом психология относится к информационной безопасности — как дисциплина, наука и профессия? Она актуальна и востребована, хотя и по-разному, в трёх направлениях:

- ♦ противодействие злоумышленникам, предупреждение инцидентов и их расследование;
- ♦ обеспечение информационной безопасности клиентских сервисов;
- ♦ внутрикорпоративные нужды: собственная информационная безопасность, кадровые и управленческие вопросы, маркетинг и PR.

ПРОТИВ ЗЛОУМЫШЛЕННИКОВ

Следует отметить, что сами злоумышленники уже давно активно используют инструментарий психологии. Не только как социальную инженерию, обман при личном общении, но даже при применении чисто технических средств. Яркий пример — уловка с изменением расширения вредоносного файла, в результате которого он выглядит как безобидная картинка. Этот приём основан на знании базовых шаблонов и стереотипов поведения пользователей.

И в маркетинге, и в мошенничествах социально-психологические инструментарии «атак» удивительно схожи. Методы «атак» делятся на нецелевые, «по площадям», и целевые, когда выбранные жертвы подробно изучаются. Способы сбора и анализа информации о потенциальных жертвах, способы манипулирования ими заимствованы из психологии. При фишинге, рассылках по электронной почте или обзвонах потенциальных жертв, злоумышленники используют те же самые приёмы, что и рекламные службы, рассылающие спам.

Задачи стоят одинаковые: привлечь внимание, начать общение. Далее, используя методики нейролингвистического программирования, — завоевать доверие, пробудить положительные эмоции, сформировать интерес и побудить к совершению определённых действий. Как рекламщик «впаривает» покупателю ненужный, может быть, товар, так и злоумышленник пытается втянуть потенциальную жертву в мошенническую схему.

Специалистам по информационной безопасности нужно знать злоумышленников: их «типажи», различный «почерк», особенности применения технических средств и приёмов «социальной инженерии».

Широко применяемый пентест (тест на проникновение) напрямую связан с аналитикой поведения, включая важные психологические аспекты. Пентест представляет главным образом имитацию действий злоумышленника в ходе целевой атаки. Условный злоумышленник пытается получить доступ к чувствительной информации или нарушить работоспособность критических корпоративных систем. Начальная фаза может быть как технической (поиск уязвимостей компонентов ИТ-инфраструктуры), так и социальной (получение информации по звонку специалисту).

Форензика, прикладная наука о расследовании компьютерных преступлений, включает инструментарий отраслевой психологии не в меньшей степени, чем обычная криминалистика — криминальную психологию. Методы расследования, описываемые форензикой, используют анализ отклонений и аномалий поведения участников инцидентов и причастных лиц. За техническими данными скрываются психологические особенности, которые выявляются зачастую интуитивно, на основе опыта.

ДЛЯ КЛИЕНТОВ

Социально-психологический инструментарий просто необходим для выстраивания эффективной системы информационной безопасности, предупреждения инцидентов и проведения их расследований. Представление о моделях поведения клиентов, о специфических уязвимостях различных социальных групп нужно для конфигурации профилей пользователей, определения мер безопасности для различных действий. Содержательны многие показатели: возраст, пол, место жительства, образование, профессиональный статус, уровень культуры информационной безопасности и многие другие.

На основе типичных моделей поведения пользователей для промышленных систем антифрода создаются алгоритмы выявления сомнительных операций, которые нуждаются в дополнительной проверке. Кроме того, понимание личностных особенностей клиента помогает не только преду-

¹ Полная версия статьи доступна в электронной версии журнала: <https://journal.ib-bank.ru/post/893>

преждать, но и расследовать инциденты, эффективно разрешать спорные ситуации, в частности, о «зонах ответственности» клиента и банка.

Известен тезис, что самым уязвимым звеном в защищаемой системе является человек. Что касается, хотя и по-разному, и сотрудников, и клиентов. Чтобы минимизировать личностные риски, нужно повышать их осведомлённость, формировать культуру информационной безопасности. Что включает понимание угроз, включая самые актуальные, знание правил безопасности и методик противодействия, готовность и умение их применять. Для обучающих мероприятий нужны эффективные методики, тексты, графика, иллюстрации, видео, аудио, тренинги и тесты.

КОРПОРАТИВНЫЕ НУЖДЫ

В корпорации социальная психология стихийно задействована в работе с кадрами. И с теми, кто отвечает за информационную безопасность, и с теми, чью безопасность обеспечивают. Кадровая служба оценивает сотрудников и социологически, и психологически: анкетировать, тестирует, проводит собеседования, изучает мотивации, «послужной список», анализирует его личностные особенности, достоинства и недостатки. Результаты позволяют сделать прогноз об эффективности работы специалиста, в том числе в команде.

Психология играет значимую роль в обеспечении собственной корпоративной информационной безопасности. Как уже говорилось, в устранении «слабого звена» в лице сотрудников: анализе их уязвимостей, составлении должностных инструкций в отношении информационной безопасности, обучении и проверке усвоения. Знание личностных особенностей сотрудников, коллектива в целом помогают эффективно выстроить систему предотвращения утечек данных, включая DLP-решения.

Немалое значение имеет и такая тонкая материя, как психологическая мотивация специалиста по информационной безопасности. Конкретно — его правосознание, этические принципы, корпоративная лояльность, ответственность и высокая мотивация к работе.

Далее, психология востребована при корпоративных продажах и покупках, а также при заключении контрактов. Специалисту по информационной безопасности нужно знать психологические приёмы, используемые в маркетинге и рекламе. Чтобы, с одной стороны, производя закупки решений для своей организации, «отделить зёрна от плевел», действительно необходимую и пользу предложений



Самым уязвимым звеном в защищаемой системе является человек. Что касается, хотя и по-разному, и сотрудников, и клиентов

от рекламного «шума». С другой стороны, чтобы эффективно продвигать продукцию и услуги своей организации на рынке. Создавать привлекательные продукты и убедительно «упаковывать» как для корпоративных клиентов, так и для физических лиц.

Знать психологию, учитывать личностный фактор, владеть эффективными приёмами также важно при выстраивании отношений с контрагентами, заключении контрактов с ним. И, далее, для развития общественных отношений (PR), позиционирования в отрасли, взаимодействия с государственными регуляторами.

Прошло время полагаться исключительно на практический опыт и интуицию. Однако «чистая психология», без знания специфики информационной безопасности, конкретных персон и особенностей отношений в отрасли мало поможет. Назрела необходимость в специализированной психологии, учитывающей особенности и реалии отрасли.



**Павел
БЫЛЕВСКИЙ**
шеф-редактор
BIS Journal

ОЖИДАЕМ ПРИБАВЛЕНИЯ

ПЕРЕЧЕНЬ СПЕЦИАЛИЗАЦИЙ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРИУМНОЖИТСЯ ОТРАСЛЕВОЙ
ПСИХОЛОГИЕЙ

Технологии неотделимы от «человеческого фактора» — от людей, которые их придумывают и используют. Это изначальное сродство начинает по-особенному проявляться в наш высокотехнологичный век. Наукоёмкие технологии настолько широко вошли в нашу жизнь, что качественно преобразовывают не только производство и быт каждого, но также собственно гуманитарную сферу и самого человека. Поэтому неизбежно углубление специализации, появление новых дисциплин и профессий на стыке технических и гуманитарных, теперь уже высоких, наукоёмких.

ГУМАНИТАРНОЕ НЕОТДЕЛИМО

Такова логика развития «древа» научной, образовательной и профессиональной специализации. «Ветвей» становится всё больше, в том числе и путём «перекрёстного опыления». Это касается и информационной безопасности, которая сама рождалась как междисциплинарная деятельность на стыке компьютерных телекоммуникаций и безопасности. Кстати, информационная безопасность банков имеет и третьего «родителя» — финансовую сферу. Но эта отрасль неотделима от целого ряда гуманитарных аспектов, которые могут играть решающую роль. Перечислим некоторые из них.

Первый — **обучение, профессиональное образование**, повышение квалификации, тесно связанные с воспитанием. Включая, как частную, но крайне важную задачу — выработку высшей творческой продуктивности, «сверхспособностей». Не так давно сформировалась такая важная образовательная задача, как «ликбез»,

формирование и развитие массовой культуры информационной безопасности. Как у представителей почти что любой профессии, так и у каждого в быту.

Для решения этих образовательно-педагогических задач требуется модернизация систем образования и обучения, информирования граждан, разработка методик и учебных планов. Выполнить это можно только коллективными усилиями на государственном, корпоративном и общественном уровнях.

Второй гуманитарный аспект, важный для отрасли — **этический**, важный для решения кадровых вопросов, выстраивания отношений в организации и с контрагентами, включая клиентов. Что хорошо, а что плохо, на что можно пойти, а что недопустимо. Некий профессиональный «кодекс» важен при приёме на работу, назначениях.

Кадровики внимательно изучают и анализируют доступную личную информацию кандидатов. Ту, что находится в открытом доступе в интернете, на аккаунтах в социальных сетях. Ненадёжного специалиста вряд ли примут на работу, от скомпрометировавшего себя сотрудника постараются поскорее избавиться. Подобную работу ведут и сотрудники, выбирающие контрагентов, выдающие кредиты.

Третий аспект — **философский, мировоззренческий**: понимание своего места в профессии и на занимаемой должности, позиционирования отрасли в обществе и в мире в целом. Это ценностный вопрос мотивации профессиональной деятельности: зачем я тут работаю, что должен делать, в какой степени я готов вкладываться. В значительной степени профессиональная мотивация увязывается с гражданской ответственностью и патриотизмом.

И, наконец, четвёртый аспект — **социально-психологический**. Он присущ и профессиональной этике, но особенно актуален в противодействии злоумышленникам. Противника необходимо «знать в лицо»: что это за люди, какие у них мотивы и повадки, чего от них мож-

Отрасль информационной безопасности неотделима от целого ряда гуманитарных аспектов, которые могут играть решающую роль

но ожидать. Такое знание важно и для выстраивания системы предупреждения инцидентов, для реагирования на них и для расследования. «Потенциальным противником» может оказаться как внешний, в том числе зарубежный, так и коллега — инсайдер, «крот», «оборотень», предатель.

Нужно также хорошо понимать и психологию клиентов, их разные типажи. Для того, чтобы знать психологические уязвимости, которые могут привести к техническим сбоям сервисов или сделать клиента жертвой мошенников — «социальных инженеров».

Можно ли обойтись без отраслевой психологии в противодействии «социальным инженерам» — мошенникам, этой интеллектуальной элите преступного мира?

«ТЕХЗАДАНИЕ» ОТ ПРАКТИКОВ

В информационной безопасности финансовой сферы, как, впрочем, и везде, главные участники — люди. Это они устанавливают правила, создают оборудование и пользуются им. Условно три большие группы: профессионалы, клиенты и злоумышленники. Поэтому от отраслевой психологии невозможно абстрагироваться, в любом случае она незримо присутствует как фон. В иных случаях оказывается решающей. И не вообще психология, а применительно к особенностям компьютерно-телекоммуникационных технологий и среды.

Отметим, что, казалось бы, чисто техническая тема «доверенной среды» обладает сильнейшим субъективистским, психологическим «привкусом». И это неслучайно. Недаром для специалистов по маркетингу и рекламе одним из козырей при продвижении новых продуктов является акцент на безопасности.

Именно поэтому предстоит формирование отдельной дисциплины — психологии информационной безопасности, возможно, даже и более узко: в финансовой сфере. Можно предсказать появление такой научной дисциплины со своим паспортом, входящей в перечень ВАК, новой профессии со своим профессиональным стандартом, штатными должностями, и, соответственно, специализацией обучения, нормируемой образовательным стандартом.

Фундаментальная психология сама явление довольно молодое, ей от силы около века. В нашей стране она формировалась в 1920–40 гг., а психологические факультеты МГУ и ЛГУ были созданы только в 1966 году. К настоящему времени ВАК фиксирует несколько отраслевых отделений психологии:

19.00.03 Психология труда, инженерная психология, эргономика;

Информационная безопасность банков — дисциплина, близкая к военному делу и борьбе с преступностью, где уже есть свои «отраслевые психологии»

19.00.04 Медицинская психология;

19.00.06 Юридическая психология;

19.00.07 Педагогическая психология;

19.00.12 Политическая психология.

Информационная безопасность банков — дисциплина, близкая к военному делу и борьбе с преступностью, где уже есть свои «отраслевые психологии». Военная психология занимается обширным перечнем важнейших вопросов, включая моральный дух и информационно-психологическое противоборство. Криминальная психология изучает типажи преступников, модели их поведения, а также психологические особенности жертв. Эти дисциплины родились с необходимостью — из практических потребностей.

Почему бы не появиться и такой науке, как психологии информационной безопасности? Сформировать «техническое задание», перечень вопросов к разработчикам отраслевой психологии должны практики. Собрав воедино те важные проблемы, которые принципиально не решаются организационно-техническими средствами без инструментария психологии.

Представляется, что наиболее актуальной такой проблемой сейчас является противодействие социальной инженерии в финансовой сфере. Как минимум в таком вопросе, как информирование клиентов о подобных актуальных угрозах и правилах безопасности. Потребуется исследование социально-психологических типажей клиентов, их поведенческих моделей, их уязвимостей для мошенников. Результаты послужат основой для разработки методических материалов и определения коммуникативных каналов их доведения до аудитории.

* * *

Гуманитарные аспекты информационной безопасности, включая отраслевую психологию, — не надуманный вопрос, а значимые реалии жизни. Не обращать на них внимания, полагаться на самотёк можно только до серьёзных инцидентов «с гуманитарной окраской». Чем шире и глубже информационные технологии будут входить в жизнь, тем дороже будет цена ошибок.



Татьяна НИКИТИНА
заместитель
директора ФКУ
«Центр экстренной
психологической
помощи МЧС России»

ПРЕДМЕТУ ОБЖ — ЦИФРОВУЮ МОДЕРНИЗАЦИЮ

ФОРМИРОВАТЬ КУЛЬТУРУ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ГРАЖДАН РОССИИ СЛЕДУЕТ
СО ШКОЛЬНОЙ СКАМЬИ

Предмет «Основы безопасности жизнедеятельности» должен быть актуализирован в соответствии с реалиями и угрозами цифрового общества, чтобы стать практически ценным и интересным для учащихся. Предстоит соответствующая переподготовка педагогов, преподавателей этого предмета. Сделать это помогут объединённые усилия администрации учебных заведений, методистов, родителей учащихся, экспертов по информационной безопасности и государственных регуляторов.

УЙТИ ОТ ФОРМАЛИЗМА И СКУЧНОСТИ

Формирование и продвижение культуры информационной безопасности у граждан России — актуальная задача, важный элемент общей безопасности жизни в современном обществе. Решение этой задачи нужно начинать с самого раннего возраста, на школьной и студенческой скамье — в рамках учебного предмета «Основы безопасности жизнедеятельности» применительно к угрозам, которые сопутствуют электронным сервисам и устройствам.

В настоящее время «Основы безопасности жизнедеятельности» (ОБЖ) — учебный предмет в системе начального, общего и среднего профессионального образования, воспитывающий культуру безопасности. Целями обучения являются:

- ♦ подготовка обучаемых к безопасному поведению как в повседневной жизни, так и в опасных ситуациях природного, техногенного и биолого-социального характера;
- ♦ формирование здорового и безопасного образа жизни,
- ♦ приобретение умений и навыков оказания первой помощи;
- ♦ усвоение начальных знаний об обороне государства, воинской обязанности граждан и подготовка к военной службе.

Готовность и умение противостоять «цифровым» угрозам», профилактика и предотвращение вовлечения детей и подростков в деструктивные сообщества, в том числе через интернет, напрямую относится к области ОБЖ. Вопрос в том, что эта тема должна быть прямо представлена в учебном курсе, иметь прямое отношение к практической жизни, понятно и интересно подаваться.

Культура безопасности может показаться скучной и излишне теоретической, формализованной, связанной с нормативными документами и инструкциями, неочевидно относящимися к привычной повседневной жизни. В настоящее время на мотивацию изучения ОБЖ негативно влияет и то, что этот предмет не включён в перечень государственной итоговой аттестации за курс основной школы. Однако отсутствие, низкий уровень культуры безопасности ведёт к инцидентам, в ходе которых может быть нанесён ущерб здоровью, возникнуть угроза жизни.

Одна из задач МЧС России — продвижение культуры безопасности населения, включая детей и подростков. «ОБЖ» — возможность привить культуру безопасности, которая, в свою очередь, есть элемент общей культуры человека. Предмет ОБЖ должен давать ученику не только конкретные знания, умения, навыки, но и заложить базовые ценности здоровья и безопасности. Наличие этих ценностей определяет выбор модели поведения в той или иной ситуации. Неважно, речь идёт про поведение в онлайн или офлайн среде, важны ценности, подкреплённые знаниями, умениями и навыками, которые будут способствовать правильному выбору.

К ПРОСТОТЕ, ПРАКТИЧНОСТИ, ИНТЕРЕСНОСТИ

Указанные проблемы в настоящее время решаются, в том числе при участии МЧС России и Министерства просвещения РФ. В первую оче-

редь, проблема мотивации: дети изучают ОБЖ не с очень большим интересом. Однако именно в этом предмете, согласно названию, должна быть максимальная связь с современной повседневной практической жизнью. Именно эту связь и надлежит установить.

Для этого необходима переработка учебного курса по предмету ОБЖ, его актуализация применительно к современным реалиям. В сегодняшнем учебнике есть описания чрезвычайных ситуаций с яркими иллюстрациями: катастрофы, наводнения, взрывы, включая Чернобыльскую АЭС. Большинство экспертов отмечают перенасыщенность курса критическими угрозами, вероятность наступления которых не очень велика. Напротив, минимум информации об угрозах, которые сопутствуют обычной повседневной жизни. Некоторые темы дублируются, другие отсутствуют.

Тема цифровой, кибербезопасности в курсе ОБЖ практически не представлена. В то время как электронные устройства и сервисы превратились в значительный, важный фактор жизнедеятельности большинства граждан. Молодые поколения пользуются ими, как правило, намного больше, чем старшие. Многие буквально «живут в сети». Аудитория социальных сетей превышает половину населения России. В отличие от нескольких лет назад интернет уже не «виртуальная реальность», а самая настоящая, для кого-то даже более реальная, чем подлинная.

Безопасность в интернете вряд ли можно отнести к предмету информатики. Там происходит обучение техническим вопросам работы с электронными устройствами, пользования интернетом. Правила безопасного поведения в интернете относятся к предмету ОБЖ, так называемые «правила первого знакомства».

Мы живём в большом городе и знаем, как безопасно вести себя. Но когда человек впервые идёт в новую среду — горы, в пустыню, — то тоже должен знать, какие опасности его могут подстеречь и что правильно делать, чтобы их избежать. Когда ребёнок попадает в интернет, у него должны быть представления об угрозах и о том, как в таких случаях нужно себя вести.

Именно такие правила информационной безопасности для детей и подростков должны быть разработаны экспертами и включены в курсы ОБЖ. Для этого нужно обозначить риски, проблемы в увлекательной, доступной для учащихся форме. Придётся решать и ряд сопутствующих проблем, в частности, методического обеспечения.

Ощущается дефицит кадров — преподавателей ОБЖ, тем более в требуемом качестве.

В педагогических вузах подготовка специалистов этого профиля сокращается. Ликвидируются самостоятельные профильные кафедры, их включают в состав других. Повышение квалификации ведётся излишне теоретически, без привязки к актуальным практическим угрозам.

Таким образом, для эффективного обучения безопасному поведению, в том числе противодействию информационным угрозам, предстоит модернизировать сам предмет ОБЖ, систему его преподавания, подготовку преподавателей. Предмет ОБЖ должен стать простым, практичным, интересным и современным.

НАПРАВЛЕНИЯ ПЕРЕМЕН

Не помешает, а наоборот, поможет своего рода молодёжная «мода» на ОБЖ. Некогда школьники «модничали», ходя морозной зимой по улице без шапок, но теперь наоборот. Точно так же следует помочь появлению у учащихся моды на защищённость, безопасность поведения в интернете и обращения с разными гаджетами. Можно быть уверенными, что найдутся и «законодатели моды» на культуру информационной безопасности молодёжи.

24 декабря 2018 года коллегия Министерства просвещения РФ утвердила новую концепцию преподавания учебного предмета «Основы безопасности жизнедеятельности». МЧС России принимало участие в разработке этой концепции. В настоящее время оба ведомства полным ходом работают над её реализацией.

Содержательные линии были определены по-новому.

Первый момент: прежде изучение чрезвычайных ситуаций основывалось на классификации по источнику их возникновения, что очень важно для специалистов МЧС России, но бесполезно и неинтересно для детей. Новый подход основан на специфике детской жизнедеятельности, где ребёнок бывает, с чем сталкивается в процессе развития, какие задачи решает. Как вести себя, какие опасности могут быть дома, на природе, в школе, в общественных местах,

Большинство экспертов отмечают перенасыщенность курса ОБЖ критическими угрозами, вероятность наступления которых не очень велика. Напротив, минимум информации об угрозах, которые сопутствуют обычной повседневной жизни.



Обсуждение культуры безопасности на форуме «Цифровая гигиена. Молодёжь в сети». Фото: digital-gigiena.ru

в транспорте, в сети Интернет? Проблематика и её изложение должны быть понятными и интересными. Социальные сети выступают одним из мест «нахождения» ученика наряду с домом, школой, улицей, транспортом, природой и т.п. Таков принцип построения учебного материала согласно новой концепции ОБЖ.

Второй важный момент реализации новой концепции — перемещение фокуса внимания с самих чрезвычайных ситуаций на комплекс алгоритмов поведения, помогающих избежать подобных критических инцидентов. Затем — обучение, что делать, если такой инцидент всё-таки произошёл. Для старшеклассников и далее важно понимание роли государственной политики и управления в обеспечении безопасности жизнедеятельности.

Третий важный момент модернизации курса ОБЖ — знакомство учащихся, применительно к собственному опыту, с универсальными, общими правилами безопасности:

- ♦ лучший способ выйти из сложной ситуации — в неё не попасть;
- ♦ готовиться к сложной ситуации нужно заранее;
- ♦ недостаточно только знать правила безопасного поведения, нужно уметь их применять и

своевременно, и правильно действовать в ситуациях опасности;

- ♦ кто-то должен знать, где ты и когда вернёшься — чтобы прийти на помощь, если что-то пойдёт не так;
- ♦ что-то новое (среда, люди, интернет-сообщества и т.д.) всегда требует проверки.

В отдельное направление, в целый блок, выделяется первая помощь. Формируется установка не только на здоровье и безопасность, но готовность к взаимопомощи, прийти на помощь другому человеку.

* * *

МЧС России участвует в формировании и развитии единой методической базы для новых учебных программ, учебников и пособий, учебных материалов. К работе над базой привлекаются эксперты из разных областей. МЧС России выступает как главный оператор этой работы. Эта методическая основа как для повышения профессионального мастерства педагогов ОБЖ, так и для использования ими в учебном процессе. Обновлённый предмет ОБЖ будет современный, интересный, практически полезный и для молодёжи модный.



Марина БРОДСКАЯ
обозреватель BIS Journal

ХАКЕРЫ- «ПРОСВЕТИТЕЛИ»

КТО ОБУЧАЕТ НАСЕЛЕНИЕ АЗАМ ИБ?

Взрывы газа в жилых домах, необходимость регулярной проверки приборов учёта воды и электроэнергии, грядущий капитальный ремонт дома или социальные программы помощи людям старшего возраста — это поводы для мошенников, использующих методы социальной инженерии, заработать на доверчивых гражданах. И если в реальных условиях обмануть становится всё сложнее, то в виртуальном пространстве способов быстрого и, главное, результативного обогащения, всё больше с каждым днём. Однако никакой разъяснительной работы с экранов телевизоров или страниц газет не ведётся — огромная часть населения вынуждена учиться основам информационной безопасности на собственном печальном опыте.

ТЫ ПОМНИШЬ, КАК ВСЁ НАЧИНАЛОСЬ?

Вы помните, как начинались первые атаки мошенников на мобильные телефоны граждан? С попыток симитировать короткое сообщение, пришедшее якобы от платёжной системы, о зачислении средств на счет номера мобильного телефона. И второй смски следом — якобы от гражданина, совершившего ошибочный платёж, мол, промахнулся цифрой, зачисляя средства на номер родственника... Далее следовала просьба вернуть средства

на номер другого оператора связи. Со временем операторы мобильной связи усовершенствовали сервисы оповещения, а доверчивые обладатели мобильных телефонов научились проверять баланс и не бросаться переводить деньги на счета незнакомцев. Упростилась и процедура возврата средств, ошибочно зачисленных на чужие номера. Но до сих пор на телефон иногда приходят смски «Вам зачислено XXX рублей», «верните их, пожалуйста, на номер YYY»...

Прогресс не стоит на месте: пока одни участники процесса думают, как заткнуть одну дыру в безопасности, мошенники находят новые. Фишинговые ссылки на поддельные сайты банков, заражённые мобильные приложения... Главной целью хакеров, как и прежде, являлся сбор данных и кража средств со счетов. Со временем и в этом направлении ситуация улучшилась — заражённых или поддельных приложений стало меньше, а усилий банков по защите средств вкладчиков — больше.

Отдельно можно выделить «нигерийские» письма с реквизитами банков в Лесото или Вьетнаме. На кого рассчитаны малограмотные письма якобы от африканских юристов, жаждущих всучить вам чужое наследство или часть транша Мирового банка? Ведутся ли получатели на такой развод — неизвестно, но письма от «юристов» с просьбой

указать номера банковских карт для получения причитающихся средств приходят регулярно.

Другой вариант, уже более опасный для клиентов банков, — уведомления о зачислении платежа из неизвестных источников. Для окончательного получения рекомендуется перейти по ссылке. Что или кто за ней скрывается — для получателя неизвестно. Это может быть, как реклама некой фирмы, которая «научит» как регулярно получать такие переводы, или ссылка на вирус, который удачно загрузится на мобильное устройство и получит полный доступ к мобильному банку и средствам на счету.

ОТ СТАРОГО К МАЛОМУ

Несколько лет назад крупные банки России выдали банковские карты многочисленной армии пенсионеров, не проводя при этом никакой разъяснительной работы, в том числе и по мерам информационной безопасности. И старая шутка про пожар на телефонной станции, из-за которого надо накрыть мокрой тряпочкой телефонный аппарат дома, приобрела новое звучание. Резко выросло число граждан, которые повелись на вишинг — голос в телефоне, который сообщал, что доступ к счету клиента банка получили мошенники, и, назвав номер карты и цифры на обороте, деньги можно спасти... Сколько пенсионеров попало на эту удочку и лишилось накоплен-

ных средств, доподлинно неизвестно. Люди бегали с заявлениями о краже денег между отделениями банков, где открывали счет, и отделениями полиции, и всюду им отказывали в помощи, отправляя в другое ведомство.

В интервью BIS Journal (№ 2/2019) первый заместитель директора Департамента информационной безопасности Банка России Артём Сычев отметил, что «раньше основной группой риска всегда были пожилые граждане — клиенты банков. Сейчас они научились распознавать мошенников и давать им достойный отпор. Но пошла другая волна, под прицелом злоумышленников оказались граждане от 28 до 40 лет. Почему? Они иначе относятся к информационным технологиям, слишком им доверяют. Фокус внимания в нашей разъя-

нительной работе будет смещён на эту категорию и на молодёжь, которая ещё больше доверяет IT, не очень понимая, как они работают».

Да, ценой многочисленных ошибок и финансовых потерь пенсионеры получили знания по ИБ. А новая разводка явно рассчитана на молодое поколение.

Зимой 2018/2019 гг. стало известно о новом мошенничестве — атакам с подменой номера подверглись клиенты банков из ТОП-10. Звонки с номеров, определяемых как номера горячих линий банков, знание оператором всех персональных данных клиента и, нередко, сумм на счету, звуки колл-центра на заднем плане, уверенный тон, владение профессиональной лексикой и упоминание «информационной безопасности» ввели в заблуждение многих.

Сообщения о попытках снять деньги со счета после убедительного разговора с «сотрудником банка» посыпались одно за другим в социальных сетях. Кто-то успел остановиться в последний момент, кого-то остановили родные, оказавшиеся свидетелями разговора, а кто-то остался без денег...

В комментариях многие винили сотрудников банков в нечистоплотности, которая привела к утечке данных клиентов. В новостной ленте появились предположения экспертов компании DeviceLock, что масштабная атака стала возможной благодаря кратковременному доступу злоумышленников к внутренней информации банков. Внятных объяснений ни со стороны банков, ни со стороны операторов связи на момент написания статьи никто не дал.



Ирина МЕЛЬНИКОВА
менеджер Отдела
киберкультуры
Сбербанка

ШАГ ЗА ШАГОМ, ПОТИХОНЬКУ

В СБЕРБАНКЕ ПОЖИЛЫХ ЛЮДЕЙ УЧАТ ПРИЁМАМ ФИНАНСОВОЙ САМООБОРОНЫ

От действий «социальных инженеров» в первую очередь страдают самые доверчивые — пожилые люди. Они легко идут на контакт, когда им предлагают помощь, т.к. часто действительно в ней нуждаются. Ситуацию усугубляет и то, что и потерю денег, и сам факт обмана они воспринимают особенно тяжело.

Преступления, совершаемые путём социальной инженерии, нужно и можно предотвращать. И тут задача банка — научить клиента простым правилам безопасности при использовании банковских продуктов и услуг. Сбербанк системно занимается повышени-

ем киберграмотности всех клиентов, но люди «серебряного возраста» — одна из главных наших аудиторий.

ИНСТРУМЕНТАРИЙ

Инструментов, которые помогают нам повышать киберграмотность населения, довольно много. Для старшего поколения Сбербанк разработал специальную программу, которая называется «Активный возраст». На сайте программы размещён курс по финансовой грамотности, который учит в том числе и защите от мошенников.

Другой инструмент — видеоролики. Они демонстрируются в отделениях банка и дают чёткие ответы

на актуальные вопросы финансовой безопасности. Как правильно пользоваться банковской картой, мобильным и интернет-банком? На какие уловки идут кибермошенники? Как распознать мошенничество и что делать, если злоумышленникам всё же удалось добыть своего?

Любые знания важно закреплять с помощью проверок, поэтому мы часто предлагаем клиентам пройти несложные тесты. Поиск новых форматов ведётся постоянно. Например, в апреле Сбербанк начал проводить в своих московских офисах образовательные встречи с пожилыми клиентами. Сотрудники банка рассказывают о правилах ки-

ЧТО ДЕЛАТЬ, КОГДА НИКТО НЕ ВИНОВАТ?

На детском ТВ несколько лет живёт персонаж Аркадий Паровозов. Он спешит на помощь попавшим в беду детям и рассказывает об элементарных правилах безопасности в быту, на улице и в природных условиях. Дальше за просвещение подрастающего поколения берутся в школе, где детям, помимо, например, основ правил дорожного движения, дают основы безопасного поведения в интернете и — намного реже — информационной безопасности, как её принято понимать в ИБ-сообществе. Если в будущем школьник не пойдёт учиться по направлению IT или ИБ, то образование в этой сфере завершится, практически не начавшись. Пенсионерам же на всевоз-

можных курсах активного долголетия (иногда) дают азы компьютерной грамотности, но не информационной безопасности.

Почему на телевизионных каналах наряду с массовой рекламой банковских услуг не крутятся ролики о том, как можно (и нужно) обезопасить свои средства в тех же самых банках? Почему в самих банках клерки, открывая счет и выдавая пластик, предлагают оформить страховку на случай хищения средств со счета, но не выдают хотя бы брошюру с описанием действий, которые можно произвести по счету с помощью простейшего кнопочного телефона? Сколько клиентов крупнейших банков знают о USSD-кодах и их возможностях для доступа к счету с мобильного телефона? Попро-

сов много, ответов нет — зачем тратить на фактически социальную рекламу?

А тем временем Федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика России» ставит целью к 2024 г. повысить грамотность в сфере информационной безопасности, медиапотребления и использования интернет-сервисов 50 % граждан из числа тех, кто этими сервисами пользуется. 97 % постоянных пользователей интернета должны использовать средства защиты информации. До наступления 2024 г. осталось меньше пяти лет.



Пример обучающего материала Сбербанка по теме «Социальная инженерия»

бербезопасности в сфере личных финансов и отвечают на вопросы. Важность личного общения трудно переоценить — ведь только так мы можем понять, насколько эффективна наша работа.

ОБРАТНАЯ СВЯЗЬ

Обратная связь может быть самой неожиданной. К примеру, мы рассказываем о том, что нельзя записывать ПИН-код на бумажке, а в ответ слышим от старушки: «Да знаю я, что нельзя, а что же мне делать, раз у меня склероз...». Действительно, дорога от знаний к навы-

кам может быть очень долгой и тернистой, особенно для пожилых людей. Однако одолеть этот путь необходимо.

ПРОСТЫЕ ВЕЩИ

Мы учим наших пожилых клиентов очень простым вещам. Например, всегда внимательно относиться к звонкам незнакомцев, никому не сообщать подтверждающие коды из СМС, ПИН- и CVV-коды от банковских карт, не хранить ПИН-код вместе с картой, прикрывать клавиатуру рукой при вводе ПИН-кода, использовать только офици-

альные банковские приложения Сбербанка из App Store, Google Play и Microsoft store, не переходить по ссылкам в подозрительных СМС-сообщениях и письмах.

СПЕЦСЕРВИСЫ

Кроме того, Сбербанк разрабатывает специальные сервисы, которые помогают пожилым людям защитить свои деньги. Например, в web-версии Сбербанка Онлайн можно ввести ограничения на сумму переводов. И если злоумышленник получил доступ к интернет-банку клиента, большая добыча ему не светит. А совсем недавно появилась возможность сделать свои счета «невидимыми»: скрыть их во всех удалённых каналах обслуживания. Разумеется, мы рассказываем клиентам об этих дополнительных способах защиты и учим ими пользоваться.

Наш опыт показывает, что вся эта просветительская работа приносит результаты. Конечно, сложившуюся ситуацию невозможно изменить в одночасье — так, чтобы все клиенты тут же стали абсолютно киберграмотными, а «социальным инженерам» пришлось искать другие занятия. Однако пожилых людей, которые освоили и научились применять навыки «финансовой самообороны», становится всё больше.



Валерий КУЛИКОВ
обозреватель BIS Journal

ЧТО НАМ МЕШАЕТ ОБУСТРОИТЬ ИТ- И ИБ-ОБРАЗОВАНИЕ?

ШЕСТЬ ЭЛЕМЕНТОВ РУКОТВОРНОГО ХАОСА

Прошедший год стал, похоже, отправной точкой для осознания, что ИТ — это та сфера, откуда отрасль ИБ должна черпать свои кадровые резервы. Единственным препятствием может оказаться царящий в системе ИТ-образования и вокруг неё рукотворный хаос. Посмотрим на его элементы.

ПРО ЦИФРЫ И СРАВНЕНИЯ

На последнем заседании Комитета АПК-ИТ по образованию в очередной раз били в набат: ИТ-отрасли грозит кадровый коллапс! Откуда же такой тезис взялся?

Вывод о дефиците кадров в данном конкретном случае был сделан в том числе на основе того, что в России доля трудоспособного населения, «занятого» в сфере ИТ (в докладе приводится цифра 1,5%), в четыре раза меньше, чем в Великобритании.

Эффектные сравнения с зарубежными странами у нас популярны и, наверное, поэтому серьёзными аргументами их считать трудно. Например, по данным Фонда развития интернет-инициатив (ФРИИ) доля ИТ-специалистов в России составляет 2,4% от всего занятого населения, а в США, Германии и Великобритании этот показатель — 4,3%.

Так сколько же в России ИТ-специалистов — 1,5 или 2,4%? И сколько в Великобритании — 6 или 4,3%? Да и нуж-

но ли именно так оценивать потребность нашей страны в ИТ-специалистах? Тем более, что со статистикой у нас сегодня действительно не всё в порядке. Руководителя Росстата сменили, у национальной программы «Цифровая экономика РФ» тоже новый руководитель. А значит, и цифры скоро будут совсем другие.

ОТКУДА ВЕТЕР?

Так откуда ветер дует? Очень просто: в России есть очень крупные ИТ-компании («Лаборатория Касперского», «1С» и др.), и есть солидная прослойка ИТ-СМБ-компаний. Они и жалуются (очень громко, потому что у них есть такая возможность) на дефицит кадров. Но их дефицит специалистов принципиально отличается от кадровой проблемы России в целом. Они отлично знают, сколько и каких специалистов им требуется, и справляются с этим самостоятельно вполне успешно.

А В РОССИИ...

А в России в целом нет понимания и даже полноценного описания, что представляет из себя ИТ-отрасль, не говоря уж об её кадрах в количественном и качественном измерениях.

Характерная цитата: «Сейчас в России 1,9 млн ИТ-специалистов, из них лишь 380 тыс. — разработчики ПО, подсчитали в Фонде развития интернет-инициатив. Остальные — систем-

ные администраторы, тестировщики, специалисты по безопасности, консультанты ПО, администраторы баз данных, администраторы сетей, архитекторы сетей...»¹.

Подобных бессмысленных высказываний много. Из них (в разных вариациях) следует, что в России проблема только с «разработчиками ПО». А «тестировщики, специалисты по безопасности, архитекторы сетей»... эти и многие другие специальности и специализации не нужны? Или то ли нужны, то ли не нужны...

А каковы потребности ИТ-отрасли в специалистах по аппаратным платформам и разработке ПО для такого специфичного, но массового класса ИТ-оборудования, как встроенные (embedded) системы? Эта тема в явном виде в объёмах, достойных её экономической и оборонной значимости, даже не отражена в программе «Цифровая экономика РФ», и уж тем более и близко не находит своего отражения в кадровых «стенаниях».

ВСЁ БЫСТРО МЕНЯЕТСЯ!

Следующий аспект. Цитата: «ИТ — это очень быстро меняющаяся сфера деятельности. Одна технология, не успев прочно закрепиться на рынке, уже вы-

¹ <https://vc.ru/flood/32575-frii-predupredil-o-nehvatke-it-specialistov-v-rossii>

тесняется другой, постоянно выходят новые версии существующих фреймворков и внедряются новые решения. Знания и опыт, которые вы получили сегодня, через 10 лет будут никому не нужны».

Приведённая цитата настолько же верна, насколько и банальна, поэтому нет нужды приводить источник. Но это «откровение» позволяет прийти к мысли о бессмысленности и вредности погони за кадровыми «хотелками» как лидеров, так и рабочих лошадей отечественного ИТ-рынка. Эти пожелания по большей части эгоистичны и сиюминутны. Вот типичные примеры:

«Сейчас у нас большой запрос на разработчиков и аналитиков Siebel, что связано с активным ростом направления внедрения и развития CRM-систем...».

«Традиционное обучение идёт вразрез с потребностями рынка, где всё больше востребованы молодые специалисты с современным стеком технологий: Go, Java/Spring, Scala, Python/Big Data, Swift и другими...».

Ну, что сказать? Siebel, конечно, неплохая CRM-система, но это лишь одна из таких систем. А стек технологий, безусловно, модный и трендовый... Но как сложится судьба молодёжи, которая поступится ценностями «традиционного обучения» во имя скорейшего освоения сиюминутного «стека технологий»? Если (повторимся): «Одна технология, не успев закрепиться на рынке, уже вытесняется другой». И, добавим, интересы бизнеса компаний также волатильны.

СТАНДАРТЫ? ХМ...

Сегодня во главу угла решения образовательных и кадровых проблем поставлен процесс написания проф- и обрстандартов. Но чем, скажите, в реальном мире отличаются обладатели дипломов «Информационная безопасность» и «Компьютерная безопасность»? А ведь это два разных ФГОС!

Понятно, что ФГОСы нужны, но трудно представить, что в СССР во времена индустриализации, становления атомного флота или реактивной авиации затеяли подобные игрища. Скорей всего нам не пришлось бы экспортировать РД-180 в страну, где была сделана

Чем, скажите, в реальном мире отличаются обладатели дипломов «Информационная безопасность» и «Компьютерная безопасность»? А ведь это два разных ФГОС!

ракета для лунной программы, и конкурировать с этой же страной на рынке производства атомного топлива.

В США местный апологет североамериканского ЕГЭ развенчан и только что не судим (пока)! «Жёлтые жилеты» во Франции возмущены не только ценами на горючее, но и развалом образования! А в нашей стране, чью систему образования некогда копировали в обеих америках, персоны, принимающие решения, озабочены латанием отсталой системы ЕГЭ, тогда как лица, которым отказано в возможности влиять на образовательную политику, занимаются партизанщиной, втихую создавая факультеты СПО при вузах!

На одном из Интернет-форумов довелось прочесть, что раньше получали деньги для строительства дорог, а теперь дороги строят для получения денег. Похоже, это справедливо не только для дорожного строительства. Предложено, например, создать Фонд высшего образования. В обоснование приводятся красивые слова о том, что вкладчики Фонда смогут оплатить высшее образование детей, заключив фьючерсный контракт и оплачивая обучение за три года до, четыре года во время обучения и год после. Однако что-то подсказывает, что ключевыми в этом предложении являются слова «Фонд будет действовать под управлением профессиональных инвесторов».

ВЫ НЕ АГРОНОМ?

А могут ли кураторы российского ИТ-образования взглянуть на его проблемы иначе, чем через призмы венчурных фондов, фьючерсных контрактов и отчётов Gartner? Вряд ли. Рабочая группа, созданная для решения кадровых проблем в рамках программы «Цифровая экономика РФ», лишь на четверть укомплектована «представителями бизнеса, экспертного сообщества и органов власти», имеющими отношение к вузам. Больше 70 % лиц даже формально не отягощены опытом препода-

вательской или научной работы, хотя, несомненно, молоды и являются управленцами новой формации.

И в чём тут беда? Чем плохи бизнесмены? Может, и не плохи, однако слишком часто они оценивают возможности решения инженерных проблем с позиций оценки рисков, что является стреноживающим фактором для инженерного поиска и может негативно повлиять на формирование будущих ИТ-инженеров и специалистов по ИБ. Другим недостатком «бизнесменов и управленцев» является заложенная в них ab initio установка на ведомый характер отечественных специалистов в мировом разделении труда. Тот самый подход, когда наше дело — «успеть вскочить на подножку уходящего поезда».

Принятие подобной установки за аксиому нельзя признать обоснованным. Как нельзя согласиться с искусственным устранением преподавателей-профессионалов от подготовки специалистов для ИТ&ИБ.

НАРОЧНО НЕ ПРИДУМАЕШЬ

Не так давно CNews сообщил, что Рособrnadzor отказал в аккредитации факультету СПО при ИТМО. ИТМО подавал заявку на аккредитацию по укрупнённой группе профессий 09.00.00 «Информатика и вычислительная техника» в сфере среднего профессионального образования. По данным CNews, отказ в аккредитации был обоснован отсутствием необходимой инфраструктуры, в частности, на арендованном вузом стадионе нет полосы препятствий! Замечаний по заявленным образовательным программам у экспертной группы Рособrnadzora не нашлось.

Так может всё же при решении проблем образования стоит передать эту тему на откуп профессионалам, а не организовывать им соревнования по преодолению полосы препятствий?

**Екатерина ЗОБОВА**

сотрудник Фонда содействия развитию
безопасности информационных
технологий (ФСРБИТ)

НАКАНУНЕ

НАЧИНАЕТСЯ ВСТУПИТЕЛЬНАЯ КАМПАНИЯ 2019.
ВСПОМНИМ, КАК ЭТО БЫЛО В 2018-М

По итогам 2018 года в Москве порядка 20 государственных вузов принимали абитуриентов для обучения специальности «информационная безопасность», «компьютерная безопасность», «информационная безопасность автоматизированных систем». Всего на столицу было чуть более 500 бюджетных мест. Для сравнения в МГУ им. Ломоносова на специальность «фундаментальная математика и механика» ежегодно набирается 380 абитуриентов.

ОГРОМНЫЙ КОНКУРС

Конкурс на бюджетные места по специальности «информационная безопасность» высокий во все высшие учебные заведения. Однако в некоторые вузы он и вовсе космический.

В МЭИ в 2018 году на 20 бюджетных мест претендовало 1383 абитуриента. Конкурс составил 69,15 человека на место. И это не самый высокий результат.

Его побил Московский политех, где на те же 20 мест претендовало уже 1500 абитуриентов. А это уже 79,35 человека на место. Не намного ниже показатели у МТУСИ. Университет в 2018 году набирал 33 студента по специальности

«информационная безопасность». Было подано 2416 заявлений (73,21 человек на место). Поступить смогли абитуриенты, по результатам трёх экзаменов ЕГЭ, имевшие 236 баллов и выше.

ВЫСОКИЙ ПРОХОДНОЙ БАЛЛ

Из-за большого конкурса на специальности, связанные с информационной безопасностью, высокий проходной балл практически во всех высших учебных заведениях.

Одним из рекордсменов по данному показателю в 2018 году выступил НИЯУ МИФИ. На 20 бюджетных мест претендовало 368 человек. Чтобы поступить в данный вуз на ИБ, за три экзамена ЕГЭ студенты должны были набрать 276 баллов.

И это ещё «цветочки» по сравнению с МГТУ им. Баумана, где на специальность «Информационная безопасность автоматизированных систем» (10.05.03) проходной балл составил 298 (!).

Неожиданно высокий проходной балл в 2018 году был в РГЛУ — 259, всё-таки лингвистический университет больше славится своими специалистами в гуманитарной сфере. Тем не менее, вуз набирал 14 студентов на специаль-

ность «информационная безопасность». Конкурс составил 28,36 человека на место.

В другие высшие учебные заведения проходной балл колебался в районе 250 баллов. Один из самых низких результатов по данному показателю у РГСУ — 188 баллов. Университет набирал в прошлом году на ИБ 35 студентов.

ПЛАТНО ДОРОГО

Высокий конкурс и проходной балл обуславливают и высокую стоимость обучения на договорной основе. Здесь тоже есть свои лидеры.

В РЭУ им. Плеханова за год обучения по специальности «информационная безопасность» нужно платить 260 тысяч рублей в год. Проходной балл здесь летом оказался столь же высоким, как и в технические вузы — 255 баллов, а конкурс составил 24,15 человек на место.

Впрочем, в 2019 году цены в РЭУ, похоже, побьёт Высшая школа экономики. Чтобы обучаться в МИЭМ НИУ ВШЭ на платной основе, необходимо будет платить 400 000 рублей в год. Летом абитуриенты на специальность «информационная безопасность» будут набираться впервые. Ранее была



КОМИТЕТ
ОБЩЕСТВЕННЫХ СВЯЗЕЙ
И МОЛОДЕЖНОЙ ПОЛИТИКИ
ГОРОДА МОСКВЫ

Публикация подготовлена в рамках проекта «Безопасность цифровой экономики Москвы: Новое поколение», поддержанного грантом Мэра Москвы №085-МГ/18

только «компьютерная безопасность». В 2018-м в МИЭМ было чуть-чуть дешевле. Стоимость обучения по договору составляла 315 тысяч рублей в год.

Не так дорого поступать в МАИ. Институт выпускает ежегодно 40 специалистов по информационной безопасности. Проходной балл в прошлом году на бюджет составил 246 баллов, а стоимость обучения по договору — 150 тысяч рублей в год.

Московский государственный университет геодезии и картографии предлагает обучаться ИБ за 176 тысяч рублей в год. Конкурс в данный вуз в 2018 году на бюджет составил 24 человека на место, проходной балл — 226.

САМЫЙ БОЛЬШОЙ ПОТОК

Наибольшее число специалистов по ИБ на бюджетной основе выпускает, как ни странно, Финансовый университет при Правительстве РФ — 42 человека в год. Проходной балл здесь довольно высокий — 255. При этом конкурс «все-го» 7,17 человек на место. В 2018 году в университет на специальность «информационная безопасность» было подано 301 заявление. Стоимость обучения по договору составила 230 тысяч рублей в год.

По 40 бюджетных мест в МАИ и РТУ МИРЭА. В последнем конкурс в 2018 году составил 38,8 человек на место, было подано 1552 заявления (проходной балл — 245).

В среднем же вузы набирают на специальность «информационная безопасность» по 20 студентов. В МИИТ конкурс на 17 бюджетных мест составил 25,76 человек. Также информационной безопасности обучают в РГГУ. Здесь выделено 27 бюджетных мест. Конкурс — 21 человек на место. При этом проходной балл — 218. Национальный исследовательский университет МИЭТ набирал в 2018 году 25 абитуриентов на ИБ. Конкурс составил 14 человек на место. А проходной балл — 248. Обучение по договору стоило 200 тысяч рублей в год.

НОВЫЕ ФАКУЛЬТЕТЫ

Потребность в специалистах в области информационной безопасности чувствуют и другие московские вузы. В РТУ им. Губкина в феврале 2018 года



Финансовый университет при Правительстве РФ выпускает наибольшее число специалистов по ИБ на бюджетной основе — 42 человека в год

был создан целый факультет — комплексной безопасности ТЭК, что «явилось ответом на обращение компаний отрасли, обеспокоенных сохранением в безопасности своих объектов и минимизации возможного ущерба в условиях цифровизации современного общества», говорится на сайте университета.

Впервые в 2019 году будет набирать студентов на специальность «информационная безопасность» и Высшая школа экономики. До этого МИЭМ вел набор только на специальность «Компьютерная безопасность».

В СТОРОНЕ

Особняком в ряду вузов, предлагающих обучение по специальности ИБ, стоят МГУ им. Ломоносова и Академия ФСБ России.

На факультете ВМК в МГУ с 2013 года функционирует Кафедра информационной безопасности. Однако студенты официально получают образование по специальностям «прикладная математика и информатика», «фундаментальная информатика и информационные технологии». Для поступления в МГУ помимо русского, физики и математики нужно сдавать ЕГЭ по информатике, а также внутренний экзамен по математике.

Также два внутренних экзамена (физика и математика) в Институте криптографии, связи и информатики.

Здесь у студентов есть возможность обучаться специальностям «Компьютерная безопасность», «информационная безопасность автоматизированных систем». Отметим, что готовиться поступать в ИКСИ абитуриенту нужно ещё в 10 классе. Подробнее о поступлении в вуз можно прочитать на официальном сайте института.

ПОДВОДЯ ИТОГИ

◆ Несмотря на то, что вопрос информационной безопасности компаний в мире стоит достаточно остро, вузы готовят не так много специалистов в данной отрасли.

◆ По сравнению с прошлыми годами число бюджетных мест в вузы на специальности, связанные с информационной безопасностью, растёт, но не так существенно, чтобы решить проблему нехватки кадров.

◆ Всё больше непрофильных вузов предлагают студентам обучение специальности «информационная безопасность». Правда, здесь уже встаёт вопрос квалифицированности выпускаемых этими учебными заведениями специалистов.

◆ Стоимость обучения по договору и конкурс на ИБ очень высоки, поэтому абитуриентам заранее стоит задуматься о поступлении в вузы через олимпиады или целевой набор, чтобы увеличить шансы на поступление в желаемый вуз.



**Марина
БРОДСКАЯ**
обозреватель
BIS Journal

МИРОВАЯ ПРОБЛЕМА

НА ПОМОЩЬ УНИВЕРСИТЕТАМ СПЕШАТ
ИНТЕГРАТОРЫ, ГУБЕРНАТОРЫ И СПЕЦСЛУЖБЫ

По расчетам Федерального учебно-методического объединения по информационной безопасности, к 2022 г. в России должно втрое вырасти число выпускников университетов по специальностям в сфере ИБ. Но откуда они возьмутся, если прием в вузы и колледжи в настоящее время составляет порядка 7 тыс. человек в год и не увеличивается? Ответа нет. А пока его нет, давайте посмотрим, что происходит за рубежом. По прогнозам аналитической компании Cybersecurity Ventures, к 2021 г. дефицит кадров в области ИБ в мире приведет к 3,5 млн вакантных рабочих мест. Поэтому поиск различных методов подготовки специалистов является главной темой многих конференций и собраний по кибербезопасности не только в России.

ФИЛИППИНЫ

Компании и предприятия Юго-Восточной Азии страдают от киберпреступников больше остальных. Это связано с особенностями межрегиональных взаимосвязей и отсутствием согласованности в методах регионального управления. По данным «Лаборатории Касперского» за 3 квартал 2018 г., Филиппины входят в десять стран, более других подверженных онлайн-атакам. Страна есть и в первой десятке рейтинга Global Terrorism Index 2018, составленного Институтом экономики

и мира. Такие показатели отпугивают потенциальных инвесторов и служат серьезным препятствием для переноса бизнеса на Филиппины.

Усилий правительства, утвердившего Национальный план кибербезопасности до 2022 г., явно не хватает. В период с 2017 по 2025 г. необходимо инвестировать в ИБ страны порядка \$67 млрд чтобы вывести Филиппины хотя бы на средний уровень киберугроз. Еще больше средств требуется для решения местных проблем, в числе которых — нехватка квалифицированных кадров. Департамент информационных и коммуникационных технологий Филиппин координирует свою деятельность с Министерством образования. Большую надежду возлагают на частный AMA Computer University (AMACU), который планирует выпускать бакалавров в области кибербезопасности на основе учебной программы, разработанной совместно с Минобороны США и Европейским центром по изучению проблем безопасности им. Джорджа Маршалла Федерального министерства обороны Германии.

Пока идут согласования, интегратор Level 11 Tech предлагает решать проблему кадрового голода с помощью платформы для обучения и тренировок Cyberbit Range, разработанной компанией Cyberbit. Эта разработка — ключевой компонент многих академических программ по кибербезопасности в мире. Cyberbit Range, адаптированный к раз-

личным уровням опыта и должностных функций, представляет собой учебную платформу, которая имитирует широкий набор кибератак в контролируемой среде. Платформа позволяет организациям создавать гиперреалистичные учебные центры, что способствует повышению эффективности работы команд специалистов в области ИБ.

Обучение в таких центрах идет по нарастающей — от начального до продвинутого уровня. Участники — специалисты по различным направлениям, включая команды реагирования на инциденты, аналитиков, руководителей предприятий и студентов, — могут узнать, что такое настоящая кибератака и как ей противостоять. Платформа также дает возможность встроить элементы ИБ в курс классического программирования, пройти упражнения по киберсимуляции в любой из учебных программ по ИБ. По утверждению Level 11 Tech, помимо Филиппин, платформа доступна для Азиатско-Тихоокеанского региона еще в Сингапуре и Индии. И прошедшие полный курс обучения на ее базе по уровню подготовки якобы не уступают выпускникам лучших университетов мира.

Пишут, если технология от Cyberbit получит пропуск в филиппинские университеты и войдет в программу высшего образования, то филиппинские эксперты в области ИБ станут конкурентоспособными на мировом уровне. Стоит отметить, что Cyberbit при-



КОМИТЕТ
ОБЩЕСТВЕННЫХ СВЯЗЕЙ
И МОЛОДЕЖНОЙ ПОЛИТИКИ
ГОРОДА МОСКВЫ

Публикация подготовлена в рамках проекта «Безопасность цифровой экономики Москвы: Новое поколение», поддержанного грантом Мэра Москвы №085-МГ/18



Азиатско-Тихоокеанский университет (Малайзия) запускает программу CyberSecurity Talent Zone (фото: easyuni.com)

существует и в России, однако широкого распространения учебная платформа Cyberbit Range у нас не получила.

МАЛАЙЗИЯ

В отличие от филиппинских коллег, которые только разрабатывают свои программы по ИБ, сотрудники Азиатско-Тихоокеанского университета (APU) уже демонстрирует сильные стороны малайского образования в области кибербезопасности. В университете есть материальная база, квалифицированные кадры, учебные планы и партнерские отношения с компаниями, специализирующимися на ИБ. Университет готовит бакалавров по направлениям «информационные технологии» со специализацией «безопасность информационных систем», «кибербезопасность», «криминалистические вычисления» и «компьютерные науки» с уклоном в цифровую криминалистику.

При поддержке отраслевых партнеров и Малайзийской корпорации цифровой экономики (MDEC) APU постоянно реагирует на потребность в талантах, стремясь обучать и воспитывать «супергероев» цифрового пространства. Отраслевая консультативная группа экспертов по кибербезопасности (в т.ч. CompTIA, ISACA, CSM, MDEC, TecForte, Cyber Test Systems, Cyber Intelligence и SecureKi) участвует в

корректировке учебной программы в APU, обеспечивая актуальность учебного плана.

В 2018 г. APU запустила первую в стране CyberSecurity Talent Zone, объединившую студентов, работающих с системами мониторинга кибербезопасности в реальном времени военного уровня, исследовательскими центрами и инфраструктурами моделирования, для развития глобальной кибербезопасности и IoT-талантов будущего.

Также создан Центр моделирования и реагирования на киберугрозы (Cyber Range) и Центр операций безопасности (SOC), который в режиме реального времени передает данные мониторинга, извлеченные из базы данных кибератак по всему миру, обеспечивая студентам уникальную базу для практической работы. На основе этих данных студенты APU учатся отслеживать, устранять неисправности, расследовать и решать проблемы, связанные с нарушением безопасности.

Малайский Азиатско-Тихоокеанский университет уже подготовил студентов, которые превосходят своих свер-

стников на соревнованиях международного уровня. Они имеют высшие награды на KPMG Cyber Challenge 2018, Азиатско-Тихоокеанского глобального хакатона Ernst&Young 2019 г., трижды становились чемпионами F-Secure Intervarsity Challenge, а на Cyber Challenge Heroes Challenge 2019 получили награду за самого ценного игрока (MVP). Выпускники APU работают в LGMS, FusionEx, Maybank, IBM, Accenture, Standard Chartered Bank...

США

Скандалы с атаками неизвестных хакеров на серверы компаний в США, громкие взломы последних лет постоянно напоминают американцам о необходимости образования в области ИБ. Еще в 2016 г. президент и генеральный директор колледжей и университетов профессионального образования (CECU) Стив Гандерсон заявил: «Если мы не примем меры и не подготовим студентов на пустующие рабочие места, мы будем регулярно читать о серьезных взломах». Поставщики специалистов по ИБ — колледжи и университеты, где

Малайский Азиатско-Тихоокеанский университет уже подготовил студентов, которые превосходят своих сверстников на соревнованиях международного уровня

В настоящее время в США действует 21 школа, в которых есть Центры академического мастерства в области киберопераций, поддерживаемые АНБ

открыто направление ИБ, — могут помочь обучить американцев навыкам, необходимым для борьбы с растущей угрозой киберпреступности.

На рынке труда США активно ищут профессионалов, готовых заняться защитой ИТ-инфраструктуры. Как отмечают рекрутеры, диплом выпускника колледжа или степень бакалавра в области компьютерных наук отлично подходит для старта карьеры в ИБ. Еще лучше, если образование в сфере информационных технологий сочетается с одним-двумя годами стажировки или опытом работы в области ИБ.

У окончивших курсы повышения квалификации в сфере ИБ и сдавших экзамены на сертификат больше шансов получить высокооплачиваемую работу с перспективой роста. Средняя зарплата аналитика ИБ составляет от \$63 тыс. на начальном уровне до \$91 тыс. на завершающем. Специалист в расцвете карьеры получает \$82–89 тыс. в год. По прогнозам, за 10 лет с 2014 по 2024 г. число вакансий аналитиков безопасности вырастет на 28%.

Все больше университетов заключают договоры с госструктурами или вступают в частно-государственное партнерство. Так, губернатор штата Луизиана в мае 2019 г. объявил о создании первого Учебного центра кибербезопасности штата. Центр создан по инициативе властей штата, общественного колледжа Bossier Parish и компании Cybint Solutions, которая специализируется на образовании в области ИБ. К подготовке учебных программ планируется подключить также местные технические университеты и профессиональное сообщество. Обучение будет проходить в режиме онлайн, приоритет — жителям штата. Сам центр расположится на территории колледжа и даст возможность обучения и повышения квалификации как для студентов, так и для специалистов по ИБ со всей Луизианы. Главной целью центра станет превращение

района Шривпорт-Боссье, где расположен центр, в киберцентр Луизианы. В планах — оказание всесторонней поддержки в области ИБ частным и государственным компаниям штата, создание т.н. «киберкоридора», центра для ориентированных на технологии бизнес-структур, учебных и исследовательских учреждений.

Онлайн-обучение по программе магистратуры для всех желающих предлагает и Кафедра электротехники и вычислительной техники Университета штата Айова. Программа состоит из 30 учебных часов в неделю, включая 18 ч. из основного набора курсов по направлению, 6 ч. на исследования и 6 ч. факультативных занятий. В обычный набор магистратуры входят углубленное изучение компьютерных сетей, компьютерная безопасность, информационные войны, этические и правовые проблемы компьютерной безопасности, а также 2 предмета из 4 по выбору: криптография, стеганография, криминалистика, безопасность беспроводных сетей. Факультативные предметы выбираются студентом из предложенного университетом списка программ других кафедр. Как проводится защита диплома, на сайте университета не уточняется.

А частный Университет Нью-Хейвена (Новая Англия, шт. Коннектикут) получил статус Национального центра академического мастерства в области кибербезопасности (CAE-CO), который присвоило ему Агентство национальной безопасности США. Подобная сертификация признает программы бакалавриата университета в области компьютерных наук, кибербезопасности и сетей.

В настоящее время в США действует 21 школа, в которых есть Центры академического мастерства в области киберопераций, поддерживаемые АНБ. Университет Нью-Хейвена стал вторым университетом в штате, получившим подобный статус. Программа

CAE-CO поддерживает национальную инициативу по образованию в области ИБ и ставит целью расширить круг специалистов по киберзащите. Программой предусмотрены углубленное изучение технических и междисциплинарных предметов на уровне высшего образования в области компьютерных наук, вычислительной техники и электротехники. Студенты получают новые возможности для применений знаний на лабораторных и практических занятиях.

Согласно данным Бюро статистики труда Министерства труда США, число рабочих мест в сфере компьютерных и информационных технологий с 2016 по 2026 г. возрастет на 13%. Это значит, что безработица среди специалистов по ИБ находится почти на нулевом уровне.

АФРИКА

Некоторые африканские страны всё ещё находятся под угрозой оказаться вовлечёнными в кибервойны и страдать от терроризма, если не будет разработана надлежащая инфраструктура и политика для устранения угроз ИБ. Об этом заявил Евгений Касперский на симпозиуме «Современные вызовы безопасности: африканская перспектива» в Руанде. Глава Лаборатории Касперского заявил, что уже созданы технологии защиты африканских инфраструктур, которые делают взломы более дорогими, чем вероятная прибыль хакеров, но её стоимость превышает возможности африканских стран и компаний. Касперский отметил, что оптимальный выход из положения — найти баланс в инвестировании в собственные системы, привлечь инженеров извне и развивать своё образование в области кибербезопасности.

Профессор Владимир Антви-Дансо из Ганы, специалист по ИБ и участник симпозиума, рассказал, как стал жертвой кибератаки с целью получения выкупа во время поездки в Канаду. Хакеры требовали от него \$40, которые профессор отказался платить и потерял всю информацию на ноутбуке.

Глава Службы национальной безопасности Руанды генерал-майор Джозеф Нзабамвита считает, что киберугро-



Fortinet объявил, что Университет Табук станет первым образовательным учреждением в Саудовской Аравии, которое войдёт в программу Академии сетевой безопасности Fortinet (фото: cxoinsightme.com)

зы стали орудием кибернетического терроризма. Выход из ситуации — инвестиции в ИБ-образование, поправки в законодательство, запрещающие распространение радикальных идей, в т.ч. через интернет, реформа судебной системы и просвещение судей в области ИБ. Генерал привёл пример невежества судейского корпуса, когда из 40 подозреваемых в терроризме, привлечённых к уголовной ответственности в 2018 году, только 18 человек были осуждены. Остальных подсудимых освободили, хотя их арестовали за радикальные высказывания в соцсетях и прямое планирование террористических атак, — судьи элементарно не разбирались в вопросах ИБ.

АКАДЕМИЯ FORTINET И ВСЬ МИР

Компания Fortinet, одна из ведущих компаний в области интегрированных и автоматизированных решений по кибербезопасности, расширяет Академию сетевой безопасности Fortinet

(FNISA). С начала 2019 г. в неё вошли 30 новых институтов, в т.ч. учебные заведения в Сингапуре, Перу и Бразилии. Вновь присоединившиеся к программе Академии учебные заведения смогут использовать комплексную платформу сетевой безопасности Fortinet для проведения занятий по сетевому администрированию и информационной безопасности.

Академия предоставляет своим партнёрам возможность обучения и сертификации специалистов по программе сетевой безопасности компании Fortinet, готовит студентов к практической работе в области сетевой безопасности. В курс Академии входят теоретические лекции и практические лабораторные работы. Учебные и сертификационные программы по ИБ разработаны для разной аудитории — старшеклассников, студентов колледжей и университетов. Цель Академии — дать слушателям те профессиональные навыки в ИБ, которые востребованы работодателями.

Академия работает в 60 странах (США, Канада, Австралия и Океания, страны Европы, Латинской и Южной Америки, Юго-Восточной Азии), охватывает 150 учебных заведений. Расширяя доступность программы Академии сетевой безопасности, Fortinet привлекает и обучает молодых специалистов в области ИБ и частично решает глобальную проблему нехватки кадров и слабой подготовки сотрудников компаний в сфере кибербезопасности.

В 2018 г. в России подготовили около 7 тыс. специалистов с высшим и средним образованием в области ИБ, в 2022-м выпускников должно быть около 21 тыс. Какие меры для этого принимаются, новостная лента умалчивает. Резкого роста числа университетов, выпускающих специалистов по ИБ, BIS Journal не наблюдает. Посмотрим, что будет осенью после вступительной кампании 2019 г.



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

ЗАВОД КУЛАКОВА

КАК В БЛОКАДНОМ ЛЕНИНГРАДЕ СОЗДАВАЛИ ШИФРОВАЛЬНУЮ ТЕХНИКУ

Среди современных петербургских предприятий хорошо известен приборостроительный завод им. А.А. Кулакова. Это один из старейших производителей техники связи в России. Уже в годы Первой мировой войны большинство военных судов Балтийского флота были оборудованы водонепроницаемой телефонией, всевозможными корабельными приборами управления, произведёнными именно на этом петроградском заводе. Ныне он известен и весомым вкладом коллектива своих работников в создание отечественной шифровальной и засекречивающей аппаратуры в годы Великой Отечественной войны.

«ДЛЯ ОСУЩЕСТВЛЕНИЯ СВЯЗИ ПО ФРОНТУ...»

До войны Завод им. Кулакова был ведущим предприятием страны по разработке и производству телеграфной техники. Достаточно указать созданный там аппарат СТ-35. Он устойчиво работал на линиях с пониженной изоляцией, в сырых и холодных помещениях, обеспечивал работу до 300 км. В силу этого он оказался весьма ценным для армии, где его стали применять в звеньях от армии к корпусу, от корпуса к дивизии и для осуществления связи по фронту. Возможность увеличения дальности действия СТ-35 до 600 км сделала его

одним из основных телеграфных аппаратов, принятых на вооружение войск связи РККА [1].

«ТЕХНИКА ОСОБОЙ СЕКРЕТНОСТИ»

Среди многих направлений работы завода особое место заняло участие в разработке шифровальной аппаратуры. Ещё в ноябре 1934 г. по заданию 8-го отдела Штаба РККА завод привлекли к новому делу — разработке шифровальной аппаратуры для телеграфных линий связи. Была сформирована группа инженеров В. М. Домничева, В. Н. Рытова, О. А. Примазовой и Е. П. Изотовой. К 1937 г. они разработали шифровальный комплект «В-4», который в мае 1938 г. был принят на вооружение РККА. Благодаря этому успеху, в составе завода, получившего номер — № 209, был образован Комбинат техники особой секретности. В него вошли отдел № 33 (включал КБ и лабораторию спецтехники) и сборочный цех спецтехники.

Новое подразделение завода сразу же приступило к работам по модернизации аппаратуры «В-4». Во второй половине 1938 г. двумя группами конструкторов (их возглавили В. Н. Рытов, П. А. Судаков и Н. М. Шарыгин) были разработаны два варианта для различных уровней управления армией и флотом. На их базе в 1939 г. была создана шифровальная машина «Изумруд», ко-

торая с 1940 г. также стала выпускаться заводом. В 1939 г. специалисты завода разработали кодировочную машину «Кристалл», пригодную уже для всех звеньев управления войсками, и создали шифрующие приборы-приставки к различным типам телеграфных аппаратов: С-306 — к аппарату Морзе, С-308 — к Бодо, С-309 — к СТ-35. Уже с третьего квартала 1939 г. началось серийное производство всех этих приборов. В 1940 г. под общим руководством П. А. Судакова на заводе разработали новый военный стартовый телеграфный аппарат «НТ-20» со съёмным шифрующим прибором-приставкой, тогда же принятый на вооружение армии.

Так, в последние предвоенные годы, завод № 209 превратился ещё и в один из ведущих центров по разработке и серийному изготовлению шифртехники [2, 4]. Уникальное место завода в этой сфере ярко обозначилось в годы Великой Отечественной войны.

ПРИКАЗАНО ПЕРЕЖИТЬ БЛОКАДУ

Перед началом войны, как известно, развернулось форсированное строительство флота. На обеспечение вступающих в строй судов средствами проводной и радиосвязи в значительной степени был ориентирован и Завод им. Кулакова. После перехода предприятия в ведение НКСП (Судпрома) про-



ФОНД
ПРЕЗИДЕНТСКИХ
ГРАНТОВ

Публикация подготовлена с использованием средств гранта Президента Российской Федерации на развитие гражданского общества №18-2-012576, представленного Фондом президентских грантов.

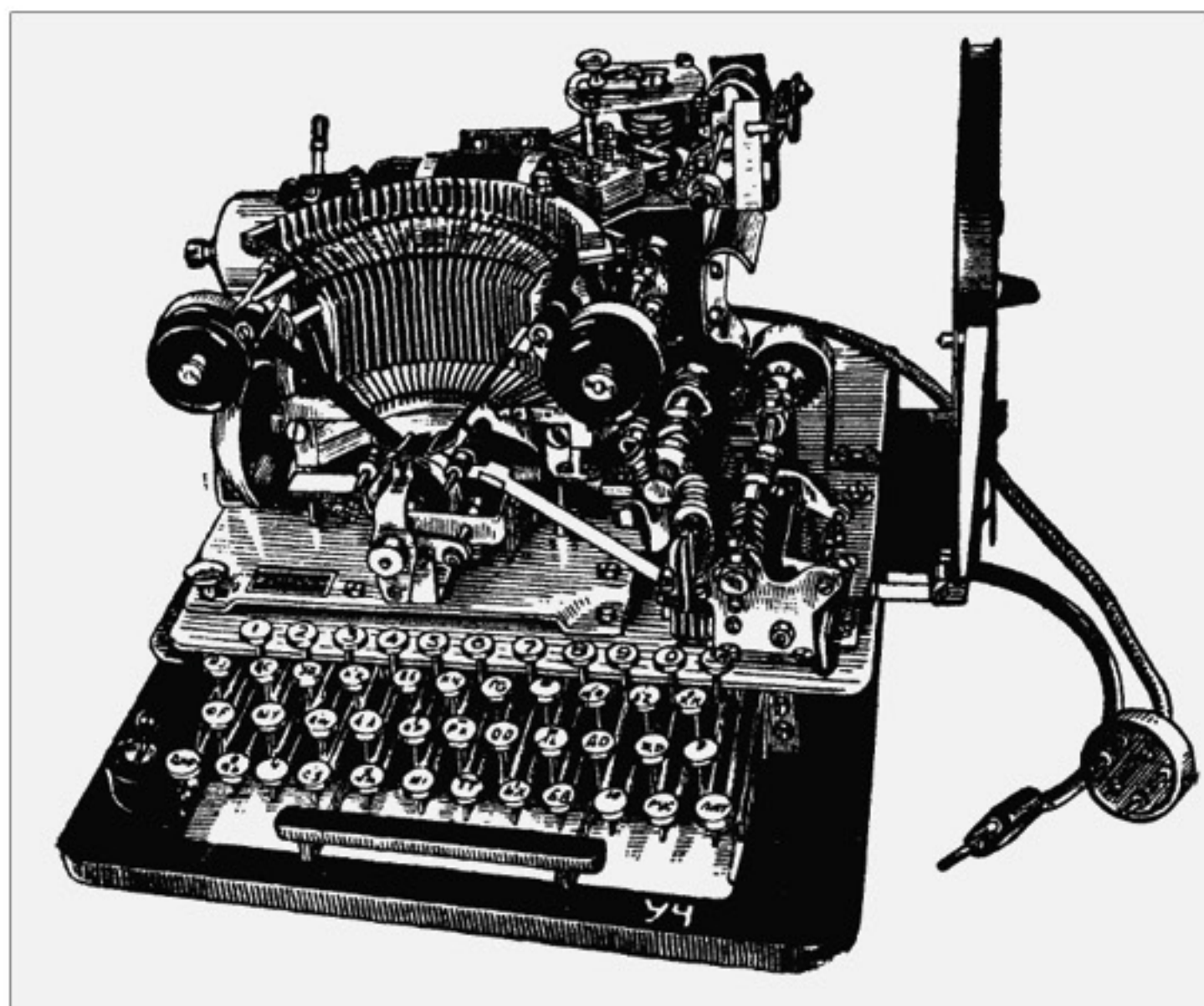


Иллюстрация 1. Аппарат СТ-35

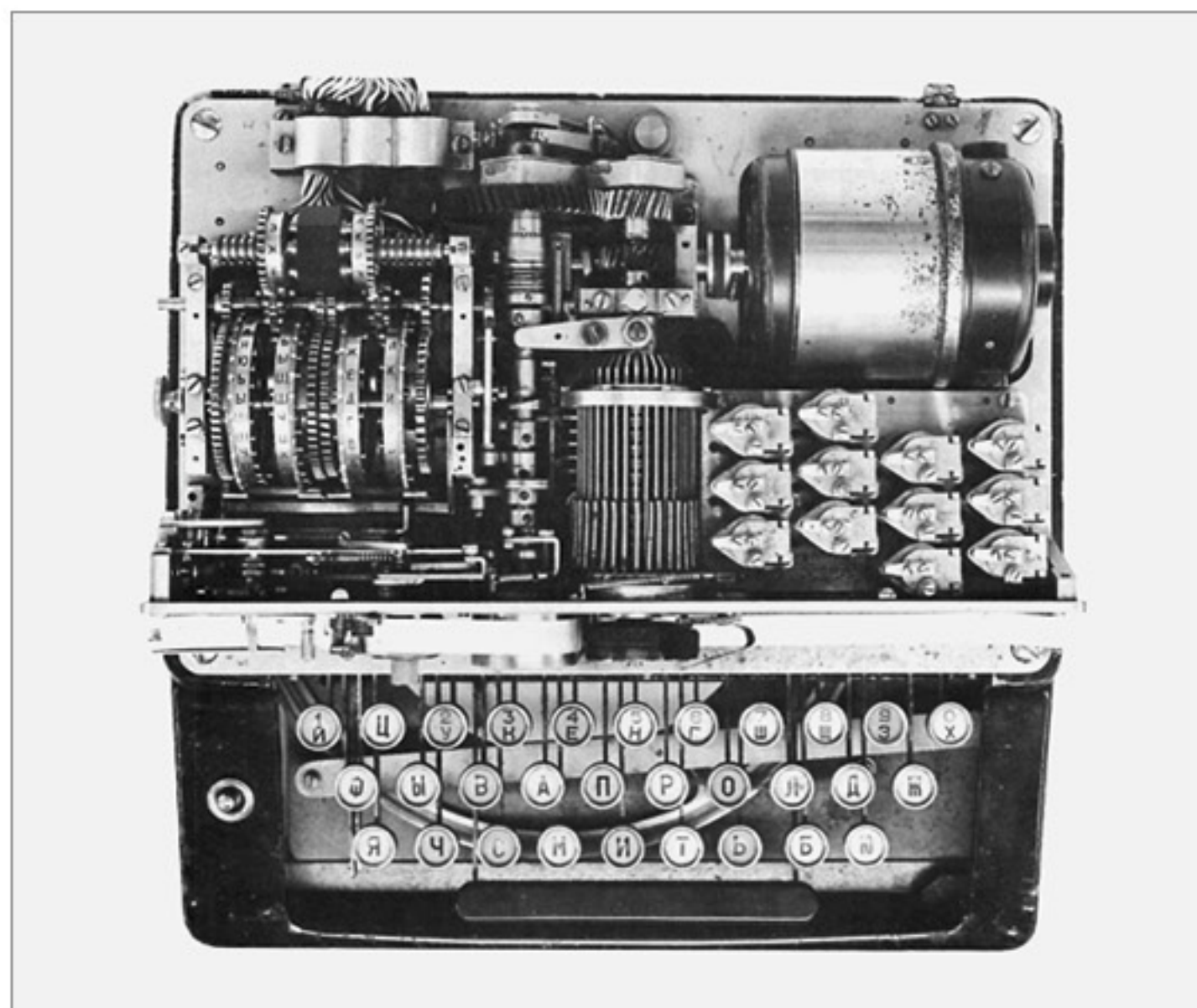


Иллюстрация 2. Кодировочная машина «Кристалл»

исходило его постепенное переключение на преимущественное выполнение заказов ВМФ.

Работа завода после 22 июня 1941 г. потребовала коренной перестройки его цехов, завершённой уже в августе, несмотря на уход рабочих в армию и отрыв персонала на строительство оборонительных сооружений. Заметим, что ленинградские предприятия средств связи в основном остались в городе. Полностью были эвакуированы из Ленинграда всего один завод и Ленинградский проектно-экспериментальный институт (ЛПЭИ) № 56, который был переведён в Уфу, сменив название на ГСПЭИ № 56 [1]. Что касается эвакуации завода № 209, то такое правительственное распоряжение было получено на предприятии только 23 августа 1941 г. Завод прекратил производство, его работники демонтировали, упаковали и погрузили оборудование в эшелоны. Но их отправка так и не состоялась ввиду прекращения железнодорожного сообщения. Всё имущество было возвращено на предприятие, и оно возобновило производственную деятельность [1].

ОРУЖИЕ ДЛЯ ЗАЩИТНИКОВ ЛЕНИНГРАДА

С 17 сентября на заводе приступили к подготовке изготовления пистолетов-пулемётов Дегтярева (ППД) с проектной мощностью 100 штук в месяц, а в ноябре началось их серийное произ-

водство. Выпуск телеграфной аппаратуры продолжался ещё до ноября 1941 г. лишь за счёт мощностей оборудования, предназначенного для производства ППД. При этом были достигнуты впечатляющие объёмы выпуска: в октябре завод изготовил 402 телеграфных аппарата СТ-35, хотя среднемесячный выпуск в 1-м полугодии не превышал 110 аппаратов.

Война прервала многие разработки отдела главного конструктора (ОГК) в области телеграфной техники, корабельной телефонии, аппаратуры засекречивания связи. Лишь часть работ в виде макетов, образцов, специального инструмента, технической документации была эвакуирована в Свердловск на заводской филиал. Даже в условиях начавшейся блокады сотрудники ОГК продолжали выполнение заказов вплоть до момента отключения завода от электроэнергии 27 декабря 1941 г.

ВРЕМЯ ЖЕСТОКИХ СТРАДАНИЙ ЛЕНИНГРАДЦЕВ

«Зимние месяцы 1941–1942 г. и начало весны 1942 г. стали самым трагичным периодом в истории блокадного Ленинграда. Это было время жестоких страданий его жителей и время полного паралича практически всей промышленной инфраструктуры города. В полной мере это относится и к работникам производств средств связи, и к членам их семей» [1]. Известно,

что зима 1941–1942 г. стояла необычно ранняя, холодная и продолжительная, без оттепелей. Правда, по этой причине Ладожское озеро раньше сковало льдом и начался подвоз продовольствия по ледовой «Дороге жизни». Но в домах не было электричества и отопления, прекратились подача воды и работа канализации. Встал городской транспорт. Согласно известным статистическим данным, от голода и холода в декабре умерли 53 тысячи ленинградцев, в январе — в два раза больше, в феврале и марте умерли ещё 200 тысяч человек, с апреля смертность заметно пошла на убыль.

«МОГЛИ ПРИХОДИТЬ НЕ БОЛЕЕ 300 ЧЕЛОВЕК ИЗ 3525»

23 января 1942 г. в результате бомбардировки на заводе произошёл большой пожар. Сгорел корпус «Д», где находились наиболее важные цеха: инструментальный, сборочные телеграфии, морской аппаратуры. Но самый ощутимый урон был нанесён кадровому потенциалу. Большинство работников на почве дистрофии потеряли работоспособность и перестали являться на предприятие. «На заводе при списочном составе 3525 человек на работу зимой 1942 г. могли приходить не более 300 человек» [1]. Их в основном использовали для проведения профилактических мероприятий по сохранению оборудования. С завода в конце



Иллюстрация 3. Старый корпус завода им. А.А. Кулакова (конец XIX века)

февраля — начале марта 1942 г. было вывезено 360 единиц оборудования, а также эвакуировано более пятисот рабочих и ИТР [2]. В марте в Москву отправили техническую документацию по корабельной аппаратуре, выпускавшейся на заводе, а в июне в Москву вывезли техническую документацию на всю электрослаботочную аппаратуру и откомандировали специалистов по этой аппаратуре. Оставшееся оборудование и персонал были использованы при создании девяти ремонтных бригад, выезжавших для обслуживания слаботочной аппаратуры по запросам воинских частей.

ВЕСЕННЕЕ ДЫХАНИЕ ЖИЗНИ

Тем не менее «весной 1942 г. блокадный Ленинград в целом, его промышленность, в том числе и электротехническая, начали постепенно оживать» [1]. Специальным постановлением ГКО от 6 января 1942 г. производства средств связи в части материально-технического и рабочего снабжения были приравнены к заводам авиапрома. Запрещалась мобилизация рабочих и ИТР, а также автотранспорта с предприятий, производивших военные средства связи. Для оказания повседневной помощи на заводы промышленности средств связи были назначены уполномоченные ГКО. Резко улучшилось снабжение за-

водов материалами и электроэнергией. Поставки материалов и изделий для заводов электропромышленности рассматривались как поставки особой важности, т.е. непосредственно обеспечивающие выпуск танков и самолётов и боевые действия РККА [1].

Ключевым вопросом стала проблема кадров. «На заводе № 209 в мае 1942 г, при списочном составе 1345 человек, на работу выходили чуть более 500, 469 человек были больны, а остальные — откомандированы на строительство оборонительных сооружений и другие работы» [1]. Уже в июне предприятие вынуждено было привлечь 812 учеников (женщин и подростков).

Постановление СНК СССР разрешало руководителям предприятий принимать для обучения и работы лиц с 14 лет при наличии заключения о состоянии здоровья. Для несовершеннолетних устанавливался 6-часовой рабочий день, запрещалось привлечение их к сверхурочным работам.

ВСЁ ДЛЯ ФРОНТА И ДЛЯ ПОБЕДЫ

Завод подключили к электроэнергии 20 апреля 1942 г. и уже в середине года оказался востребованным прежний опыт в области создания изделий точной механики для аппаратов шиф-



Иллюстрация 4. Пятнадцатилетняя ударница, токарь 3-го разряда Вера Тихова

рования и засекречивания правительственной связи. После начала войны основные работы в этой области были сосредоточены в ГСПЭИ № 56, расположенном в Уфе. Там под руководством выдающегося учёного и организатора В.А. Котельникова был собран большой коллектив специалистов. Институт занялся разработкой и подготовкой к серийному производству новых типов аппаратуры засекречивания телефонных переговоров в портативном исполнении [3, 4, 5].

Завод № 209 оказался единственным предприятием, где было возможно организовать производство сложных электромеханических узлов, являвшихся важными составными частями такой аппаратуры — магнитных барабанов. Они обеспечивали кратковременное запоминание (не более 0.2 сек.) микроучастков речи для их последующего «перемешивания» (10 раз в секунду) под управлением «случайной» гаммы, поступающей с шифратора.

Поэтому предприятие подключили к выполнению Постановления ГКО от 18 августа 1942 г. «Об обеспечении фронтовых правительственных связей специальной аппаратурой для телефонных и радиотелефонных разговоров» [3]. Для выполнения столь ответственной задачи в 4-м квартале 1942 г. на заводе организовали новый 70-й

цех и собрали в нем всех квалифицированных рабочих, создав под их руководством бригады работников низких разрядов [1]. Кроме этого, в Ленинград были откомандированы сотрудники лаборатории ОПС НКВД и ГСПЭИ № 56 [1].

Уже в 4-м квартале 1942 г. в 70-м цехе были изготовлены 12 электро-механических узлов аппаратуры «Соболь-П», применявшейся для связи фронтов с Москвой и между собой, а также 60 узлов шифрующей аппаратуры «Сова», предназначенной для работы в едином комплексе как с аппаратурой ВЧ связи, так и на проводных линиях связи [1]. При этом заказ «Сова» был выполнен на месяц ранее установленного срока. Хотя объём продукции цеха не превышал 10% от валового выпуска завода, учитывая значимость изделий и их сложность, уже к концу 1942 г. цех стал ведущим на предприятии [1]. Важную роль сыграли и сотрудники ОГК. Ими были переработаны поступившие из ГСПЭИ-56 чертежи аппаратуры, на основании которых шла работа в цехе. И это было только начало.

НАЧАЛО «РЕЧНОЙ» ТЕМАТИКИ

Для проведения проектных и конструкторских работ по заказам ОПС НКВД приказом наркома судостроительной промышленности в ноябре 1942 г. в составе ОГК было организовано специальное исследовательское конструкторское бюро (СИКБ), укомплектованное прикомандированными специалистами из тыловых районов, а также специалистами завода и возвращёнными из Красной Армии. Бюро поставили задачу разработки более совершенной переносной шифрующей аппаратуры «Волга» [1]. С её помощью предполагалось обеспечивать работу проводных каналов ВЧ связи между Москвой и штабами фронтов, а также основных тыловых магистралей. Работа была выполнена по техническому заданию ОПС НКВД с учётом иностранного опыта. При этом использовались лишь отдельные принципиальные решения некоторых узлов системы, указанные в общем виде в эскизном проекте ГСПЭИ-56. Все



Иллюстрация 5. Шифрование данных в боевых условиях

принципиальные вопросы, а также вся система в общем комплексе были проработаны заново [1].

КАК ИЗ «ВОЛГИ» ВЫТЕКЛА «НЕВА»

Для лучшего выполнения исследовательских и опытных работ, связанных с разработкой и изготовлением аппаратуры специального назначения, в апреле 1943 г. был восстановлен отдел новых разработок — 33-й отдел. Для серийного производства аппаратуры на заводе организовали и 65-й механико-сборочный и регулировочный цех [1]. Одновременно с работами по «Волге» начались разработки стационарного варианта этой аппаратуры — «Волга-С». Для увеличения дальности специальных линий связи 33-м отделом по собственной инициативе были разработаны и изготовлены лабораторные макеты устройств «Ладога-I» и «Ладога-II», положительно оценённые по результатам испытаний на линиях связи ОПС в Москве [1].

В процессе освоения аппаратуры «Волга» возникла идея и появилась техническая возможность дать более простую, малоразмерную, удобную в эксплуатации переносную аппаратуру, обладавшую и более высокими техническими качествами по сравнению с «Волгой». Вскоре был изготовлен лабораторный макет комплекса «Нева-П», прошедший успешные испытания на реальных линиях связи ОПС [1].

ПЛЕЧОМ К ПЛЕЧУ

После частичного снятия блокады Ленинграда зимой 1943 г. дефицит рабочих кадров стал ещё заметнее тормозить расширение производства. Даже к концу 1945 г. численность работников завода достигла лишь 29% от его предвоенного состава [1]. Единственным средством восполнения этого дефицита становилось всё более активное привлечение труда женщин и подростков. Заметим, что «заводу № 209 ещё в 1942 г. передали лагерь из системы ГУЛАГа НКВД. Заключённые были обучены производственным профессиям и использовались в качестве рабочих в механических цехах. Численность заключённых к 1945 г. была доведена до 423 человек, что составило 31% от общего состава предприятия» [1]. Заключённые в основной своей массе за три года работы на производстве стали квалифицированными работниками с высокой производительностью труда. «Их трудовые потери были ниже средних по заводу, а продолжительность рабочего дня выше других категорий работников на 20%. Такого рода персоналом были укомплектованы многие цеха предприятия, включая цех спецаппаратуры. В отдельных из них численность заключённых доходила до 72% от общего состава цеха. Когда в августе 1945 г. лагерь по решению НКВД был полностью ликвидирован, Завод им. Кулакова понёс та-

«Нева-П» разрабатывалась по инициативе самого завода как решение важной задачи: создать для проводных линий правительственной связи аппаратуру автоматического засекречивания телефонных переговоров, работающую преимущественно в полевых условиях

кие серьёзные кадровые потери, что ряд цехов пришлось временно обновить» [1].

ТРУДОВОЙ ПОДВИГ 33-ГО ОТДЕЛА

Вехой в истории Завода им. Кулакова стало вышедшее 18 мая 1944 г. Постановление ГКО «Об организации производства шифровальной и засекречивающей аппаратуры на заводе № 209 Наркомсудпрома», в соответствии с которым предприятие превращалось в один из ведущих центров страны по разработке и выпуску приборов такого типа [1]. Постановление обязывало завод обеспечить к определённым срокам выпуск пяти модернизированных аппаратов «Соболь-П», 20 аппаратов «Нева-П», 10 комплектов «Нева-С». Разработка всей этой аппаратуры для автоматического засекречивания телефонных переговоров осуществлялась по заказам ОПС НКВД, а исполнителем её на предприятии стало специальное КБ — 33-й отдел.

Заметим, что «Нева-П» разрабатывалась по инициативе самого завода как решение важной задачи: создать для проводных линий правительственной связи аппаратуру автоматического за-

секречивания телефонных переговоров, работающую преимущественно в полевых условиях. Её предполагалось использовать для всей сети правительственной связи, так как она сопрягалась со всеми типами каналообразующей аппаратуры ВЧ связи. К разработке «Нева-П» в 33-м отделе приступили в январе 1944 г. Было опробовано пять вариантов. По результатам испытаний в аппаратуру был внесён ряд существенных изменений. Опытные образцы к концу апреля 1944 г. были сданы заказчику. А до конца 1944 г. вся партия «Нева-П» была изготовлена и сразу же установлена для эксплуатации на ответственных участках ОПС, в 1945 г. специалистами 33-го отдела была проведена модернизация аппаратуры. Весь огромный объём работы, включавший и многие тысячи чертежей, выполнил коллектив 33-го отдела, состоявший из 33–35 человек [1].

ГДЕ «ТОПАЗ», ТАМ И «АЛМАЗ»

Большой объём работ по созданию специальной шифровальной техники проделали и специалисты ОГК. В 1944 г. это подразделение завода, вы-

полнявшее функции обслуживания текущего производства, сразу переросло в крупный технический отдел со своей конструкторской и опытной базой. В первом полугодии 1944 г. там была проведена модернизация приборов для шифровки письменных сообщений П-200, выпущенных пробной серийной партией в 1943 г. Армия и флот получили портативный шифровальный прибор, не требующий для работы источника питания, и очень простой и надёжный в эксплуатации [1]. Ряд принципиально новых приборов засекречивания связи был разработан по заказу 5-го Управления НКГБ. Это аппаратура предварительного шифрования «Рубин», перешифровальный аппарат «Кварц», шифровальный аппарат для работы с радиотелеграфной аппаратурой «Топаз».

Первые два вида шифровальной техники передали заказчику в виде опытных образцов, а в 1945 г. осуществили их серийный выпуск в количестве 201 и 28 комплектов соответственно [1]. В 1945 г. на заводе № 209 происходила концентрация производственных заданий по шифровальной и засекречивающей технике связи. С других предприятий приняли ряд разработок, имевших заделы для серийного производства. Это была аппаратура «Малахит», «Аметист», «Алмаз» для РККА и ВМФ.

Идя в ногу со временем, возрождённый завод им. Кулакова наладил в дальнейшем серийный выпуск ещё более совершенной и стойкой аппаратуры засекречивания связи.

ЛИТЕРАТУРА

1. Алексеев Т. В. Индустрия средств связи Петербурга-Ленинграда для армии и флота в эпоху потрясений и модернизации. 1900–1945 г.г. Монография. СПб.: СПбГПУ, 2010.
2. Булатов В. Ф. История петербургского приборостроительного завода им. А. А. Кулакова // Электросвязь: история и современность. 2008. № 3.
3. Правительственная электросвязь в истории России. М., 2001.
4. Емельянов Г. В., Ларин Д. А., Бутырский Л. С. Гигант радиоинженерной мысли. // Информационная безопасность банков. М., 2013. № 2.
5. Сапрыкин А. Секретная связь: от тайнописи до криптомаршрутизатора. «Красная звезда» от 25 марта 2019 г.

Борис СТОЛПАКОВ

историк криптографии, кандидат
физико-математических наукЭсминец Северного флота «Разумный»
отходит от причала в Полярном

РАДИОМОЛЧАНИЕ ПОРОЙ ДОРОЖЕ ЗОЛОТА

ПРОВЕРЕНО В ВОЕННЫХ РЕЙСАХ НА СЕВМОРПУТИ¹

Северный морской путь (СМП) во время Великой Отечественной войны начинался в Архангельске и Молотовске (ныне Северодвинск), проходил через арктические порты и заканчивался в бухте Провидения на Чукотке. Плавание судов по СМП было возможно только в летние месяцы. И короткое арктическое лето военный флот Германии использовал для активных действий на советских арктических маршрутах.

ОПАСНОЕ ДВОЕВЛАСТИЕ

Именно западная часть СМП, включая Карское море, находилась в зоне дей-

ствия германского флота. Безопасность транспортного сообщения в этих условиях существенно зависела от поддержания секретности планирования морских операций и использования только кодированной или шифрованной связи. Но сложилось так, что Севморпуть подчинялся и военному флоту, и Главсевморпути во главе со знаменитым полярником И.Д. Папаниным. Это было связано в том числе и с вынужденным недостатком сил, выделяемых военным флотом для защиты СМП. Двойственность подчинения и кажущаяся удалённость от линии фронта снижали внимание местных руководителей к защите информации, которой они располагали [4]. Среди этой обильной информации содержались и сведения большой государственной важности, ведь движение по восточной части СМП,

начинавшейся с моря Лаптевых, требовало согласования с Тихоокеанским маршрутом ленд-лиза и авиатрассой Аляска-Сибирь.

СЕВЕРНЫЙ ТИХООКЕАНСКИЙ МАРШРУТ ЛЕНД-ЛИЗА

Через Тихий океан СССР получал по ленд-лизу из США прежде всего продовольствие и предметы потребления, горючее, промышленное оборудование, транспортные средства. После нападения Японии на США 7 декабря 1941 года перевозками грузов в СССР могли заниматься только транспорты под советским флагом и с советскими экипажами [1]. Тогда положение СССР на Тихом океане было крайне невыгодным. Все проливы, ведущие к портам советского Приморья, контролировались Японией. Ей принадлежали

¹ Публикация подготовлена с использованием средств гранта Президента Российской Федерации на развитие гражданского общества №18-2-012576, представленного Фондом президентских грантов.



Иллюстрация 1. Маршруты СМП

и южный Сахалин, и все Курильские острова. Поэтому значительная часть советских транспортов из США направлялась по северному Тихоокеанскому маршруту к берегам Камчатки. Там в качестве перевалочной базы использовался Петропавловск-Камчатский. Но часть транспортов сразу направлялась в бухту Провидения, где формировались арктические караваны.

АВИАТРАССА АЛЯСКА — СИБИРЬ

Рядом с северным Тихоокеанским морским маршрутом проходил и воздушный путь, получивший название трассы Аляска — Сибирь (АлСиб). 9 октября 1941 года Государственный Комитет Обороны принял решение об организации воздушного перегона самолётов из США в СССР. Был выбран маршрут от города Фэрбэнкса на Аляске через Берингов пролив, центральные районы Чукотки, Колымы и Якутии до Красноярска, протяжённостью около 6500 км. Уже осенью 1941 года в срочном режиме в тяжелейших условиях развернулись подготовительные работы. Было реконструировано и построено заново 17 аэродромов, сооружались также узлы связи и радионавигации, метеостанции и другие необходимые объекты. Движение по АлСибу было открыто 6 октября 1942 года. Всю трассу разбили на пять участков. Сменяя друг друга, лётчики пяти авиаполков доводили самолёты до Красноярска. Далее боевые

машины отправляли своим ходом или, чаще, в разобранном виде по железной дороге за Урал и после сборки они летели на полевые аэродромы.

Специально для АлСиба была сформирована 1-я перегоночная авиадивизия. Первым её командиром и одновременно начальником трассы стал И. П. Мазурук, известный полярный лётчик. Для службы в дивизии отбирались лишь опытные лётчики. В основном из полярной и морской авиации, ведь полёты проходили в крайне сложных условиях: в дождь, снег, туман, морозы, над горами и тайгой. Случалось, лётчики погибали. Но темпы перегонки самолётов по АлСибу нарастали: в 1942 г. успели доставить 114 самолётов, в 1943 г. — уже 2465. Всего за годы войны из США до Красноярска добрались почти 8 тыс. самолётов: около 3 тыс. бомбардировщиков и 5 тыс. истребителей.

Кроме того, транспортные самолёты перевозили особо ценные грузы и дипломатическую почту. Летали по этой трассе даже высокопоставленные государственные деятели, в том числе вице-президент США Г. Уоллес [1]. Всё необходимое для строительства и обеспечения жизнедеятельности АлСиба доставлялось в основном через порты СМП. Тяжелогружённые транспорты собирались в бухте Провидения на Чукотке и в сопровождении ледоколов шли через Берингов пролив в Арктику и далее на запад. В устьях круп-

ных сибирских рек разгружались те материалы, которые предназначались для обслуживания самого СМП, АлСиба или для Норильского горно-металлургического комбината и рудников [1].

ОПЕРАЦИЯ «ВУНДЕРЛАНД»

В июле и августе 1942 года в Карском море немцы провели крупную наступательную операцию «Вундерланд» с участием тяжёлого крейсера «Адмирал Шеер» и подлодок, намереваясь прервать арктическое судоходство. Готовились к летней навигации 1942 г. и флотские радиоразведчики. В Архангельске сформировали радиоотряд, его включили в состав Беломорской военной флотилии, отвечавшей за защиту СМП. Под особым вниманием находился радиообмен немецких подводных лодок [2]. Тем не менее, лодка U-601 27 июля обстреляла полярную станцию на Новой земле, а 1 августа торпедировала пароход «Куйбышев» с грузом угля, его радист неосторожно сообщил открытым текстом о времени своего прибытия на Диксон [4].

Каждый рейс в арктической навигации становился испытанием для команды и судна. «Хотя немецкие подлодки были обнаружены в юго-восточной части Баренцева моря, на подходах к проливам Новой Земли, суда выходили из Архангельска в Арктику по мере готовности. 9 августа вышел караван из 9 транспортов и 11 кораблей охраны, среди них 2 английских эсминца. 14 августа — 2 транспорта и 4 корабля охраны. От горла Белого моря до Новоземельских проливов осуществлялось прикрытие самолётами Северного флота» [4].

А на тихоокеанском побережье Чукотки перемещение транспортов отслеживала японская разведка. Она засекла проход первых судов через Берингов пролив, и 1 августа из Токио в Берлин ушла шифровка: «Советский конвой в составе четырёх ледоколов и 19 транспортных средств 1 августа прошёл через Берингов пролив в северном направлении...» [1]. Получив столь ценную информацию, немецкое командование решило атаковать оба конвоя там, где тогда никто не ожидал — в Карском море. По их расчетам,



Иллюстрация 2. Немецкий тяжелый крейсер «Адмирал Шеер»

именно там должны были встретиться западный и восточный караваны торговых судов. 18 августа «Адмирал Шеер» тайно пересёк Карское море и направился к западному побережью Таймыра. Но ледовая обстановка не позволила напасть на уже обнаруженный западный караван, да и корабельный самолёт-разведчик вышел из строя. Тяжёлый крейсер сам с трудом выбрался из плена плывущих льдов близ пролива Вилькицкого и искал встречи с каким-нибудь судном для получения ледовой информации [4]. Так на пути «Адмирала Шеера» оказался ледокольный пароход «Сибиряков».

ПОДВИГ «СИБИРЯКОВА» И ЗАЩИТНИКОВ ДИКСОНА

«25 августа в 13ч.27м. с «Александра Сибирякова» на Диксон поступило сообщение, что неизвестный военный корабль запрашивает сведения о состоянии льда, а «Сибиряков», не отвечая, повернул к берегу. В 13:34 новое сообщение: судно идёт к берегу, а неизвестный крейсер преследует его, повторно запрашивая состояние льда. 13:38 — «Сибиряков» передал: крейсер сообщил своё название — «Сисияма». В ответной радиограмме Диксон сообщил, что такое судно Штабу морских операций

не известно. 13:47 — тревожное сообщение: «началась канонада», 13:48 — «СОС!» и связь прекратилась» [4].

Советский экипаж не имел никаких шансов против огневой мощи тяжёлого крейсера, но принял бой. И главное, прежде чем погибнуть, с парохода успели передать сообщение и рассекретили «Адмирала Шеера». По немецким документам, в 14:15 «Сибиряков» затонул. Но ещё в 13:30 из Диксона на ледокол «Красин» ушла команда: незамедлительно следовать с караваном судов через пролив Вилькицкого в море Лаптевых. Восточному каравану, также шедшему к проливу Вилькицкого, поступил приказ оставаться в море Лаптевых.

Командир «Адмирала Шеера», понимая бесперспективность поиска караванов среди льдов, решил совершить налёт на Диксон в Енисейском заливе, чтобы уничтожить этот важный центр управления и один из главных портов на трассе СМП. Но когда через сутки он подошёл к Диксону, его уже ждали. Крейсер обнаружили ещё при подходе в трёх милях от берега. В 01:13 была объявлена боевая тревога и суда на рейде встретили крейсер огнём. В начале боя германские моряки не заметили батарею из двух 152мм орудий, располо-

женную на причале. После нескольких её выстрелов удалось накрыть крейсер, и он под прикрытием дымовой завесы отошёл в море, отказавшись от высадки десанта.

Затем крейсер обстрелял город и порт с другой позиции, снова получил накрытие и окончательно удался. Весь бой длился около двух часов [4]. Видимо, командир крейсера не ожидал организованного отпора, да и наличие в Диксоне тяжёлой артиллерии стало полной неожиданностью. Вместе с тем, рейд «Адмирала Шеера» показал слабости защиты советских коммуникаций в Карском море. Всего в навигацию 1942 г. германским флотом на СМП было совершено 9 нападений, при этом потоплено 7 судов, уничтожено 2 гидросамолёта, повреждены 4 полярные станции и порт Диксон [4].

«КАПИТАНЫ ТОРГОВЫХ СУДОВ ПРАКТИЧЕСКИ НЕ ПОЛЬЗОВАЛИСЬ ШИФРСВЯЗЬЮ»

Причиной успехов вражеских рейдов в советской Арктике стало активное использование германскими моряками радиоперехвата вместе с соблюдением режима радиомолчания: вне нападения их подлодки в Карском море обна-

руживали 10 раз, из них лишь дважды средствами радиоразведки [4]. К сожалению, «в навигацию 1942 г. сотрудники Главного Управления СМП не всегда предпринимали шаги по обеспечению скрытности и безопасности связи. Капитаны торговых судов и ледоколов, лётчики полярной авиации, зимовщики полярных станций практически не пользовались шифрсвязью. Переговоры о местонахождении судов, маршрутах конвоев и т.д. велись открытым текстом. Несмотря на неоднократные предупреждения военных специалистов о недопустимости подобного состояния дел, полярники не использовали документы скрытой связи (так на флоте называли шифры). Мало того, на некоторых судах они просто отсутствовали» [4]. Лётчики, капитаны, полярники и метеорологи практически до лета 1943 года считали, что находятся в глубоком тылу. А потому постоянно использовали радиосвязь в открытом режиме, поставляя тем самым противнику ценные сведения. «Только потери от действий немецких подводных лодок заставили сотрудников Главсевморпути осознать необходимость использования шифрованной радиосвязи. К лету 1943 г. передачи открытым текстом важной информации в основном прекратились» [4].

ДИРЕКТИВА УПРАВЛЕНИЯ ОСОБЫХ ОТДЕЛОВ НКВД

В суровых условиях Арктики особенно значимы метеопрогнозы. Метеосводки регулярно передавали по радио полярные станции, которые только по берегам Карского моря располагались в 17 местах. Судя по документам, к весне 1942 г. у гидрометеослужбы Вооружённых Сил СССР накопились проблемы с безопасностью передачи метеоданных не только на Севере.

Директива Управления ОО НКВД СССР от 22 апреля 1942 г. «О мерах по обеспечению конспирации в работе гидрометеослужбы Красной Армии»

«Всем начальникам особых отделов фронтов, округов, флотов и флотилий!

По поступившим в Управление особых отделов НКВД СССР сведениям, командный состав частей, школ и подразделений Красной Армии, в которые входят авиаметеорологические стан-

ции гидрометеослужбы Красной Армии, нарушает правила ведения шифрования гидрометеорологических сведений, предусмотренных инструкцией гидрометеослужбы по ведению секретного кодирования: работает с шифром в присутствии всего обслуживающего персонала станции, знакомит с шифром лиц, не имеющих допуска к секретным работам, и т.д.

В целях обеспечения конспирации шифрования гидрометеорологических сведений предлагаю:

Провести проверку выполнения органами гидрометеослужбы частей и подразделений Красной Армии правил использования и хранения гидрометеорологических шифров и секретных материалов гидрометеослужбы Красной Армии.

О всех выявленных нарушениях в обращении с шифром и секретными материалами гидрометеослужбы информировать командование и виновных привлечь к ответственности» [5,6].

ВЗАИМНЫЙ ИНТЕРЕС КРИПТОГРАФОВ И МЕТЕОРОЛОГОВ

Эта директива преследовала цель, прежде всего, недопущения использования противником наших метеоданных для более эффективного применения своих сил и средств. Но сам вопрос правильного шифрования метеоданных очень серьёзен, ведь неудачное засекречивание сводок погоды могло дать дешифровальщикам противника весьма важную информацию о шифре. Например, «в годы войны немецкая метеостанция, расположенная в районе Бискайского залива в течение многих месяцев подряд передавала сообщения, которые начинались примерно так: «Метеопрогноз для Бискайского залива...», далее шли сами прогнозы, не отличавшиеся большим разнообразием в смысле текста: температура — такая-то, ветер такой-то и т.д. При этом практически один и тот же открытый текст постоянно шифровался на разных ключевых установках. Англичане убедились, что прогноз раз от раза почти не меняется и стали эффективно использовать этот факт для вскрытия новых ключевых установок «Энигмы». Заметим, немецкая служба связи предупреждала о недопустимости передачи ежедневно в одно и то же вре-

мя практически одинаковых прогнозов, но немецкие метеорологи не обратили внимание на это предупреждение» [5]. Сумели вскрыть немецкую систему шифрования метеодонесений и дешифровальщики СФ. Так, старший лейтенант Е. Казанцев «установил систему и разработал таблицу для перешифровки метеодонесений, применявшуюся немецкими постами СНиС (службы наблюдения и связи — Б.С.) района Тромсё и Лофотенских островов. В результате этого служба погоды и ВВС СФ получали данные о метеообстановке в этих районах, что способствовало проведению боевых операций у полярного побережья Норвегии» [3].

КОНТРОЛЬ ЭФИРА И ОТРАЖЕНИЕ АТАК НЕМЕЦКИХ ПОДВОДНИКОВ

В навигацию 1943 года гитлеровцы вновь активизировались в западном секторе СМП. Их подводные лодки даже использовали тайные радиостанции на берегах Карского моря. Одновременно радиоразведка СФ создавала пункты радиоперехвата в Губе Белушья и на мысе Желания на островах Новой Земли, на острове Диксон в Енисейском заливе [2]. Военный флот должен был обеспечить безопасное выполнение плана перевозок по западной части СМП, это более 50 тыс. тонн грузов — четверть от полного грузооборота по СМП [4].

По послевоенным немецким данным, у западного побережья Новой Земли несколько лодок занимались перехватом наших сообщений и их расшифровкой. В Карском море по данным радиопеленгационных постов одновременно действовали 6–8 немецких лодок группами, каждая лодка находилась там полтора-два месяца, после чего заменялась [2].

Соблюдая меры предосторожности, первый конвой вышел из Молотовска 17 июня [4]. В Карском море была установлена зона радиомолчания. Первая подлодка противника в Карском море была обнаружена радиоразведкой 19 августа [2]. А «9 сентября полярная станция острова Уединения сообщила о работе на волне 720 метров неизвестной радиостанции с позывным «180», которая вызывала «0845» и передава-

ла шифрограмму пятизначными буквенными группами. 9, 10 и 11 сентября радиостанция острова Уединения систематически наблюдала в эфире работу неизвестных раций. 11 сентября работу неизвестной рации обнаружил и радицентр острова Диксон. По характеру передаваемых шифрограмм предположили, что передачу вели судовые и береговые немецкие радиостанции. По сведениям рыбаков в Енисейском заливе, в течение 5 дней находилась подводная лодка. 11 сентября радиостанцией самолёта при попытке взять пеленг у радиостанции мыса Стерлегова (на западном побережье Таймыра — Б.С.) была обнаружена работа неизвестной радиостанции, которая намеренно забивала рацию мыса Стерлегова» [4]. Вновь случились и нападения, и потери. Ввиду серьёзной опасности для судоходства осенью 1943 года 15 шедших на запад гружёных судов были даже оставлены на зимовку в порту Диксон вместо того, чтобы идти в пункты назначения [4].

ПОСЛЕДНЯЯ ВОЕННАЯ НАВИГАЦИЯ НА СМП

К навигации 1944 года, последней навигации военного времени, на Диксоне создали Карскую военно-морскую базу Беломорской военной флотилии, усиленную современными кораблями, полученными по ленд-лизу. Была разработана и доведена до сведения капитанов судов и командиров самолётов система опознавания «свой-чужой» [4]. Но морская война на Крайнем Севере продолжалась, и угроза советским судам от вражеских мин и торпед сохранялась. Летом 1944 г. погиб теплоход «Марина Раскова» с 500 рабочими, полярниками и членами их семей на борту, спастись удалось лишь половине пассажиров и членов экипажа. Всего в навигациях военного времени на СМП погибли около тысячи тружеников Севера и военных моряков [4].

«НЕМЦЕВ ИНТЕРЕСОВАЛ КОД „ПОЛЮС“»

С уже упомянутой радиостанцией мыса Стерлегова на Таймыре связан также известный эпизод 1944 г. «В ночь на 25 сентября в 2,5 км от мыса Стерлегова на берег высадился десант с двух не-

Форма № 1
СЕКРЕТНО

ПЕРЕГОВОРНАЯ ТАБЛИЦА "МЕТЕО"

Гидро метео служба изданных вое и за фронта для

передачи провозами метеостанций.

I	1	Погода, в/н	II	1	наблюдения
	2	Прогноз погоды		2	Условия
	3	Разведка погоды		3	Срок, и/им
	4	Метеорологич.		4	ожидаются
	5	Гидрологич.		5	Уточн./см/нго
	6	Обслуживание		6	Обстановк, в/у/н
	7	Начат, о/н/б; нача, лась/леса		7	Организуите
	8	Прекращен, о/н		8	Анемометрич. разведка
	9	Данные		9	На...
	0	Сведения		0	Телеграмма
III	1	Обла, ка/чность	IV	1	Преимущество
	2	Низк, ле/ая		2	Облака опред. трудно
	3	Высок, ле/ая		3	Снижение
	4	Меняющ. облачн. с проясн.		4	Полноты
	5	Сплошная		5	Бадл, в/ов
	6	С просветами неба		6	горизонт, в/е
	7	Увеличение		7	Висот, в/ой
	8	Уменьшение		8	Видимость
	9	Облаков нет /ясно/		9	Нераскодируется
	0	Пасмурно		0	Повторите
V	1	Перистые	VI	1	Вет, вр/ры/ра
	2	Перисто-кучевые		2	Направление ветра
	3	Перисто-слоистые		3	Скорость ветра
	4	Высоко-кучевые		4	Ш т и л ь
	5	Высоко-слоистые		5	Ветер по направ. доустой-
	6	Слоисто-кучевые		6	Ветер по направ. устойчив.
	7	Слоисто-дождевые		7	Усили, лся/вается
	8	Слоистые		8	Утих, ает
	9	Кучевые		9	Скорость ветра лавн
	0	Кучево-дождевые		0	ориентир /век-бурьора/
					больше 10 м/сек.
					Ветер

При угрозе пленения или захвата противником обязательно УНИЧТОЖИТЬ

Иллюстрация 3. Лист переговорной таблицы «Метео»

приятельских подводных лодок U-711 и U-957, состоящий из 25 человек. Среди десантников были радист — латыш, хорошо знающий русский язык, и переводчик, умевший работать на ключе... Десантники ворвались на полярную станцию в 3 часа ночи... Трое немцев вошли в радиорубку и скомандовали дежурному радисту: «Руки вверх!». Вслед за этим подняли с койки начальника полярной станции (он же второй

радист и механик), метеоролога и двух краснофлотцев... Во избежание обнаружения высадки десанта немцы заставляли работников полярной станции регулярно производить передачу метеосводок, грозя радисту немедленным расстрелом в случае попытки сообщить о захвате станции. При передаче метеосводок постоянно присутствовал либо радист из состава десанта, либо переводчик. Как выяснилось позже, це-

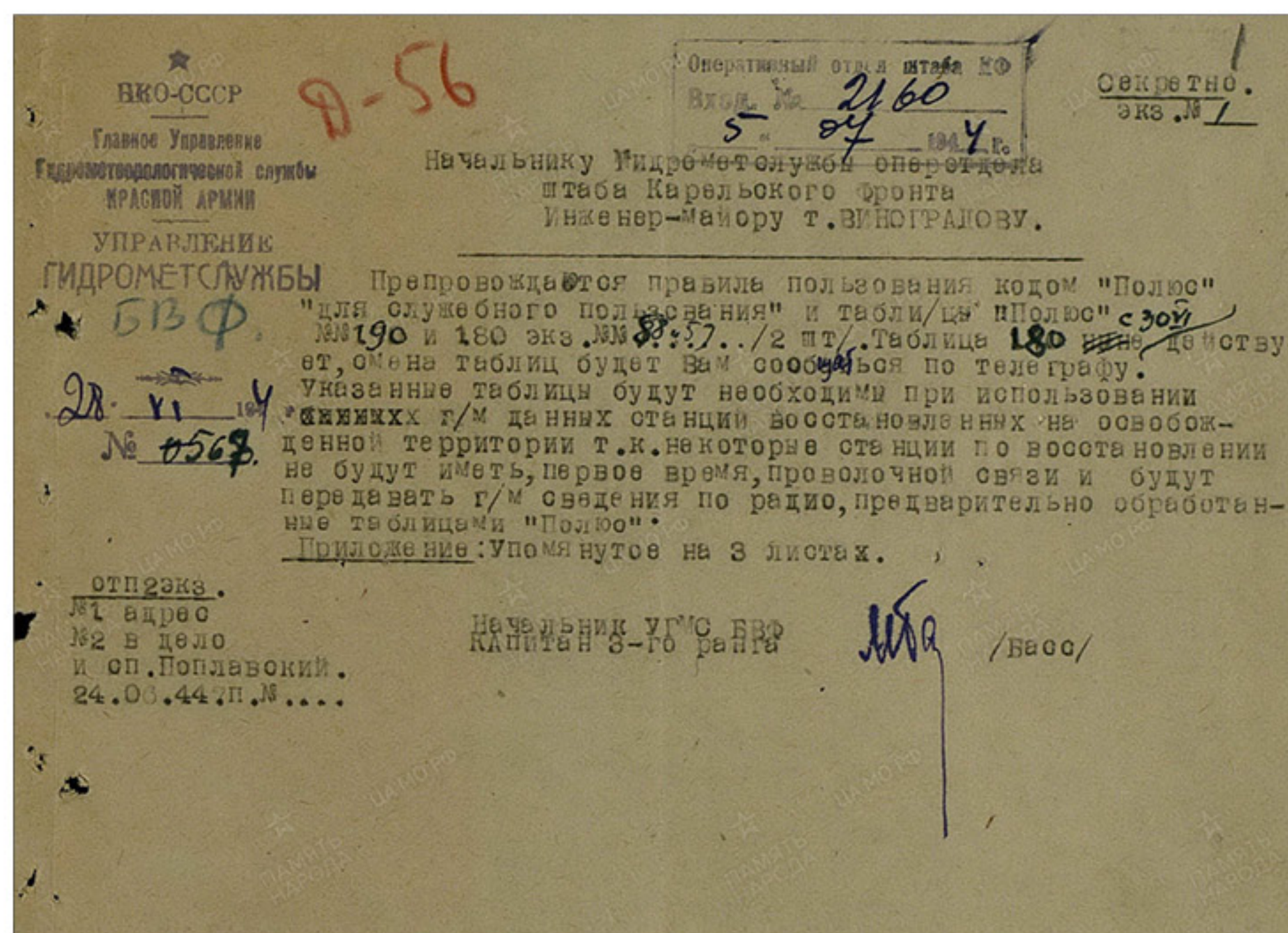


Иллюстрация 4. Сопроводительное письмо к таблицам кода «Полус»

люю немцев на мысе Стерлегова был захват самолётов, которые, как они предполагали, базировались там. Немцы забрали все находившиеся на станции шифрдокументы и документы связи, в том числе и военные, причём ко всем этим документам они не проявляли особого интереса, заявляя, что уже имеют их. Немцев интересовал код «Полус». Весь день 25 сентября лодки находились метрах в 300 от станции... 26 сентября в 12 часов пополудни лодки ушли, а в 16 часов возвратились обратно, после чего немцы начали посадку... На лодку было погружено всё имущество, захваченное на станции, а также 5 пленных... Предположение о том, что на полярной станции что-то случилось, зародилось в Штабе морских операций на том основании, что с 21 часа 26 сентября радиостанция мыса Стерлегова прекратила

работу...» [4]. На Диксоне были приняты срочные меры по выяснению причин молчания станции и смене шифров.

ДЕШИФРОВКА ДОНЕСЕНИЙ ВРАЖЕСКИХ АГЕНТОВ НА СОВЕТСКОМ СЕВЕРЕ

Радиоразведчики неоднократно фиксировали сеансы связи немецких подводников и радиостанций, находившихся на территории СССР. «Эти радиостанции использовались не только для радиоперехвата, но и для управления действиями немецких субмарин. Следы работы немцев в советском Заполярье, их брошенные наблюдательные пункты обнаружили уже после войны» [2]. Надо упомянуть также, что с 1942 г. увеличилась заброска немецких и финских агентов на Кольский полуостров. Расшифровка радиодонесений,

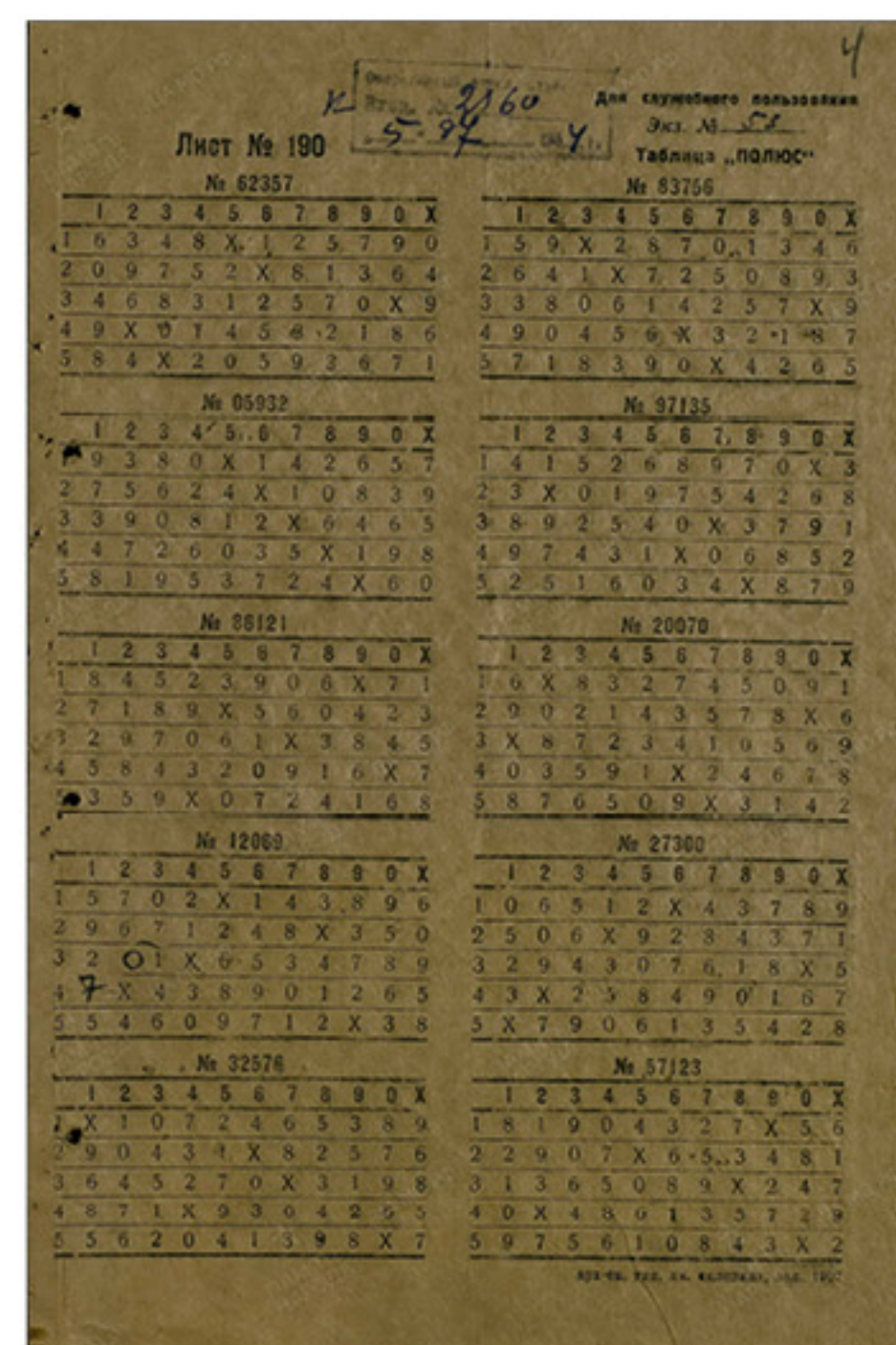


Иллюстрация 5. Таблица кода «Полус»

исходивших с нашей территории была поручена и дешифровально-разведывательной службе СФ. Для перехвата шифровок вражеских агентов с марта 1943 г. разведотдел флота специально использовал передвижной радиопеленгаторный пункт. «Непосредственно криптографическим анализом шифрдоносений немецкой агентуры занимались старшие лейтенанты А. Марков и К. Новохатский» [3].

Несмотря на чувствительные потери, своими самоотверженными усилиями флотские дешифровальщики и участники арктических рейсов сорвали планы германского командования прекратить навигацию по Северному морскому пути.

ЛИТЕРАТУРА

1. Монин С. М. Дорогами ленд-лиза // Великая Победа в 15 т. Т. 15 / М.: МГИМО-Университет, 2015.
2. Кикнадзе В. Г. Развитие сил и средств радиоразведки отечественного военно-морского флота в первой половине XX века: исторический опыт и уроки. Диссертация докт. ист. наук. Военная академия ГШ ВС РФ, 2014.
3. Фёдоров В. Развязать врагу язык... И так, чтобы он об этом не узнал. «Мурманский вестник» от 25.07.2014.
4. Бурков Г. Д. Война в Арктике. М., 2014.
5. Бутырский Л. С., Ларин Д. А., Шанкин Г. П. Криптографический фронт Великой Отечественной. М., 2017.
6. Органы государственной безопасности СССР в Великой Отечественной войне 1941–1945. Сб. документов. М., 1995.



Анастасия СКОГОРЕВА
обозреватель BIS Journal

ЧЁРНОЕ ЗЕРКАЛО

ИСТОРИЯ ОГРАБЛЕНИЯ БАНКА, ПРЕНЕБРЕГАВШЕГО СТАНДАРТАМИ И ПРАКТИКАМИ ИБ

В рамках состоявшейся в апреле конференции по практическим аспектам борьбы с кибермошенничеством в финансовом секторе эксперты RMT Group на конкретном примере продемонстрировали, как история о несоблюдении стандартов и правил ИБ легко превращается в историю об атаке на банк, совершённой с помощью «кротов».

ВНАЧАЛЕ БЫЛИ ТОЛЬКО ХАКЕРЫ

Этот кейс о некоем банке, подвергшемся хакерской атаке, был выбран для презентации неслучайно, поскольку в нём, как в зеркале современной цифровой реальности, отразилось очень многое: начиная с того, как злоумышленники используют социальную инженерию, и заканчивая тем, какую роль в жизни банка может сыграть «человеческий фактор», наличие «кротов», технологическое несовершенство, отсутствие контроля за действиями пользователей и многое другое.

Прежде чем разбирать кейс, стоит отметить, что прецедент имел место в 2015 году, то есть довольно давно, когда ещё не было такого жёсткого регулирования сферы ИБ банков, как сейчас. Тем не менее, многие из вскрывшихся при расследовании проблем актуальны для финансовых организаций до сих пор.

Итак, путём заражения популярного сайта, дружно посещаемого сотрудниками нашего банка, злоумышленники получили удалённый доступ к компью-

терам этих сотрудников. Скопировали систему ДБО и даже ключи к ней. Далее произошло само хищение: воры направили со своих устройств нелегитимные платёжные поручения. Когда сотрудники банка эти поручения выполнили, атакующие с помощью ещё одного вредоноса «вырубили» компьютеры сотрудников. То есть «положили систему», причем, на довольно продолжительное время — на три рабочих и два выходных дня.

Казалось бы, в данном случае можно отследить два фактора: пренебрежение сотрудниками банка принципами ИБ и отсутствие должного контроля за их действиями в качестве пользователей банковской системы. О том, что такой контроль необходим, в последние годы говорилось неоднократно, но, как можно судить по кейсу, далеко не всегда дело на практике обстоит так, как в теории.

Что касается действий злоумышленников на последнем этапе атаки, то они вполне «укладываются» в распространённый сценарий. Падение системы и вывод из строя всех компьютеров, естественно, вызвал у сотрудников состоя-

ние, близкое к шоку. Чтобы восстановить систему, потребовались время и силы. Этот временной «лаг» дал злоумышленникам возможность хотя бы частично замести следы и «удалиться».

ТЕХНОЛОГИЧЕСКАЯ БЕСПЕЧНОСТЬ

И вроде бы стандартная история, но дальше стали открываться интересные подробности. Как пояснил эксперт RMT Group Фёдор Музалевский, результатом сочетания умелых действий злоумышленников, с одной стороны, и человеческого фактора, с другой, стало то, что организация практически одновременно потеряла 100 млн рублей. Было проведено пять компьютерно-технических экспертиз (при этом эксперт считает, что такое большое количество экспертиз вполне объяснимо и закономерно). Сотрудники правоохранительных структур быстро выяснили, с какого IP-адреса была совершена атака, владельца IP-адреса арестовали, а его цифровые устройства отправили на экспертизу, но ничего отражающего механизм хищения денежных средств на этих устройствах не обнаружили.

Результатом сочетания умелых действий злоумышленников, с одной стороны, и человеческого фактора, с другой, стало то, что организация практически одновременно потеряла 100 млн рублей



Параллельно этому уголовному делу шёл арбитражный процесс. Из-за несоответствия материалов уголовного дела арбитражному процессу было возбуждено второе уголовное дело, подозреваемыми по которому были определены неизвестные сотрудники банка, против которого была совершена атака. Основная проблема, по мнению следствия, заключалась в том, что банк не только не обеспечил безопасность своей ДБО, но ещё и позволил своими действиями произойти хищению.

На основании чего следствие пришло к такому выводу? Прежде всего, как пояснил Фёдор Музалевский, на основании банковских выписок и журнала работы системы ДБО. Надо отметить, что у банка было ДБО собственной разработки, довольно старое и не имевшее лицензии настраивания средств контроля защищённости информации (СКЗИ). СКЗИ банк приобрёл у внешнего вендора, они, как подчеркнул эксперт, были качественными, но при этом неверно встроенными, что, естествен-

но, сказалось на эффективности их работы.

В основу механизма хищения легла сама возможность копирования ДБО и ключей. У клиента стояла версия системы «банк-клиент», которая на момент хищения уже два года как устарела. При этом у банка были и новые версии ДБО, и в этих версиях была предусмотрена двухфакторная аутентификация, но по какой-то причине банк версию для клиента не обновил. И это тоже привлекло внимание следствия.

Отметим, что из вышеописанного можно извлечь, как минимум, следующее: пострадавший в результате хакерской атаки банк явно не уделял должного внимания технологической стороне своей информационной защиты. Ещё одной проблемой стало совмещение ролей разработчика и администратора программного обеспечения, хотя штатное расписание банка позволяло «развести» эти полномочия. Однако этого не было сделано, и, к сожалению, как дал понять Фёдор Музалевский, подоб-

ная ситуация «вскрывается» при проведении внешнего аудита состояния ИБ в разных банках до сих пор, несмотря на то, что это прямо запрещено положением Банка России 382-П.

«ЛИПОВЫЙ» ТРАНШ И ПРОЧИЕ НЕПРИЯТНОСТИ

Дальше — больше. Как рассказал Евгений Царёв, эксперт RTM Group, в марте 2016 года к нему обратился руководитель пострадавшего банка с просьбой оказать юридическую помощь в деле о краже средств путём кибермошенничества. К тому времени с момента расследования прошло уже больше девяти месяцев, дело то приостанавливалось, то возобновлялось. «В первую очередь я проанализировал работу следователей по уголовному делу и работу адвокатов по арбитражному делу. Исходя из «первички», получалось, что следствие ограничилось арестом лица, с IP-адреса которого была осуществлена атака, и поиском лиц, на счета которых были перечислены денежные средства, —

это четыре юридические фирмы, созданные всего за месяц до кибератаки. Как правило, лица, которым принадлежат такие фирмы — это люди, ведущие аморальный образ жизни, наркоманы и алкоголики, то есть заведомо понятно, что они не являются «драйвером» преступной группировки», — рассказал Евгений Царёв. После перечисления средств на счета подставных фирм деньги перевели на счета физлиц и обналичили.

В этой ситуации эксперта смутила скорость, с которой были совершены все эти операции, поэтому было решено проверить в первую очередь всех сотрудников банка, в том числе и на полиграфе. Результаты проверки оказались отрицательными. Далее внимание экспертов привлекло то, что в ходе атаки была даже не сломана, а скорее уничтожена программа «банк-клиент», поскольку восстановить информацию на жёстком диске оказалось невозможным.

«Пришлось обратиться за помощью к «бумажной» составляющей документооборота. Проще говоря, я брал банковские платёжные документы в бумажном виде и анализировал их. Анализ привёл меня к странным результатам: подсчитав все средства, зафиксированные «на бумаге», я обнаружил, что на момент хищения денег на счёту банка было на несколько десятков миллионов меньше, чем якобы похитили злоумышленники. Второй, настороживший меня, момент заключался в том, что само хищение было произведено в обеденный перерыв в пятницу, а банк-клиент был восстановлен на новом компьютере только в среду следующей недели. То есть прошло достаточно много времени, и это удивительно, если учесть, что у банка каждая минута на счёту», — рассказал специалист.

Стремясь до конца уяснить себе суть произошедшего, эксперты запросили выписки в банке. И выяснилось, что накануне хищения была совершена операция по зачислению кредитного транша на расчётный счёт одного из клиентов. При этом практически тут же стало понятно, что «в товарищах», то есть между сотрудниками банка и клиентом, на счёт которого был зачислен транш, «согласия нет». Сотрудники утверждали, что они действовали согласно одобрен-

ному банком клиентскому запросу о получении кредита. Клиент, со своей стороны, утверждал, что никакого запроса он не подавал. Банк представил суду заявку на получение кредита, банковский ордер и все документы, свидетельствующие о том, что за полчаса до хищения на счёт клиента была доначислена сумма в 60 млн рублей.

На первый взгляд, могло показаться, что врёт именно клиент, коль скоро на руках у банковских сотрудников есть все необходимые документы. Но в ходе дальнейшего расследования выяснилось следующее: сначала было совершено обрушение системы «банк-клиент» — примерно в 12 часов дня, а спустя две минуты после этого с другого IP-адреса «залетели» подложные платёжные поручения. Из-за «обрушения» клиент, на счёт которого были перечислены 60 млн рублей, не мог видеть, что происходит с его счётом. При этом в 11.50, то есть за десять минут до атаки, выписки о состоянии счёта запрашивались как самим клиентом, так и злоумышленниками с IP-адреса, откуда впоследствии были посланы «липовые» платёжные поручения. «Я думаю, сотрудники банка не могли не заметить этого обстоятельства», — резюмировал Евгений Царёв. Естественно, что далее под подозрения попал уже не столько клиент, расчётный счет которого так удачно «обогатился» в результате атаки, сколько те, кто имел то или иное отношение к совершению операции по переводу кредитного транша.

Результатом арбитражного дела, как пояснили эксперты, стало то, что операционист банка, персональные данные которой использовались при переводе кредитного транша, призналась в здании суда, что кредитный транш проводила не она, а другой сотрудник банка.

ЧТО В ИТОГЕ?

Один из главных выводов, который можно сделать на основании этого кейса, заключается в том, что злоумышленники «замаскировали» атаку под стандартное сочетание таких факторов, как недолжное исполнение сотрудниками своих обязанностей плюс технологическое несовершенство средств защиты. На деле же имело место мошенничество, совершённое внешни-

ми злоумышленниками с помощью тех, кого принято называть «внутренними кротами». Можно так же предположить, что руководство и собственники банка не уделяли должного внимания решению проблем ИБ в своей организации.

Итак, какие выводы? Да все те же, уже не раз сделанные как на уровне регулятора, так и на уровне бизнес-сообщества. Этот кейс их только «подсвечивает» и подтверждает.

1. Необходима чёткая система контроля за действиями пользователей системы.

2. Необходима работа по повышению уровня грамотности сотрудников в вопросах информационной безопасности.

3. Технологические средства обеспечения ИБ должны своевременно обновляться.

4. Необходим внешний аудит ИБ-систем, поскольку практика и в данном, и в других случаях показывает, что именно внешний аудит является максимально эффективным инструментом выявления «лакун» и пробелов в системе ИБ.

* * *

Прежде чем поставить точку, следует обратить внимание ещё на один момент. Как говорилось в известном советском фильме, «лёгким движением руки брюки превращаются в элегантные шорты». В данном случае по результатам расследования банк легко превратился из пострадавшего в объект пристального и не слишком доброжелательного внимания, поскольку, во-первых, к совершению преступления был причастен круг его «неустановленных сотрудников», а во-вторых, у суда возникли вопросы по теме должного обеспечения банком своей информационной безопасности. Даже на основании краткого изложения всех обстоятельств хищения очевидно, что пострадавшая финансово-кредитная организация не предприняла всех возможных и необходимых действий для самозащиты от хакерских атак. И это, безусловно, также оказало влияние на дальнейшую судьбу банка.

TASKMASTERS: ДЕВЯТЫЙ ГОД СТАЛ РОКОВЫМ

Рositive Technologies и «Лаборатория Касперского» выявили группу киберпреступников, которая девять лет производила атаки на российские компании и госструктуры с целью кражи данных.

Известно, что группа скомпрометировала более 30 компаний из сфер промышленности, строительства, энергетики и недвижимости. 24 из них находятся в России.

В коде инструментов хакеров есть следы китайских разработчиков. Также во время ряда атак были замечены подключения с IP-адресов из Китая. Ключи для используемых программ встречаются на китайских форумах. Для взлома использовался планировщик задач операционной системы, поэтому группу киберпреступников называли TaskMasters.

Проникая в локальную сеть, хакеры исследовали инфраструктуру, находи-

ли уязвимости, заводили вредоносные программы и использовали их для удалённого шпионажа. Цели получения информации неизвестны.

В «Лаборатории Касперского» отмечают, что скорее всего эта же группа хакеров известна под именем BlueTraveler — её целями также являются госструктуры РФ и СНГ, и они также используют метод закрепления в инфраструктуре и дальнейшего распространения с помощью планировщика задач.

Группа тщательно скрывает следы — гигабайты информации были украдены, прежде чем антивирусы или службы ИБ замечали присутствие злоумышленников.

Руководитель отдела динамического анализа вредоносного кода Group-IB Р. Миркасымов комментирует ситуацию: «Эксплуатация легитимных утилит позволяет киберпреступникам

оставаться незамеченными, скрыв следы вредоносной активности за действиями пользователей».

Случай с TaskMasters необычен тем, что используемая утилита является легитимной, но не входит в стандартный состав ПО, используемый на большинстве узлов инфраструктуры. Стоит отметить, что планировщик задач также был использован и преступными группами Cobalt и MoneyTaker для атак на банковский сектор.





Александр БОДРИК
управляющий партнёр
бизнес-инкубатора
по кибербезопасности
MoscowCyber.io, вице-
президент по ИБ ISACA
Moscow Chapter

МОСКОВСКАЯ КИБЕР-ШПАНА

Пока крупные производители ПО по кибербезопасности бьются за сертификаты и лицензии регуляторов, на горизонте появилась новая генерация предпринимателей (стартапов).

Новые предприниматели не любят привлекать инвестиции, они годами работали в отрасли до старта своих компаний, хорошо понимают корпоративную специфику и не верят в расхожие мысли «Без блата не пробиться», «На Западе нас не ждут», «Газпром покупает только у своих» и т.п. Своей задачей они видят поиск и решение глобальных проблем ИБ — неудобной, слабой и долгой аутентификации в цифровых сервисах, «человеческого» фактора в ИБ, сложности управления ИБ сотнями и тысячами активов в разных странах, оркестрации инцидентов и информации о киберугрозах.

Приведу примеры ИБ-предпринимателей новой генерации (в алфавитном порядке).

АНТИФИШИНГ (ООО «Антифишинг»). Созданная в 2016 году компания из Твери всего за пару лет заключила контракты с Ростелекомом, QIWI и Банком Санкт-Петербург. Вероятно, помогли ей правильно выбранное стратегическое направление «Решение проблемы человеческого фактора в ИБ» и обширный практический опыт основателей (пен-тестеры из именитой компании и CISO кластера стран международной группы). Предприниматели позиционируют свой продукт как «платформу измерения и развития навыков в области информационной безопасности», ведут психологические исследования, исследования цифровых атак и выпустили более 120 открытых дайджестов с информацией об актуальных атаках (blog.antiphish.ru).

COUCH (ООО «Инксекьюрити»). Сформировавшаяся выходцами из крупных аудиторских отделов системных интеграторов «Инксекьюрити» последние четыре-пять лет запомнилась клиентам услугами по практической безопасности — тестами на проникновение, RedTeam, расследованием инцидентов и анализом безопасности приложений. Однако в 2018 году компания разработала решение по управлению активами и конфигурациями информационных систем в целях обеспечения соответствия (technical compliance). Примечательно, что первыми клиентами стали британско-казахские металлургические и энергетические компании, для которых было важно понимать в деталях, какой информационный актив в какое время и каким стандартам безопасности соответствует на глобальном уровне (Казахстан, ЕС, Африка).

IDENTITY BLITZ (ООО «Реак Софт»). Коллектив вендора сформировался при работе над Единой системой идентификации и аутентификации (ЕСИА) государственных услуг России, пользователями которых являются десятки миллионов наших соотечественников. Вендор производит инфраструктуру безопасности для бизнес-приложений — сервер аутентификации (identity provider), плагин для онлайн-подписи документов и коннектор к ЕСИА, делая тем самым доступ к цифровым сервисам более удобным и безопасным.

R-VISION (ООО «Р-Вижн»). Наиболее старая и известная в нашем списке компания, которая начинала с автоматизации подготовки ИБ-отчетности по СТО БР ИББС/382-П и автоматическому формированию моделей угроз

персональным данным. Сейчас ориентирована на развитие способности организаций-клиентов реагировать на инциденты ИБ и оркестрацию информационных потоков о киберугрозах (IRP/SOAR/TIP). Публичные контракты включают Пенсионный Фонд РФ, Газпромнефть, ВТБ и др. Отличается активным набором персонала под растущее число проектов, иногда задавая рынку новые публичные планки по компенсациям сотрудников.

И СОВСЕМ МОЛОДЁЖЬ

Есть и другие примеры предпринимателей, что фокусируются больше на локальном рынке (тренд импортозамещения). Их развитие структурировано несколько иначе и столь яркими кейсами (клиентами) они пока похвастаться не могут. Но примеры вполне достойные. Это и продукт по защищённому созданию и хранению резервных копий RuBackup, и система активного контроля безопасности удалённых АРМ Сакура, и система шифрования, сохраняющего формат EnigmaPro (Format-Preserving Encryption), и некоторые другие.

Общая черта «кибер-шпаны» в стратегии. Несмотря на успешную динамику в России, эти компании смотрят на внешние рынки, ведь глобальная киберпреступность игнорирует национальные границы, и нельзя проактивно защищать российские организации, не имея представительств и интересов за рубежом.

Пожелаем коллегам успеха, ведь именно их проекты показывают нашим зарубежным партнёрам, что в России есть организации, ставящие перед собой задачи по защите не только российских, но и иностранных граждан и организаций.



ПОДСЕВШИЕ НА ИГРУ

РЕПОРТАЖ С ФИНАЛА ПЕРВОГО СЕЗОНА «НАШЕЙ ИГРЫ»

24 июня зрители Youtube-канала BIS TV увидели завершение первого сезона интеллектуального шоу «Наша игра». О чём говорили А. М. Сычев и А. А. Вассерман на финале «Нашей игры»? Чем шантажировали Дениса Батранкова организаторы, чтобы тот собрал команду? На что ещё кроме Игры подсади Лев Шумский и его люди? Куда может завести азарт Антона Шипулина? Читайте не об этом, но о закулисах «Нашей игры».

КАМЕРА. МОТОР

Как и всегда на площадке царила лёгкая суeta. Организаторы улаживали последние технические нюансы, настраивали камеры, свет, проверяли звук и главное — сигнальные кнопки на столах команд. Об их исправности капи-

таны волнуются больше всего, поэтому перед стартом нервно пробуют кнопку на зуб, а точнее — на палец.

Сегодня играют Steak holders (капитан Лев Шумский), Anti-APT-Group (капитан Денис Батранков) и «HeSOCрушимые» (капитан Антон Шипулин).

Зрители равномерно распределились по залу. Самые смелые сели на первые ряды, троешники, маркетологи и организаторы разместились на галёрке. Оттуда было значительно удобней фотографировать специального гостя — Анатолия Вассермана, сидевшего в первом ряду. Его заметили все, но вида не подавали: «Что мы, дикие что ли!» Рядом разместился Артём Михайлович Сычёв (Банк России), его тоже, конечно, заметили, и тут уж вид подавали все.

Камера, мотор, поехали. Игра началась.

ПРЕДЛОЖЕНИЕ, ОТ КОТОРОГО...

«Наша игра» стала совершенно новым для отрасли событием. Беспрецедентным и захватывающим. Антон Шипулин, капитан команды «HeSOCрушимые», рассказывает, что с проектом столкнулся случайно. Однако раз попробовав, уже не смог остановиться.

— Мельком увидел анонс на Facebook и решил подать персональную заявку из любопытства, посмотреть, что это такое изнутри, проверить знания. Первая игра для меня была просто экспериментом, не было явной цели бороться до победного конца. Но после того, как мы не вылетели, а прошли в следующую игру, я задумался, что стоит побороться. И уже в следующих играх появились боевой настрой, расчёт и азарт.

Денис Батранков, капитан команды Anti-APT-Group, попал в игру, став «жертвой» выбора организаторов. Ему позвонили и сделали предложение, от которого — как это водится — отказаться невозможно.

— Я получаю удовольствие от решения сложных задач. И если впереди есть «challenge», то жизнь наполняется смыслом. Я рад, что прошёл это очередное испытание, и «Наша игра» была необычайным удовольствием.

Денис принял эстафетную палочку и тоже стал звонить с предложением Дмитрию Пудову, Дмитрию Кострову, Александру Кузнецову, Сергею Журину, а перед последней игрой — Михаилу Курзину. И какая удача — они тоже не смогли отказаться.

Лев Шумский, большой любитель интеллектуальных игр по ИБ: на его счету, наверно, самое большое количество побед в разных игровых форматах. Он поделился с нами, что «Наша игра» — это хорошая возможность переключиться от ежедневных задач, встретиться с коллегами, профессионалами, друзьями и расширить кругозор. Коллеги, профессионалы, друзья — это одни и те же люди (прим. авт.).

МОТОР. ПОЕХАЛИ

Команды начали осторожно: долго совещались, мало отвечали, «выбивали» дорогие вопросы. Режиссёр начал волноваться об отсутствии драмы, накала страстей и динамики. Подождите, милейший! Пока Anti-APT-Group и «HeSOСрушимые» медленно уходили «в минус», Steak holders под конец первого раунда забрались на верх турнирной таблицы. Почувствовав запах победы (слишком ещё далёкой), лидер стал совершать ошибки.

«Какая ожесточённая борьба!» — вскричал внутренний Дмитрий Губерниев в душе каждого зрителя, когда команда Льва Шумского вступила на тропу невезения и неверно ответила на несколько вопросов подряд, потеряв все свои баллы. В то время, как и Денис Батранков и Антон Шипулин давали верные ответы и оставили далеко позади бывшего лидера.

Несмотря на колебания турнирной таблицы, к финальному вопросу пришли все 3 команды, но реальная борьба

ожидалась только между Anti-APT-Group и «HeSOСрушимыми».

— Какие математики! — заметил Алексей Лукацкий, принимая ставки команд.

На финальный вопрос все три команды ответили неверно.

ТИМБИЛДИНГ ПО-НОВОМУ

Запуская новый проект, организаторы мандражируют: а понравится ли аудитории, а будет ли востребован формат, а как на этот раз нас подведут подрядчики, а где мы ошибёмся, а что если... И так далее и так далее. Теперь, после завершения первого сезона игр, у организаторов всё ещё остались вопросы, но пропали сомнения. Второму сезону быть, командам играть, сообществу формироваться.

Любая из команд-финалистов — отличный пример того, как капитанам удалось заразить своим азартом и объединить одной целью людей из разных компаний: вендоров, интеграторов, клиентов. И провести время исключительно с пользой: узнать что-то новое о безопасности, Лукацком, о коллегах и своих собственных способностях и знаниях.

Победителем первого сезона стала команда Anti-APT-Group, сделав аккуратную ставку и обойдя «HeSOСрушимых». Анатолий Вассерман вручил победителям дипломы, значки «Мастеров ИБ», подарочный сертификат на командное приключение. Денис по секрету рассказал нам, что они выбрали полёт в аэротрубе. Мы секреты хранить умеем, поэтому вам этого не говорили. А самое главное, из рук Вассермана, человека, который стал живым синонимом эрудиции, команда получила «Золотой мозг отрасли» — переходящий символ победы в сезоне «Нашей игры».

Какая судьба ждёт «Золотой мозг» в следующем сезоне? Узнаём! Мотор. Поехали?

Мы благодарим компании «Ростелеком-Solar» и Bi.Zone за поддержку при проведении финального игры сезона. Организатор «Нашей игры» — Медиа Группа «Авангард».

Тамара Чечёткина
специально для BIS Journal



Лев Шумский, капитан команды Steak holders:

— Отрасль обесценила и выхолостила формат конференций, но при этом не смогла удовлетворить потребность в неформальном общении профессионалов, поэтому в последнее время заметна тенденция к формированию кулуарного, клубного формата мероприятий. «Наша игра» — удачная и качественная реализация такой потребности. Мы уже подсели на Игру, и с нетерпением ждём очередного сезона.

Денис Батранков, капитан команды Anti-APT-Group:

— Неожиданно «Наша игра» стала проверкой того, насколько хорошо я знаю людей. Чтобы подобрать команду, нужно очень чётко понимать, кто разбирается в какой отрасли: ICS, банки, нормативные документы, книги, фильмы, история. Чтобы играть в команде, нужно полностью доверять ответам коллег или принимать решение самому, если видишь, что человек сомневается. «Наша игра» — это новый опыт психологии командной игры в условиях ограниченного времени на ответ.

Антон Шипулин, капитан команды «HeSOСрушимые»:

— Не могу себе простить, что у меня из головы магическим образом вылетел ответ на вопрос про первый сертифицированный промышленный межсетевой экран, после того, как я нажал кнопку, чтобы отвечать. Это, конечно, не самые критические 500 баллов в игре, но обидно, что я абсолютно чётко знал ответ и весь его контекст, но внезапно напрочь забыл.

МОЛОДОЙ, ОБРАЗОВАННЫЙ, ЛЮБЯЩИЙ IT

BIS JOURNAL ПРОВЁЛ АНКЕТИРОВАНИЕ
СВОИХ ЧИТАТЕЛЕЙ

Результаты социологического опроса, проведённого BIS Journal на прошедших в Москве PHDays 2019, поведали много интересного о наших читателях — посетителях профильных выставок и соревнований по ИБ.

Наша анкета была простой и отчасти шуточной. Ну, кто, скажите, будет приравнивать хакера к Робин Гуду или спрашивать об ощущениях после взлома сервера крупной компании? Тем не менее, в опросе принял участие 371 человек, полностью ответил на все вопросы 361 человек. Поскольку мероприятия PHDays 2019 посетили более 8 тыс. человек, нашу выборку вполне можно считать репрезентативной, но лишь для потенциальной аудитории журнала BIS Journal.

Итак, «IT — это моё временное увлечение», — полагает 31 человек из всех, заполнивших анкету, другие 330 назвали информационные технологии призванием на ближайшие годы. При этом 137 человек постоянно участвует в таких событиях, как PHDays, 194 следят за ними, и лишь 28 человек оказались на мероприятии случайно.

Кто такой хакер? Если вы ещё не определились с ответом, то 259 ваших коллег считают его смелым экспериментатором, 39 — современным Робин Гудом, и лишь 57 человек полагают, что хакер — банальный преступник. 16 опрошенных не дали ответа на этот вопрос.

Можно ли на досуге взломать сервер крупной мировой компании? 21 человек ответил «не знаю», 39 считают взлом прикольным занятием, позволяющим хорошо провести время, а ещё 92 участника потенциального взлома чув-

ствуют себя профессионалами своего дела. Однако 219 человек (!) ответили, что взлом наказуем и не стоит ломать сервера мировых гигантов.

С реальными взломами не сталкивались всего 35 человек из 357. Пробовали взломать что-то или кого-то 107 человек, 17 ответивших сами стали жертвами взлома, а у 91 хакеры покушались на компьютеры знакомых. Ещё 107 человек на вопрос «Сталкивались ли вы с реальными взломами?» выбрали пункт «иное». Будем считать их пентестерами.

Профессионально занимаются или хотят посвятить свою деятельность информационной безопасности 310 человек, 11 не готовы заниматься кибербезопасностью всю жизнь, а 34 человека ещё не сделали свой выбор. 16 на вопрос не ответили.

Зачем вы посещаете мероприятия по ИБ? За новыми знаниями на PHDays 2019 пришли 214 из 358 ответивших, 46 человек захотели поучаствовать в конкурсах. Ради общения с единомышленниками пришли 98 участников.

В каком возрасте вы впервые услышали об информационной безопасности? — спросили мы в анкете. Практически с пелёнок (с трёх лет) знает об ИБ один ответивший. 207 человек узнали об информационной безопасности в школе (7–17 лет), ещё 108 проанкетированных — в период учёбы в университетах и колледжах (18–24 года). 27 респондентов столкнулись с ИБ в возрасте 25–35 лет. В зрелом возрасте — старше 40 лет — о кибербезопасности услышали 5 человек.

Главный источник знаний об ИБ. Для 103 человек — это интернет-ресурсы, ещё 137 человек получают сведения

от друзей и коллег. 95 человек прослушали образовательные программы, а 9 имеют некий «иной» источник информации.

Нужен ли печатный учебник по ИБ? — спросили мы. «Да», — ответили 213 человек, «нет» — 118. Ещё 14 предпочли пункт «иное», а 26 не ответили на этот вопрос. Остаётся только найти профессионалов, которые написали бы такой учебник.

Про BIS Journal. Наш журнал постоянно читает 31 человек (и это не сотрудники редакции), ещё 179 читают его, как только он попадает в руки (но попадает нечасто), а впервые узнали о BIS Journal 134 человека.

Заинтересованы в получении актуальной информации в сфере ИБ 233 из 328 ответивших. 92 человека полагают, что им такие сведения не нужны.

В заключение про возраст и образование респондентов. Половина опрошенных — молодые люди от 25 до 35 лет (181 человек), ещё 117 — моложе 25 лет (из них 17–19-летних — 16 человек). 28 опрошенных указали свой возраст в интервале 36–40 лет, а ещё 25 — старше 41 года. В колледже учатся 8 человек, 69 получают высшее образование, а 264 человека работают.

Были и школьники, один в возрасте 13 лет, ещё двое — 28 и 39 лет — несколько засиделись за партой. 27 человек на вопрос о роде занятий не ответил.

И последнее. Сервисами mail.ru пользуются 102 человека, gmail.com выбрали 118 респондентов, rambler.ru — 6 человек, сервисы Yandex предпочитают 67 опрошенных, 14 не оставили своих контактов, ещё 64 человека пользуются иными почтовыми сервисами или корпоративной почтой.



РКП Форум

Россия 2019

**XVII международная конференция по проблематике
инфраструктуры открытых ключей и электронной подписи**

**г. Санкт-Петербург
17–19 сентября 2019 года**

www.pki-forum.ru



**Встречаемся
в Питере!**

АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Образование
и карьера

ib-bank.ru