

10> Людмила БОКОВА
Совет Федерации ФС РФ
Научить граждан безопасности!



16> Роман ШЕРЕДИН
Россвязь
Кто чистит трафик?



20> Василий ОКУЛЕССКИЙ
АО НСПК
Функциональность = безопасность

26> Григорий СТЕПАНОВ
Сбербанк
Как доверять?

52> Алексей ЛУКАЦКИЙ
эксперт
К SOCy готов? Подумай!

О НОВЫЙ МИР!

ВЫПУЩЕНО 5 МЛН ПЛАТЕЖНЫХ КАРТ «МИР»



SOC-FORUM 2017

Практика противодействия кибератакам
и построения центров мониторинга ИБ

22.11.17

Москва (Конгресс-парк «Украина»)

soc-forum.ib-bank.ru



Игорь НЕКРАСОВ
главный редактор
BIS Journal

О новый мир! Стоит, наверное, объяснить по поводу обложки. Безусловно, она многозначна. Прекрасные бабочки — это не только пять миллионов карт «МИР», а скрупулезно изображенный титанический труд по их производству — не только НСПК. Отчасти картина навеяна солнцем, летом и изображает томление перед отпуском, но в большей степени все же — ситуацию в ИБ и содержание нового номера BIS Journal!

Итак, разноцветье и многообразие тем, имен, фактов, мыслей. Которые сами по себе, почти без редакторского диктата, складываются в тренды и тенденции. Кажется, вот-вот, в начале зимы Александр Баранов констатировал на наших страницах, что ключевая проблема банковской безопасности — проблема идентификации и аутентификации — принципиально не решается и вряд ли решится в ближайшее время, и вот, пожалуйста, всего за полгода, будто в учебном мультфильме: личинка — куколка — гусеница — бабочка! Много бабочек! Банк России рассказывает о концепции Единой Системы Идентификации и Аутентификации, Сбербанк выстреливает серьезнейшей статьей «Как доверять?», Банк ВТБ представляет свои идеи, а Василий Окулесский просто дразнит, интригует и бросает вызов. Цитируем: «Мы стоим на пороге маленькой революции в обеспечении безопасности, и эта революция называется „MirAccept 2.0“. Это сервис надежной аутентификации Держателя Карты ПС „Мир“...» Подробности, правда, невелики, но к следующему номеру, надеемся, можно будет рассказать и побольше.

Также — стихийной волной — выплеснулась тема повышения осведомленности граждан. Совет Федерации, Банк России и другие делятся своими обучающими проектами и опытом их внедрения. А еще в этом номере много интересного и полезного про SOC, блокчейн, а из совсем нового — про мало осмысленное еще явление «город как пространство доверия», а также про недавно созданный Фонд содействия развитию безопасных информационных технологий. Возникновение такого фонда — событие незаурядное, знаковое. Как сказано в статье о нем, «...наша отрасль растет и множится», и по велению времени в действие вступают «механизмы саморегулирования и общественной поддержки».

А чисто по-человечески встревожила статья про вирусы-вымогатели и вредоносное ПО, требующее выкуп за возврат доступа к данным. В той части, где вымогатели предлагают пользователю вместо платежа разослать «ссылочки» своим друзьям. Если хотя бы двое из них заплатят, пользователь получит ключ расшифровки бесплатно. Представьте это явление в развитии и масштабной перспективе, когда почти все население планеты будет вынуждено периодически делать подобный выбор. Времена политических доносов покажутся пионерским лагерем.

Бабочки бабочками, но, если кто и спасет мир в такой ситуации, то только ИБ.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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

Сычев А.М. — заместитель начальника Главного управления безопасности и защиты информации

Банка России, кандидат технических наук, доцент

Шпилов В.В. — исполнительный директор Ассоциации

российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

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

Велигура А.Н. — председатель комитета по банковской

безопасности Ассоциации российских банков,

руководитель комитета по безопасности НП «НПС»,

CISA, кандидат физико-математических наук

Виноградов А.Ю. — начальник управления

информационной безопасности АО КБ «Златкомбанк»

Вихорев С.В. — директор по информационной безопасности

Филиала «ПЕТЕР-СЕРВИС Спецтехнологии»

Дзержинский Ф.Я. — главный эксперт — координатор

системной экспертизы блока «информационные

технологии» ПАО «Промсвязьбанк», CSDP

Зубков А.Н. — генеральный директор ООО «Медиа

Группа „Авангард“, директор Фонда содействия развитию

безопасных информационных технологий (ФСРБИТ)

Курило А.П. — главный советник, компания «РНТ», кандидат

технических наук

Левинов Д.О. — председатель Совета НП «Партнерство

специалистов по информационной безопасности»

Мельников С.Ю. — заместитель генерального директора

ООО «Лингвистические и информационные технологии»,

кандидат физико-математических наук

Некрасов И.В. — главный редактор журнала

Окулесский В.А. — начальник управления безопасности

АО «НСПК», кандидат технических наук

Пазин С.В. — начальник Управления по обеспечению

информационной безопасности ОАО Банк ВТБ, кандидат

физико-математических наук

Шумский Л.С. — начальник Управления контроля

информационных рисков, ДОР (АО) Связной Логистика

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

Филиппчук А.А. — вице-президент АБ «ГПБ-ипотека»

(группа «Газпромбанка»)

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**

Шеф-редактор: **Былевский П.Г.**

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

Арт-директор: **Мельников Н.С.**

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

Северный В.П., Хвастунова О.Н.

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

Фото в номере: фотобанк DepositPhotos, waralbum.ru,

Салаватова Я.М.

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

Цветокорректор: **Науменко М.Б.**

Корректор: **Бальтерманц Л.Ф.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»

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

д.21 (м. «Достоевская»)

Координаты: 55.779380, 37.61150

Тел./факс: +7 499 271-70-85

Интернет-версия: journalib-bank.ru

E-mail: bis@ib-bank.ru

Отдел рекламы: reklama@ib-bank.ru

Отдел распространения: tirazh@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной

службой по надзору в сфере связи, информационных

технологий и массовых коммуникаций (Роскомнадзор).

Свидетельство ПИ № ФС77-55062 от 14 августа 2013 г.

Все права на материалы, опубликованные в номере,

принадлежат журналу «BIS Journal — Информационная

безопасность банков».

Перепечатка и воспроизведение иными способами

без разрешения редакции запрещаются.

При использовании материалов

ссылка на журнал обязательна.

Мнение редакции может не совпадать с мнением авторов.

Присланные материалы не рецензируются

и не возвращаются.

Подписан в печать 03.07.2017. Тираж 7000 экз.

Заказ № 789/D-7. Цена договорная.

Отпечатан в «Типографии на Угрешской»

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

Тел.+7 495 720-62-28

© BIS Journal, 2017

НОВОСТИ

5 В России, в мире, криминал

РЕГУЛЯТОРЫ

10 **Совет Федерации**
Людмила БОКОВА (Совет Федерации)
Научить безопасности

13 **Идентификация**
Максим ГРИГОРЬЕВ (Банк России)
Узнать издалека

16 **Россвязь**
Роман ШЕРЕДИН (Россвязь)
Кто чистит трафик?



БАНКИ

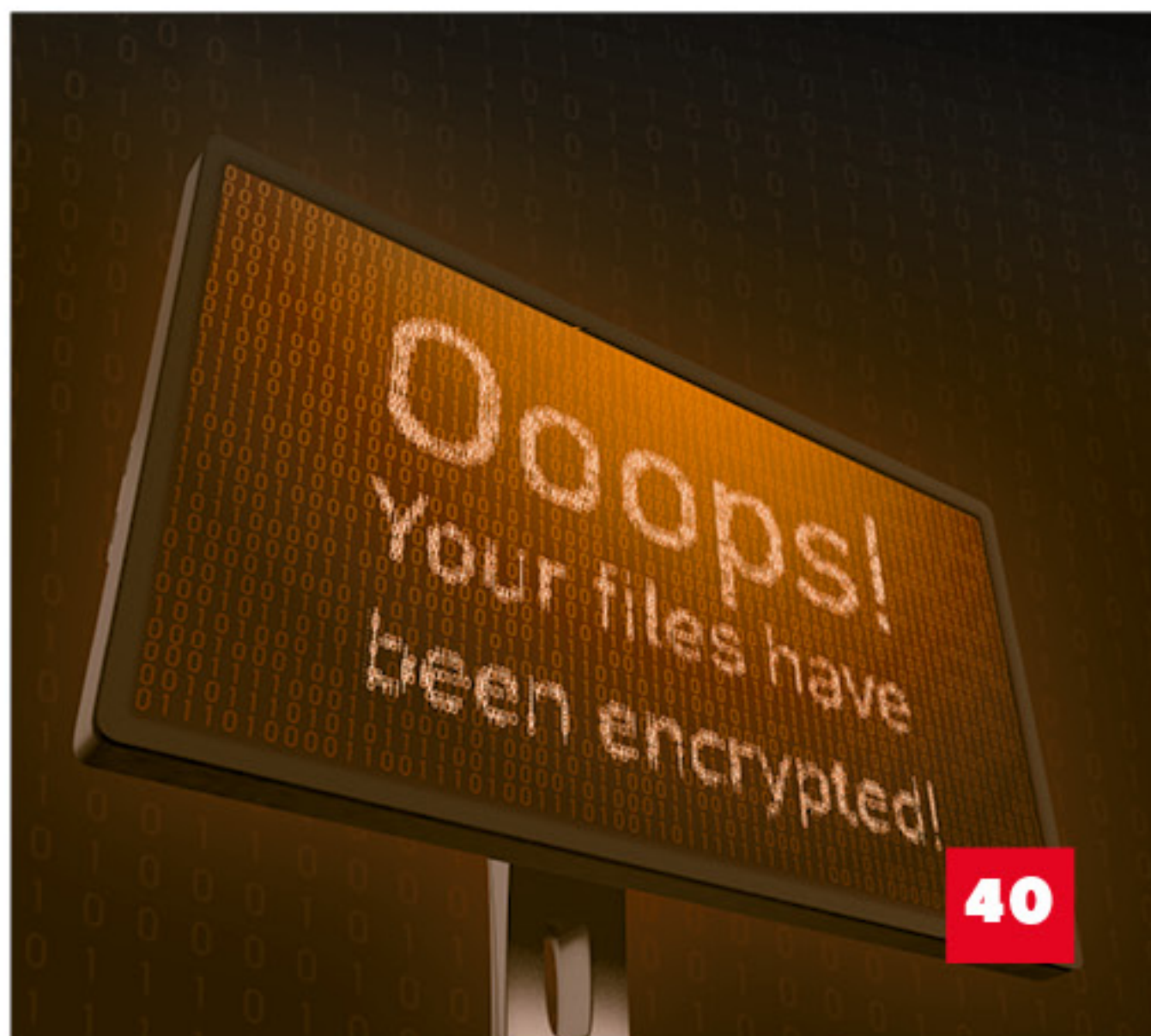
20 **НСПК**
Василий ОКУЛЕССКИЙ (НСПК)
Функциональность = безопасность

26 **Законодательство**
Григорий СТЕПАНОВ (ПАО Сбербанк)
Как доверять?

32 **Облачные технологии**
Андрей КУРИЛО (НП НСФР)
Трудный путь к универсуму

36 **Биометрия**
Антон МИТРОФАНОВ (ПАО Сбербанк)
«Объект опознан!»





УГРОЗЫ И РЕШЕНИЯ

40 Тенденции

Сергей МЕЛЬНИКОВ (ООО «Лингвистические и информационные технологии»)

Александр ПАЛЬЦЕВ (Savoy Development Ltd)

Кибервымогательство. Новый тренд компьютерных преступлений

44 VPN

Андрей ШПАКОВ (ООО «С-Терра СиЭсПи»)

Какой VPN выбрать?

46 Управление безопасностью

Антон СВИНЦИЦКИЙ, Виктор СЕРДЮК

(АО «ДиалогНаука»)

Основные векторы атак на банки

48 Облачные технологии

Станислав СМЫШЛЯЕВ, Павел СМИРНОВ,

Сергей АГАФЬИН (КриптоПро)

Неизвлекаемые ключи в облаке — путь через криптопровайдер



ИНФРАСТРУКТУРА

52 Деловые мероприятия

Алексей ЛУКАЦКИЙ (эксперт информационной безопасности)

К SO Су готов? Подумай!

56 Деловые мероприятия

Уроки Летней сессии

58 Деловые мероприятия

Беларусь — Россия: безопасность — задача общая

60 Деловые мероприятия

Артем ЗУБКОВ (ФСРБИТ)

Новый источник энергии

63 Блокчейн

Марина БРОДСКАЯ (BIS Journal)

Скованные одной цепью

68 Концепция

Александр БОДРИК (ГК Иридис)

Город как пространство доверия



ОБРАЗОВАНИЕ И КАРЬЕРА

- 72** **Персонал**
Игорь ДОЛОТИН (UBS)
Как повысить?
- 74** **Обзор**
Марина БРОДСКАЯ (BIS Journal)
СТФ. Большой транзит

СУБЪЕКТЫ

- 78** **Корифеи**
Геннадий ЕМЕЛЬЯНОВ (Академия
криптографии РФ)
Дмитрий ЛАРИН (кандидат технических наук)
Шифры трех войн. О мастере взлома кодов
Б.А. Аронском
- 84** **Корифеи**
Борис СТОЛПАКОВ (историк криптографии)
Сто лет назад. Триумф и трагедия радиоразведки
Балтийского флота
- 88** **Мысли вслух**
Сергей ВИХОРЕВ (ООО «ПЕТЕР-СЕРВИС
Спецтехнологии»)
Обезличивание: количество убивает качество
- 93** **Мысли вслух**
Александр БОДРИК (ГК Иридис)
Конвейер кибербезопасности для 200 ИТ-
проектов в год

ОФФТОПИК

- 96** **Блогеры улыбаются**
Кроссворд, юмор



ГОСДУМА ОДОБРИЛА ИДЕНТИФИКАЦИЮ В МЕССЕНДЖЕРАХ

Госдума Российской Федерации приняла в первом чтении законопроект, регулирующий деятельность мессенджеров. Инициативу поддержали 356 депутатов, двое проголосовали против и один воздержался.

В конце мая представители «Единой России», «Справедливой России» и КПРФ внесли на рассмотрение законопроект, предусматривающий обязательную идентификацию пользователей в мессенджерах. Документ определяет понятие сервисов мгновенного обмена сообщениями, а также прописывает их обязанности. Помимо идентификации пользователей, мессенджеры обязаны обеспечить рассылку по инициативе органов государственной власти, а также ограничить рассылку и передачу сообщений, содержащих противоречащую законодательству информацию. Идентифицировать пользователей предполагается по абонентскому номеру.



Ранее глава Роскомнадзора Александр Жаров поддержал законопроект. При этом он заявил, что документ не предполагает контроля за частной перепиской граждан и не посягает на свободу слова. В свою очередь, в Федеральной антимонопольной службе раскритиковали инициативу, указав, что она предоставляет иностранным корпорациям возможность доступа к базе данных российских абонентов, а это нежелательно.

В РКЦ ИСПЫТАЛИ КВАНТОВЫЙ БЛОКЧЕЙН

Ученые Российского квантового центра (РКЦ) первыми в мире протестировали технологию квантового блокчейна.

Квантовый блокчейн — система распределенного хранения данных, реализованная с помощью квантового распределения ключа. Представители РКЦ заявляют: «Технология позволяет обойтись без посредников и третейских судей, которые контролируют честность сделки и наказывают за мошенничество. Футурологи полагают, что на базе блокчейна будет создана экономика будущего —



без арбитражных судов, банков и налоговой полиции».

Главной угрозой новой технологии может стать появление у злоумышленников квантовых компьютеров. По словам научного сотрудника РКЦ Алексея Фролова, соавтора разработки, в теории квантовый компьютер легко сможет решать математические задачи, на которых основана защита блокчейна. Фролов сказал: «Для большей безопасности платформы мы использовали квантовую криптографию, то есть в нашей сети мы заменили цифровую подпись пользователя на квантовые коммуникации, так что безопасность системы защищают законы квантовой физики». По мнению РКЦ, к середине 2020-х технологии блокчейна позволят производить услуги на \$62 трлн.

БАНК РОССИИ. НОВЫЙ ГОСТ



Банк России
Центральный банк Российской Федерации

Банк России разработал новый ГОСТ, согласно которому кредитно-финансовые организации должны внедрить у себя более 400 мер информационной защиты.

Документ вступит в силу в 2019 году, но, как сообщила пресс-служба Центробанка, 329 организаций уже приступили к внедрению нового ГОСТа. По мнению экспертов, банкам придется потратить до 15% от чистой прибыли на модернизацию своих систем в соответствии с требованиями нового стандарта.

Напомним, что размер краж с банковских карт граждан за год снизился на 55%, достигнув отметки 1,7 миллиарда рублей. По прогнозам Банка России, в текущем году этот уровень существенно снизится.

НОВОСИБИРСК. ЦЕНТР КИБЕРБЕЗОПАСНОСТИ В ГОССЕКТОРЕ

По распоряжению губернатора Новосибирской области Владимира Городецкого в Новосибирске создается Центр защиты информации НСО.

Основное направление деятельности Центра — поддержание стабильной работы государственных информационных систем региона. Предполагается, что Центр повысит уровень защищенности этих систем и сократит общие расходы на их киберзащиту до 40%.

Специалисты новой структуры будут заниматься созданием централизованных систем защиты, аттестацией по требованиям к безопасности госинформационных систем, обеспечением функционирования защищенных сетей областных исполнительных органов власти.

ХАКЕРЫ ОБМА- НУЛИ СКАНЕР ГЛАЗА

Участники немецкого хакерского объединения CCC взломали систему аутентификации по радужке глаза, которая применяется в Samsung Galaxy S8.

Глаз владельца смартфона нужно сфотографировать, применив функцию «ночного режима». Далее снимок распечатывается на лазерном принтере, на изображение для имитации кривизны накладывается контактная линза. С таким нехитрым приспособлением Samsung Galaxy S8 оказалось легко обмануть: смартфон воспринял фотографию с линзой за настоящий глаз владельца.

Производители позиционировали аутентификацию по радужке глаза как супернадёжную защиту и интегрировали ее с платежным сервисом Samsung Pay. Представитель CCC Дирк Инглинг посоветовал всем, кто дорожит данными на своем смартфоне, использовать обычный PIN-код, который гораздо надежнее.

КИТАЙ. 2 МЛН ВРЕДОНОСНЫХ ПРОГРАММ

Китайский Национальный центр интернет-безопасности опубликовал отчет, в котором говорится, что только в прошлом году выявлено более 2 млн новых вредоносных программ, созданных на территории страны.

Наиболее уязвимой для хакерских атак стала система Android. Однако дело не в конструктивных недочетах, а в стремлении хакеров атаковать именно эту систему. По данным Национального центра, в КНР функционируют 2,5 млрд коммуникационных устройств. Из них 2 млрд на платформе Android.

Специалисты только констатируют массовые запуски вредоносных программ на Android, но не могут установить причину такой активности взломщиков. Эксперты говорят о финансовой составляющей в действиях хакеров.

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ В БАНКЕ

В июне банк BNP Paribas объявил о запуске услуг с использованием виртуальной и дополненной реальности (VR/AR) по трем направлениям — розничный банкинг, консалтинг в сфере покупки недвижимости и страхование мобильных устройств.

По словам представителя банка, инструменты с применением VR/AR постепенно станут частью повседневной жизни. Например, клиенты смогут пройти виртуальную экскурсию по заинтересовавшим их объектам недвижимости, не тратя время на поездки.

В последнее время все больше банков обращают внимание на VR/AR. Национальный банк Омана использует приложение дополненной реальности, которое, подобно игре Pokemon Go, позволяет при помощи смартфона найти ближайшее отделение или банкомат. Американский банк Wells Fargo работает над созданием масштаб-



ной виртуальной презентационной площадки. Он уже отправляет клиентов в виртуальный исторический тур по старой Америке. Банк Citi проводит для своих клиентов виртуальные концерты многих звезд и эксклюзивные интервью с ними.

Эксперты считают, что использование VR/AR поможет увеличить выручку. К 2020 году по самым пессимистичным подсчетам выручка компаний во всем мире от использования этих технологий составит \$14,6 млрд, а при самом оптимистичном — \$126 млрд.

ТАК ВОТ КТО ВЗЛОМАЛ ПЕНТАГОН!

В Национальном криминальном агентстве Великобритании наконец-то обнародовали имя 25-летнего киберпреступника, получившего доступ к данным Пентагона. Он выкрал личные данные о служебном положении сотрудников Минобороны США, а также взломал спутниковую коммуникационную систему. Пентагон оценил ущерб от атаки в \$638 тысяч.

Кибератака была совершена 15 июня 2014 года. После этого хакер выложил скриншоты личных данных сотрудников Пентагона в свободный доступ в Сети.

Правоохранителям удалось задержать британского хакера только через девять месяцев — в марте 2015-го, после того, как разведка выяснила, что именно он был причастен к взлому. При задержании на его жестких дисках нашли украденные данные, а также выявили учетную запись, с ко-

торой были размещены личные сведения о сотрудниках Минобороны США.

До заседания суда британские власти не раскрывали информацию о личности хакера. Теперь стало известно, что киберпреступник — это Шон Кэффри, житель города Саттон Колдфилд. На суде в Бирмингеме он признал вину за вменяемые ему преступления. Многочисленные поклонники считают его последним героем из поколения хакеров-романтиков.





Лучшие в России – 2016

24 Апреля в Меркурий Сити Тауэр при поддержке РСПП состоялась торжественная церемония награждения лауреатов бизнес-премии Лучшие в России – 2016/Компании, Персоны, Проекты Года.

Церемония прошла в стиле фильма «Пятый элемент». Открыли ее известный шоумен харизматичный мужчина Иван Траоре и ведущая канала РБК-TV Елена Хрупова, а атмосферу торжественности, таинственности и непринужденности создал эффектный номер балета «Тодес».

Героев года чествовали знаменитая телеведущая Анна Шатилова; кинопродюсер Борис Грачевский; член бюро правления РСПП Давид Якобашвили; Президент МТПП Владимир Платонов; российский политический деятель, финансовый омбудсмен Павел Медведев; генеральный директор ММБА, Председатель Комитета Торгово-промышленной палаты России по развитию потребительского рынка Александр Борисов; Председатель Комитета ТПП РФ по финансовым рынкам и кредитным организациям Владимир Гамза; актриса, юмористка и пародистка Елена Воробей; экономист Михаил Делягин; художник Никас Сафронов; актриса Ирина Безрукова; актриса Яна Поплавская; Президент Российской академии общественных связей Виталий Расницын.

Премия «Персона года» в номинации региональная власть получил Президент республики Татарстан Рустам Минниханов. Диплом победителя был вручен представителю Президента республики. Отмечая один из наиболее инновационных и успешных проектов в Татарстане – электронное правительство, Первый заместитель Полномочного представителя Республики Татарстан Ильдар Мухамедьяров сказал: «Главное – это наше общее сознание. Если мы все вместе что-то захотим – у всех все получится. Мы ставим во главу угла качество жизни людей. Благодаря электронному правительству мы смогликратно увеличить скорость реагирования и принятия решений. Наш успех – это общий успех».

Достижения портала Banki.ru в 2016 году были отмечены в категории «Проект года» в номинации MARKETPLACE: «Мы исторически сильны журналистским контентом. Сейчас стоит цель монетизировать наши знания и информацию. Banki.ru будут развиваться как финансовый супермаркет, где «на полках» находятся финансовые услуги: депозиты, кредиты, страховки, продажа недвижимости со скидкой и т.д.», – сказала исполнительный директор Банки.ру Елена Ищеева.

«Персоной года» в ОБЛАСТИ МЕДИЦИНЫ стала доктор медицинских наук, пластический хирург Наталья Мантурова: «90% поставленных целей я достигла, во многом, благодаря симбиозу работы моих коллег, друзей, сотрудников. Пластическая хирургия – это не только операции и аппаратная косметология, но и смежные области, и новая образовательная программа, которая поможет достичь нашей отрасли новых высот».

Компаний года в номинации IT/ТЕЛЕКОМ стало ОАО «Межрегиональный ТранзитТелеком». «Все разработки МТТ в сфере телекоммуникаций и IT направлены на то, чтобы помогать российскому бизнесу становиться эффективнее и стабильнее,

предоставляя ему такие инновационные «облачные» инструменты как платформа «МТТ Бизнес». Мы очень рады тому, что наша работа была признана и поддержана деловым сообществом России, теми, кто вдохновляет нас и для кого мы создаем наши новые сервисы», – отметила директор по корпоративным коммуникациям ОАО «МТТ» Анна Бойко.

В категории «Компания года» – негосударственным пенсионным фондом стал АО «НПФ Сбербанка». «Выражаем слова благодарности организаторам, Экспертному совету, партнерам и всем участникам церемонии. Признание заслуг очень важно для нас. Это придает новые силы для нашей работы на благо страны и наших клиентов. НПФ Сбербанка продолжает сохранять лидирующие позиции на пенсионном рынке России благодаря профессиональной работе сотрудников Фонда и ПАО Сбербанк. По итогам переходной кампании 2016 года число клиентов увеличилось до 7,4 млн. чел. и активы достигли 450 млрд. руб. Такими показателями можно гордиться. Мы ведем постоянную работу по внедрению новых технологий, развитию каналов продаж, эффективному управлению инвестиционным портфелем и постоянному улучшению качества работы. Демонстрация оптимального баланса доходности и надежности позволяет нашим клиентам быть уверенными в своих пенсионных накоплениях. Мы предлагаем всем заранее выбрать достойное будущее для себя и своих близких вместе с НПФ Сбербанка, – отметила Елена Тетюнина, заместитель генерального директора».

«Персона года» в области ОБРАЗОВАНИЯ ректор Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации Владимир Мау считает: «В обучении будущих российских экономистов будет расти роль «активных методов», проектной работы, образование будет все более международным и индивидуальным. Студент сможет выбирать те программы и курсы, которые он посчитает наиболее важными для его ближайших и отдаленных перспектив».

Управляющий директор компании «АМФ-международная сеть доставки цветов» Мария Пласковицкая отметила главные достоинства «Проекта года» в номинации услуги: «Качество и Сервис»: Мы стараемся разработать такие варианты, чтобы можно было найти предложение на любой вкус. Мы умеем воплощать самые смелые мечты, самых требовательных клиентов».

«Персона года» в номинации «Алкогольная промышленность» президент группы компаний Simple Максим Каширин отметил, что любит свое дело и достигает поставленных целей вместе с командой единомышленников. «Год был непростой, большое количество задач и целей, но команде удалось достичь многого: мы провели ребрендинг сети винотек SimpleWine, запустили собственный бренд «Онегин» и грузинскую линейку вин Shildis Mtebi, точно усилили портфель брендов – у нас появились такие бриллианты как австралийский Penfolds и французский Darroze. Винный бар Grand Cru совершил несомненный прорыв и остаётся Меккой для всех ценителей вина и гастрономии, а наш бренд-шеф Адриан Кетглас получил звезду «Мишлен».



Наталья Касперская - Президент Группы компаний InfoWatch, соучредитель «Лаборатории Касперского»; Елена Борщёва - актриса, ведущая; Ирина Безрукова - актриса, телеведущая; Артем Инютин - сооснователь фонда TMT Investments и медиахолдинга РБК



Наталья Мантурова
Доктор медицинский наук,
пластический хирург



Анна Бойко
Директор по корпоративным
коммуникациям ОАО «МТТ»



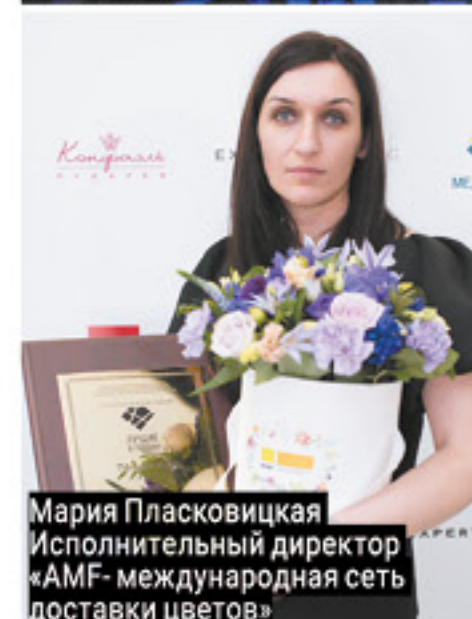
Владимир Мау
Ректор РАНХиГС



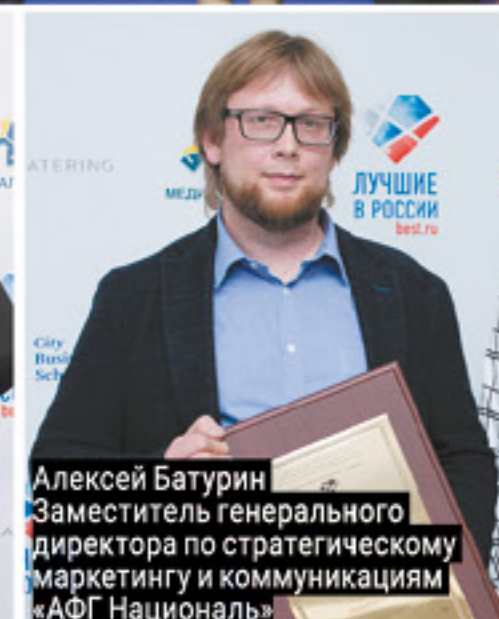
Елена Тетюнина
Заместитель генерального
директора НПФ Сбербанка



Марина Ким - ведущая Первого канала; Филипп Ильин-Адаев - Председатель Совета директоров холдинга Банки.ру; Елена Ищеева - Исполнительный директор холдинга Банки.ру, руководитель проекта Finparty; Александр Борисов - Генеральный директор ММБА, Председатель Комитета Торгово-промышленной палаты России по развитию потребительского рынка



Мария Пласковицкая
Исполнительный директор
«АМФ- международная сеть
доставки цветов»



Алексей Батури
Заместитель генерального
директора по стратегическому
маркетингу и коммуникациям
«АФГ Националь»

Рейтинговый
партнер



Аналитический
партнер



Генеральный
медиа партнер



Генеральный
информационный
партнер



Официальный
печатный
партнер



Официальный
партнер



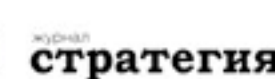
Партнеры



Официальный
кейтеринг партнер



Информационные
партнеры



Реклама

МВД ПОДВЕЛО ИТОГИ 2016 ГОДА

В 2016 году Министерство внутренних дел пресекло деятельность двух преступных групп, осуществлявших хакерские атаки на кредитно-финансовые организации.

«Сотрудниками полиции пресечена деятельность двух организованных преступных сообществ, осуществлявших целевые атаки на учреждения кредитно-финансовой сферы. Возбуждены уголовные дела по признакам состава преступления, предусмотренного статьей 210 УК РФ („Организация преступного сообщества“), — сообщили на пресс-конференции в МВД.

Всего в прошлом году МВД выявило 77 мошенничеств с банковскими картами, 994 случая несанкционированного доступа к компьютерной информации, 751 факт создания, использования и распространения вредоносных программ, а также 4329 мошенничеств в сфере компьютерной информации.

ЗАРАЗИЛИ МИЛЛИОН СМАРТФОНОВ

Российские правоохранители задержали хакерскую группировку Cron, которая занималась хищением средств с банковских счетов граждан при помощи вредоносного ПО для мобильных телефонов. Жертвами стало более миллиона человек, а ущерб превысил 50 млн рублей.

В группировку входили 20 злоумышленников, проживающих в Ивановской, Московской, Ростовской, Челябинской, Ярославской областях и Республике Марий Эл. Организатором оказался 30-летний житель Иваново. Атакам подвергались клиенты Сбербанка, Альфабанка и платежной системы Qiwi.

Хакеры использовали банковский троян Cron. Оказавшись в системе, он мог автоматически переводить деньги с банковского счета жертвы на подконтрольные злоумышленникам счета (для этого было открыто 6 тыс. сче-

тов). Вредонос помещался в автозагрузку устройства и сам мог отправлять SMS-сообщения на указанные хакерами телефонные номера, пересылать текст получаемых жертвой сообщений на удаленные серверы, а также прятать получаемые от банка уведомления.

Заражение осуществлялось либо через SMS-сообщения, содержащие ссылку на вредоносный сайт, либо через поддельные приложения (Navitel, Framaroot, Pornhub, Avito и пр.), замаскированные под настоящие. Ежедневно злоумышленники заражали в среднем 3,5 тыс. устройств.



СПОНСОРЫ



18-19 октября
2017 года
Москва, ЦВК "Экспоцентр"

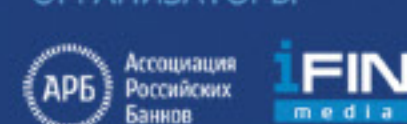


IV МЕЖДУНАРОДНЫЙ ФОРУМ

ВСЯ БАНКОВСКАЯ
АВТОМАТИЗАЦИЯ

2017

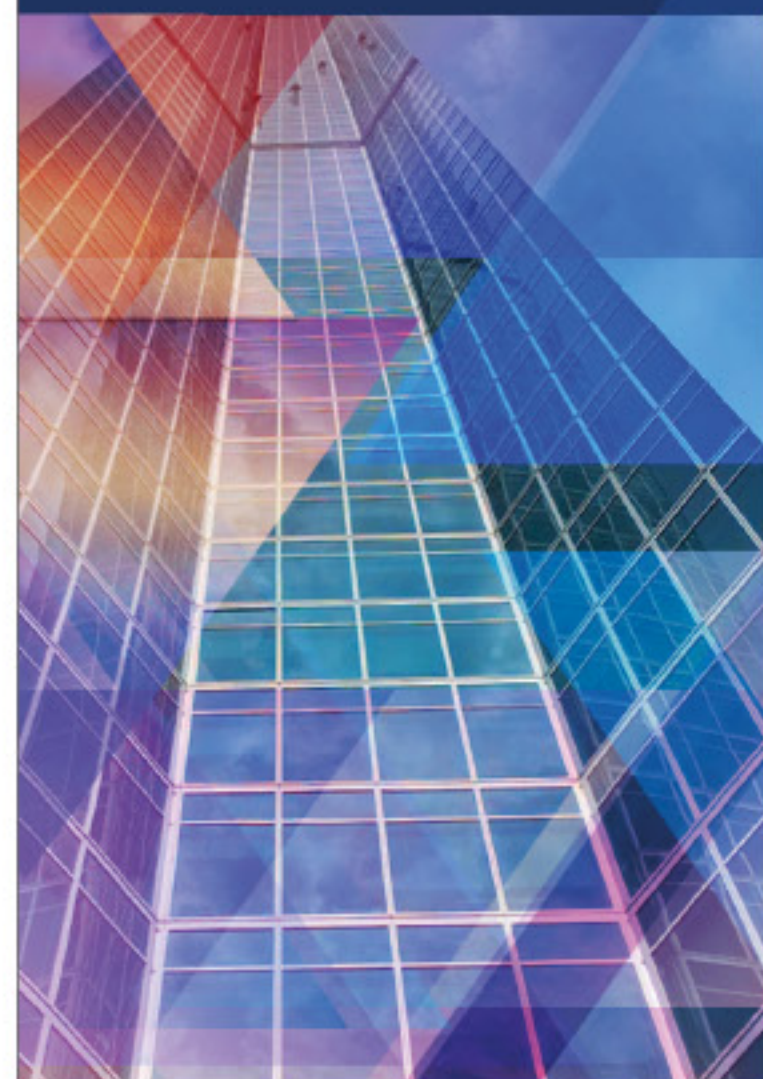
ОРГАНИЗАТОРЫ



18-19 октября 2017 года на Форуме "ВСЯ БАНКОВСКАЯ АВТОМАТИЗАЦИЯ 2017" / ВБА-2017 в Москве (ЦВК "Экспоцентр") будут представлены все сегменты банковской автоматизации:

- Автоматизированные банковские системы (АБС, ИБС, core banking)
- Автоматизация фронт-офиса, филиальной сети, розничного и корпоративного бизнеса
- Электронный и мобильный банкинг, системы ДБО
- Банковские карты, платежные системы, процессинг, бесконтактные платежи, NFC
- Системы самообслуживания, банкоматы, платежные терминалы
- Управление продажами и банковским обслуживанием, CRM-системы, call-центры
- Управление эффективностью и бизнес-аналитика, BPM и BI системы, управление рисками
- Банковская ИТ-инфраструктура, ЦОД, оборудование, сети и телекоммуникации
- Управление ИТ-активами, сервисами, изменениями, ITSM
- ИТ-аутсорсинг и облачные технологии для банков
- Информационная безопасность банков
- Электронный документооборот, ЕСМ-системы, электронные архивы
- ЭДО с государственными органами (ГИС ГМП ФК, ФНС, ФССП, ФМС и др.)
- Управление ресурсами, управление персоналом (HRM-системы), АХД, закупки
- Интеграционные решения для банков

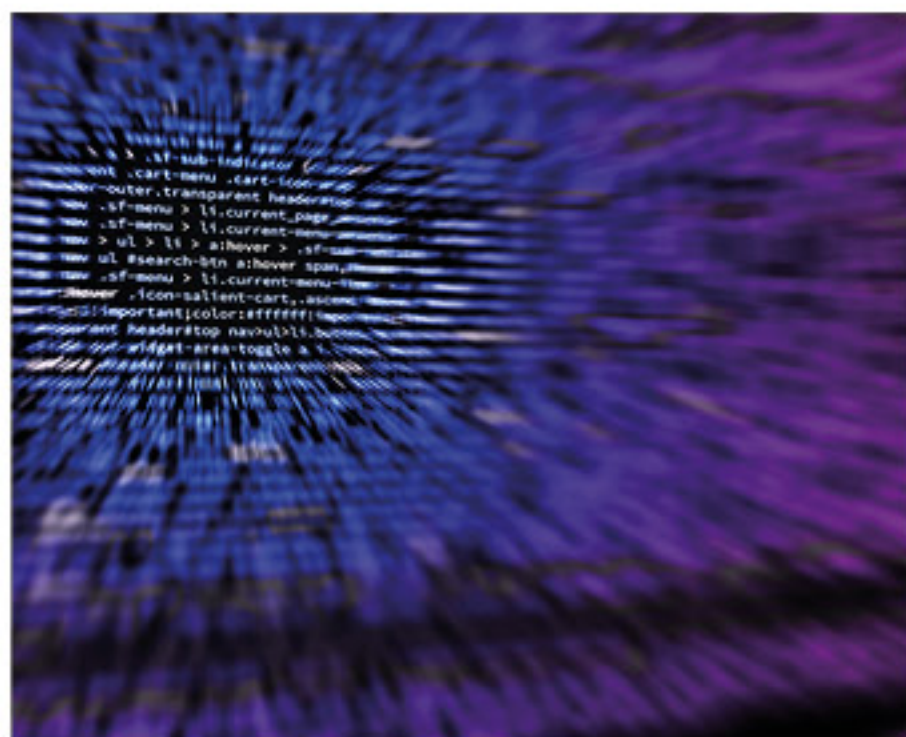
Оргкомитет Форума "ВСЯ БАНКОВСКАЯ АВТОМАТИЗАЦИЯ 2017" / ВБА-2017
Тел.: +7 (495) 229-8502, e-mail: 2017@abaforum.ru, <http://www.abaforum.ru>



ПРОДАЮТСЯ ДАННЫЕ «ЭКСТРЕМИСТОВ»

В интернете на продажу выставлена явно ворованная «база данных экстремистов», в которой содержатся данные на 100 тыс. человек, которые якобы распространяют в Сети экстремистские видеофильмы, запрещенные Роскомнадзором. Купить базу можно за 100 тыс. рублей.

В описании к базе говорится, что в ней содержится информация о пользователях социальной сети «ВКонтакте», распространяющих запрещенный контент. «Среди распространителей экстремистских публикаций (аудио, видео, текстовые записи) депутаты (муниципальные, Госдумы, их помощники), журналисты федеральных СМИ, выпускники вузов, сотрудники спецслужб и силовых ведомств, члены партии «Яблоко» и сотрудники ФБК Навального, Трансперенси и Солидарность, члены ЛГБТ и нацистских группировок, активисты протестных движений, сотрудники компаний Ян-



декс и Майл.ру», — так написали продавцы в описании к товару.

Интересно, что хакеры получили доступ только к информации о запрещенных видеороликах, размещенных на страницах «ВКонтакте». Многие фигуранты базы разместили там только по одному ролику, признанному спустя несколько лет экстремистским.

Базы данных экстремистов есть у всех спецслужб. Судя по всему, хакеры могли похитить данные именно у силовиков с целью заработать.

РЕТУА ДАННЫХ НЕ ВЕРНЕТ. ДАЖЕ ЗА ДЕНЬГИ

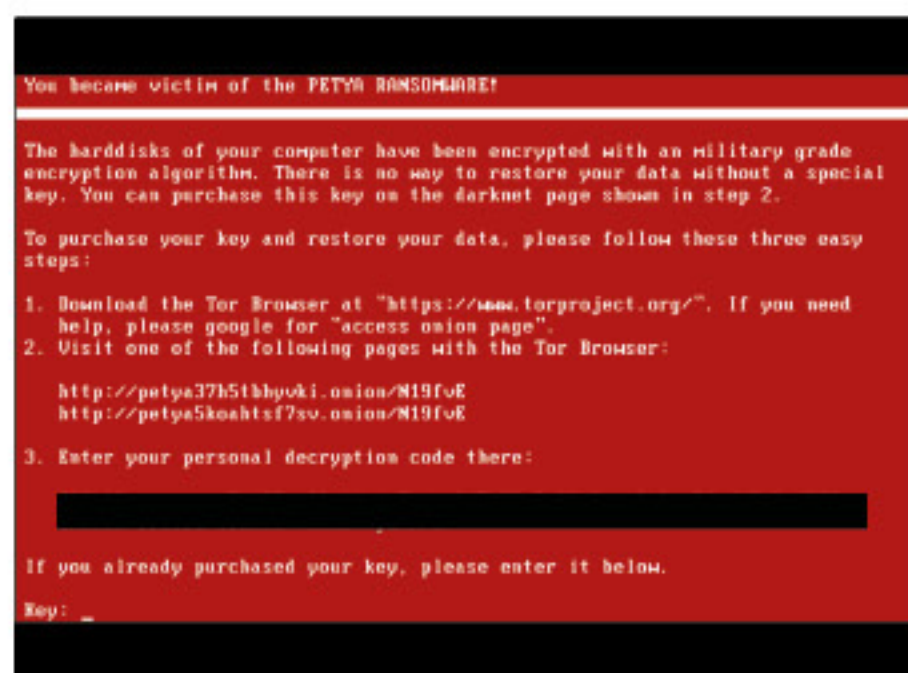
Вопреки мнению общественности, вредоносная программа Retya была создана для атаки на ряд организаций.

Специалисты тщательно изучили природу напавшего вируса-вымогателя Retya и выяснили, что хакерам не удастся расшифровать украденные данные, так как вредоносная программа этого не подразумевает. Изначально вирус Retya был создан

только для уничтожения сведений. Однако в большинстве СМИ сообщалось, что основной целью разработчиков вируса являлось денежное вознаграждение.

Теперь специалисты не сомневаются в том, что программа была создана лицами, заинтересованными в банальном уничтожении данных определенных организаций. В результате массовой атаки пострадало несколько государственных предприятий и кредитных организаций.

Впервые о вирусе Retya стало известно 27 июня, когда программа поразила бухгалтерские системы на украинских серверах. Вирус-вымогатель требовал денежные средства у владельцев компьютеров. Если деньги не перечислялись, программа permanently блокировала работу всей операционной системы.



В КРАСНОЯРСКЕ ОСУДИЛИ БАНКИРА



Красноярский суд приговорил менеджера местного банка и его сообщника к семи и пяти годам тюремного заключения за хищение 26 млн. руб. с клиентских счетов.

Схема была простая. Банковский служащий получал информацию о счетах VIP-клиентов и обеспечивал перевод с них денег на другой счет. Напарник эти деньги обналичивал. После обналичивания преступники деньги поделили и потратили.

В результате действий злоумышленников у трех клиентов банка было похищено 26,5 миллионов рублей. В ходе предварительного следствия обвиняемые свою вину полностью признали. Наказание они будут отбывать в колонии строгого режима.

ЖЕСТКИЕ ХАКЕРЫ ИЗ-ЗА БАЙКАЛА

В Забайкалье задержана преступная группировка, использовавшая вредоносное ПО для Android с целью хищения денежных средств с банковских счетов граждан. По предварительным данным, от действий злоумышленников пострадали более тысячи россиян, а сумма украденного исчисляется десятками миллионов рублей.

В течение полутора лет четверо жителей Читы распространяли вредоносное ПО для Android-смартфонов. Полученная с его помощью информация передавалась на специально созданные сайты, с которых через online-сервисы банков и крались деньги со счетов россиян. Уведомления о списании денег блокировались вредоносной программой. О хищении средств пострадавшие узнавали только через длительное время.

НАУЧИТЬ БЕЗОПАСНОСТИ

ПОВЫШЕНИЕ КУЛЬТУРЫ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ГРАЖДАН – СИСТЕМНАЯ ЗАДАЧА



Людмила БОКОВА

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



Количество электронных сервисов неуклонно растёт, уже сейчас ими пользуется почти каждый россиянин. Вместе с тем интернет-угрозы разрастаются до масштабов, сравнимых с «оружием массового поражения». От киберугроз страдает общество в целом. Чем выше информированность граждан, тем меньше риск оказаться в этой «зоне поражения». Как говорится, информирован — значит, защищён. Именно поэтому в России формируется целостная система, способствующая повышению культуры информационной безопасности граждан.

ЗАЩИТИТЬ САМЫХ УЯЗВИМЫХ

Уязвимым оказывается поколение, которое активную часть жизни провело, ничего не зная об интернете и цифровых технологиях. Это люди, давно перешагнувшие рубеж пенсионного возраста. Но с другой стороны, пожилые пенсионеры у нас пока мало пользуются цифровыми технологиями, не доверяют им. Некоторые до сих пор предпочитают, например, расплачиваться наличными. Поэтому и в сети интернет-мошенников они попадают нечасто.

Если выделять самую незащищённую категорию, то это, конечно, дети школьного возраста. Они практически не расстаются с гаджетами. Растёт новое, «цифровое» поколение. В сети многие школьники проводят по несколько часов в день, многие из них уже сейчас гораздо более уверенные пользователи, чем их родители. Но, к сожалению, пользовательские навыки и умения у них есть, а осознания рисков, которые несёт интернет, пока не появилось. Дети не понимают, что нельзя доверять всему, что они видят в сети, не умеют проверять информацию, не подозревают о том, что нельзя раскрывать персональные данные. Поэтому они в первую очередь становятся жертвами преступников — организаторов деструктивных сообществ.

Распоряжением Правительства России от 2 декабря 2015 года № 2471-р была принята «Концепция детской информационной безопасности». Главным законодательным актом в этой сфере является принятый ранее Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» № 436-ФЗ от 29 декабря 2010 года.

Благодаря поправкам к закону есть возможность во внесудебном порядке блокировать сайты, продвигающие негативный контент, в том числе рекламу наркотиков, пропаган-

**ДЕТИ НЕ ПОНИМАЮТ, ЧТО
НЕЛЬЗЯ ДОВЕРЯТЬ ВСЕМУ,
ЧТО ОНИ ВИДЯТ В СЕТИ,
НЕ УМЕЮТ ПРОВЕРЯТЬ
ИНФОРМАЦИЮ, НЕ
ПОДОЗРЕВАЮТ О ТОМ,
ЧТО НЕЛЬЗЯ РАСКРЫВАТЬ
ПЕРСОНАЛЬНЫЕ ДАННЫЕ**

ду суицида, детскую порнографию, азартные игры. Десятки тысяч таких сайтов уже заблокированы. Совсем недавно в Уголовный кодекс РФ внесены изменения, предусматривающие введение уголовной ответственности для лиц, побуждающих детей к суицидальному поведению.

Существующая законодательная база дает правоохранительным органам необходимые инструменты для противодействия киберпреступникам. Но, как мы все понимаем, невозможно отследить все действия в сети, в том числе действия самого ребенка. Поэтому лучшим средством защиты остается обучение детей безопасному и ответственному поведению в сети. И, конечно, необходим повышенный родительский контроль.

ГРАМОТНОСТЬ РАСТЕТ

Помимо создания государственной и корпоративных систем противодействия киберугрозам, большое значение имеет грамотность граждан в вопросах информационной безопасности. Согласно результатам прошлогоднего исследования Регионального общественного центра интернет-технологий (РОЦИТ), индекс цифровой грамотности населения России в 2016 году составил 5,42 пункта из десяти возможных. Еще в 2015 году этот показатель составлял 4,79 пункта. То есть положительная динамика налицо. Причем быстрее всего растут не пользовательские знания, а именно уровень информационной безопасности. Этот индекс за год увеличился с 4,86 до 5,57 пункта. Я считаю, это очень хорошая новость.

Если сравнивать эти цифры с результатами подобных исследований в мире, то мы, конечно, отстаем от лидеров, среди которых Дания, Южная Корея, Швеция, Великобритания и другие страны с высоким уровнем использования информационно-коммуникационных технологий. Но, повторюсь, динамика есть, и довольно высокая.

Для повышения уровня информационной безопасности граждан России готовятся новые законодательные акты. Советом Федерации поддержан законопроект о повышении степени защиты информации, обрабатываемой в государственных системах. ФСТЭК России (Федеральная служба по техническому и экспертному контролю) провела мероприятия по оценке состояния технической защиты информации ограниченного доступа в федеральных и региональных органах исполнительной власти.

Было выявлено, что значительное количество сведений о гражданах и деятельности государства, подлежащих защите, обрабатываются организациями, которые используют негосударственные информационные системы без соответствующей защиты. Соответственно предлагается обязать операторов указанных информационных систем устанавливать специальные средства защиты.

Кроме того, Совет Федерации одобрил концепцию законопроекта по введению нового состава преступления за неправомерное воздействие на критическую инфраструктуру, неправомерный доступ к охраняемой информации, содержащейся в критической инфраструктуре, а также за нарушение правил эксплуатации средств хранения, обработки и передачи данных, относящихся к такой информации.

ОБУЧАЮЩИЕ ПРОЕКТЫ

Осуществляются государственные и другие программы, нацеленные на повышение грамотности граждан в вопросах информационной безопасности. Единый урок безопасности в сети интернет — пожалуй, самая масштабная кампания по кибербезопасности и повышению общего уровня цифровой грамотности. Впервые он был проведен в 2014 году по инициативе Председателя Совета Федерации Валентины Матвиенко. В минувшем году нам удалось охватить мероприятиями Единого урока около 13 млн школьников из России и стран ближнего зарубежья. Урок проходит в разных форматах — это конкурсы, викторины, лекции, сетевые игры.

Важно, что к этому проекту привлечены не только школьники, но и их родители. В прошлом году мы обратились в крупные компании (ПАО «Газпром», ОАО «Российские железные дороги», ПАО «Транснефть», ГК «Ростех» и другие), а также в российские министерства с тем, чтобы сотрудники этих организаций вместе с детьми приняли участие в мероприятиях Единого урока. Этот опыт оказался успешным. Методические разработки организаторов Единого урока легли в основу школьного межпредметного курса «Основы кибербезопасности». Уже в этом учебном году начнем внедрять его в пилотных школах.

Число участников международного интернет-квеста «Сетевичок» из России и еще 11 республик постсоветского пространства к настоящему времени составляет около 260 000 человек. Об уровне этого проекта говорит тот факт, что школьники-победители «Сетевичка» стали экспертами Временной комиссии по развитию информационного общества и приняли участие в парламентских слушаниях «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», прошедших в апреле.

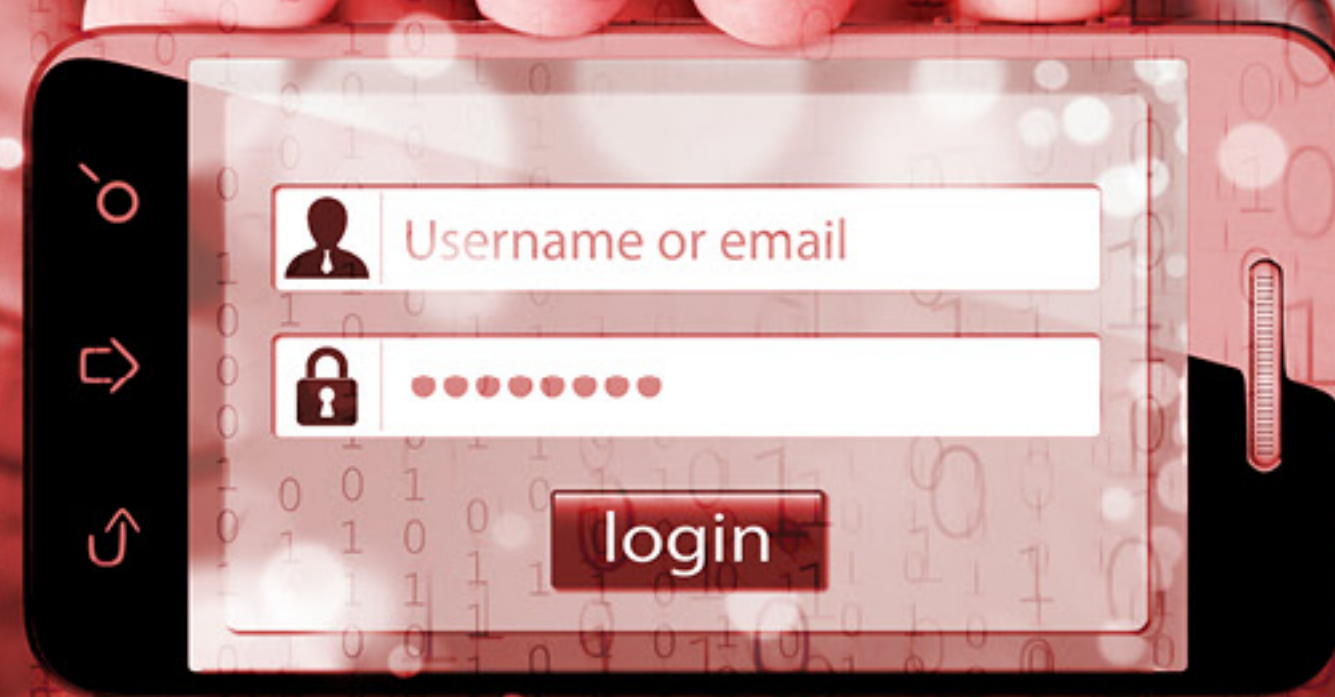
Итогами слушаний стали рекомендации мер правового регулирования жизнедеятельности детей в информационном пространстве и региональная модульная программа информационной безопасности. Комплекс мероприятий каждый регион может регулировать с учетом своих особенностей и возможностей. На основе подготовленных нами материалов план мероприятий на 2017–2020 годы в рамках реализации «Концепции информационной безопасности детей» разрабатывает Министерство связи и массовых коммуникаций России.

* * *

Постепенно формируется целостная обучающая система, способствующая повышению культуры информационной безопасности граждан России. В декабре 2016 года Указом Президента России утверждена новая «Доктрина информационной безопасности Российской Федерации». В ней перечислены основные информационные угрозы и состояние информационной безопасности в различных сферах, а также стратегические цели и основные направления обеспечения информационной безопасности и ее организационные основы. Так что процесс создания этой системы уже идет, и мы все являемся его участниками.



Максим ГРИГОРЬЕВ
начальник Центра
финансовых технологий
Банка России



УЗНАТЬ ИЗДАЛЕКА

В УСЛОВИЯХ ЦИФРОВЫХ СЕРВИСОВ
В ФИНАНСОВОМ СЕКТОРЕ ПОВЫШАЕТСЯ
ЗАПРОС НА СОВЕРШЕНСТВОВАНИЕ УДАЛЕННОЙ
ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ КЛИЕНТОВ

Взаимодействуя с участниками финансового рынка, мы не видим перспектив для его развития без внедрения соответствующих информационных технологий, без перехода в мобильные и другие каналы дистанционного обслуживания. И тут на первый план выходит тема идентификации. Идентификации надежной, которая позволит минимизировать риски и в то же время откроет перспективы для развития новых, удобных для клиента качественных сервисов.

Общаясь с участниками финансового рынка, мы задаем вопросы: что для вас сегодня особенно важно? На что нужно обратить внимание в первую очередь? С чем вы хотите поэкспериментировать? Ответы, конечно, разные, но среди них доминирует кейс, связанный с идентификацией.

ЧТО ИМЕЕМ?

Сегодня требования к идентификации определяются в первую очередь положениями Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации

(отмыванию) доходов, полученных преступным путем, и финансированию терроризма». ФЗ-115 позволяет использовать упрощенную идентификацию, предполагающую дистанционный доступ. Однако она имеет существенные ограничения на сумму и сервисы, которые могут быть предоставлены клиенту после проведения упрощенной идентификации.

Полноценной идентификацией сегодня считается та, что происходит в присутствии гражданина в момент его личной явки в финансовую организацию. Соответственно, должна быть проведена стандартная процедура: проверка подлинности документов, сопоставление информации из разных источников. И только после этого финансовая организация может оказывать клиенту полноценные услуги.

Если этот же клиент хочет обратиться в другую финансовую организацию, он снова обязан пройти идентификацию в личном присутствии. Такой подход заметно сдерживает развитие дистанционных услуг, препятствует полноценной финансовой доступности. Особенно в удаленных регионах,

ЦЕЛИ И ЗАДАЧИ

Какие цели и задачи мы видели перед собой, когда стали искать подходы к решению проблемы развития удаленной идентификации?

Цели:

- ♦ Повышение качества финансовых услуг за счет усиления конкуренции на финансовом рынке;
- ♦ Повышение доступности финансовых услуг для потребителей в труднодоступных регионах;
- ♦ Увеличение скорости предоставления услуг за счет перехода на полное электронное взаимодействие.

Задачи:

- ♦ Создание единого пространства доверия идентификации и аутентификации;
- ♦ Интероперабельность информационных систем участников взаимодействия;
- ♦ Безопасность и надежность механизма удаленной идентификации;
- ♦ Актуальность и достоверность идентификационной информации;
- ♦ Гибкость и своевременность реализации необходимых изменений.

где нет возможности лично прийти в финансовую организацию. Соответственно, конкуренция на рынке страдает, банки, имеющие привлекательные сервисы, но не имеющие возможности проидентифицировать клиента, не могут оказывать свои самые современные услуги.

КОНЦЕПЦИЯ

В прошлом году Банк России совместно с Минкомсвязью и Росфинмониторингом разработали и согласовали концепцию удаленной идентификации клиентов финансовых организаций. Сейчас в рамках этой концепции разрабатывается механизм удаленной идентификации и соответствующие правовые основания.

Мы пришли к выводу, что местом — базой данных, где будет храниться идентификационная информация, должна стать государственная система, имеющая соответствующую инфраструктуру, к которой подключено большое число участников финансового рынка. Такой системой была определена ЕСИА — Единая Система Идентификации и Аутентификации.

Там действует несколько типов учетных записей, в том числе подтвержденная учетная запись. Кстати, простая запись в ЕСИА уже сейчас может использоваться для проведения упрощенной идентификации.

ПЕРВИЧНАЯ ИДЕНТИФИКАЦИЯ

Наш подход заключается в следующем. Полноценная идентификация при личном присутствии клиента проводится однократно. Человек приходит в банк (перечень организаций, проводящих первичную идентификацию, на начальном этапе будет ограничен, чтобы обезопасить фазу тестирования), приносит необходимые документы, сообщает личные данные. Банк проверяет подлинность документов и снимает биометрическую информацию.

Биометрическая информация на начальном этапе — это фотография и голос, детали еще предстоит уточнить. В дальнейшем требования к биометрии будут меняться, возможно, усложняться. Сейчас в этой области много инноваций, она стремительно развивается. Окончательные требова-

ния к биометрии в настоящий момент прорабатываются, но очень важно, чтобы она была доступной, не требовала использования дорогих инструментов, устройств, механизмов, специально оборудованных помещений.

Проведя первичную идентификацию, банк берет у клиента согласие на передачу информации в ЕСИА и ее использование в дальнейшем другими финансовыми организациями. Также клиент дает банку согласие на право подписывать простой электронной подписью его документы (рис. 1).

Все эти сведения направляются в ЕСИА, где проводится их кросс-проверка по базам данных МВД, ФНС, Пенсионного фонда, а также проверка подлинности предоставленного номера телефона и т.д.

В итоге создается подтвержденная учетная запись. По сути, учетная запись нового типа. Клиент получает логин и пароль, которыми в дальнейшем будет пользоваться, чтобы аутентифицироваться в других финансовых организациях.

УДАЛЕННАЯ ИДЕНТИФИКАЦИЯ

В дальнейшем удаленная аутентификация может проводиться в любой финансовой организации, где пользователь хочет получить удаленные услуги. На начальном этапе в эту систему будут входить только кредитные организации, но постепенно система станет расширяться, вовлекая все новые типы организаций.

Каков порядок действий удаленной идентификации? Для дистанционного получения услуги пользователь заходит на сайт любого банка, авторизуется через ЕСИА, направляет биометрические персональные данные для сверки со следами, хранящимися в биометрической базе данных. После аутентификации в ЕСИА и подтверждения совпадения биометрических слепков банк получает из ЕСИА персональные данные физического лица, необходимые для идентификации по требованиям законодательства. В идеале набор этих операций должен занимать у клиента не больше нескольких минут. Более подробно порядок действий будет определяться рекомендациями Банка России, Минкомсвязи и Росфинмониторинга (рис. 2).

После того, как подтвердились все атрибуты клиента, и идентификация пройдена, клиент может получить требуемую услугу.

ОБНОВЛЕНИЕ ИНФОРМАЦИИ

Наша концепция подразумевает и предусматривает обновление информации. Сейчас прорабатывается вопрос синхронизации информации с базами данных МВД, ФНС, Пенсионного фонда и других организаций. Как только в одной из них информация изменяется, она тут же должна обновиться и в ЕСИА (рис. 3).

Кроме того, банки сами будут актуализировать информацию. Процедура еще будет определена и отработана, но логика простая: примерно один раз в год банк, который провел первичную идентификацию клиента, или его постоянный банк будет делать запрос на актуализацию информации.

РЕАЛИЗАЦИЯ ПРОЕКТА

Депутатом Государственной Думы А.Г. Аксаковым и членом Совета Федерации Н.А. Журавлевым был внесен 24.04.2016 в Государственную Думу законопроект № 157752-7 «О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», направленный на совершенствование механизмов предоставления банковских услуг без личного присутствия клиента с использованием государственных информационных ресурсов. Данный законопроект был разработан при участии Банка России, Минкомсвязи России и Росфинмониторинга в целях развития финансового рынка, обеспечения доступности финансовых услуг для граждан, в том числе в удаленных регионах и для людей с ограниченными возможностями, а также для снижения стоимости их предоставления.

По итогам реализации механизма удаленной идентификации для дистанционного предоставления банковских услуг будет рассмотрен вопрос возможности масштабирования механизма на другие финансовые услуги и иные сектора экономики.

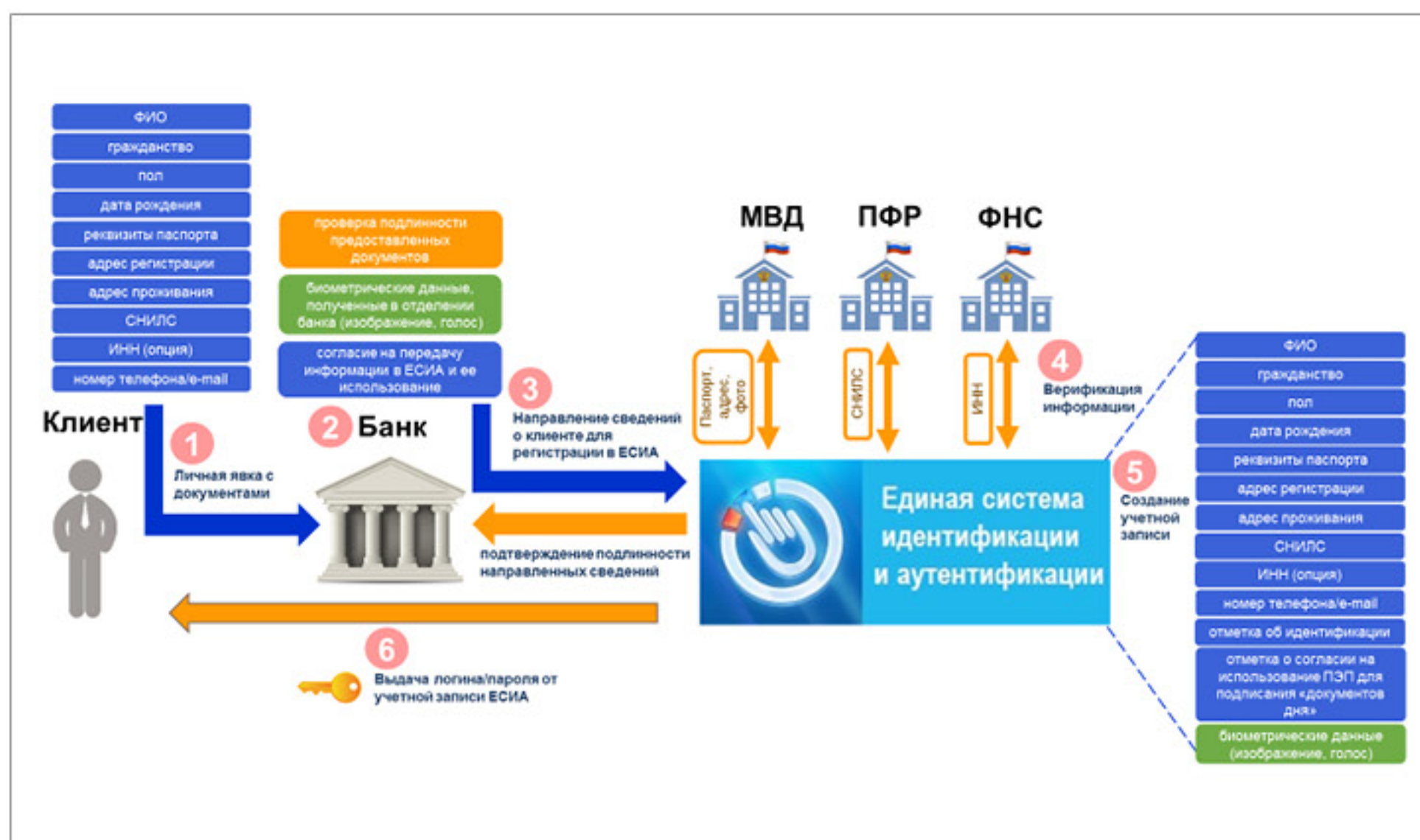


Рисунок 1. Первичная идентификация

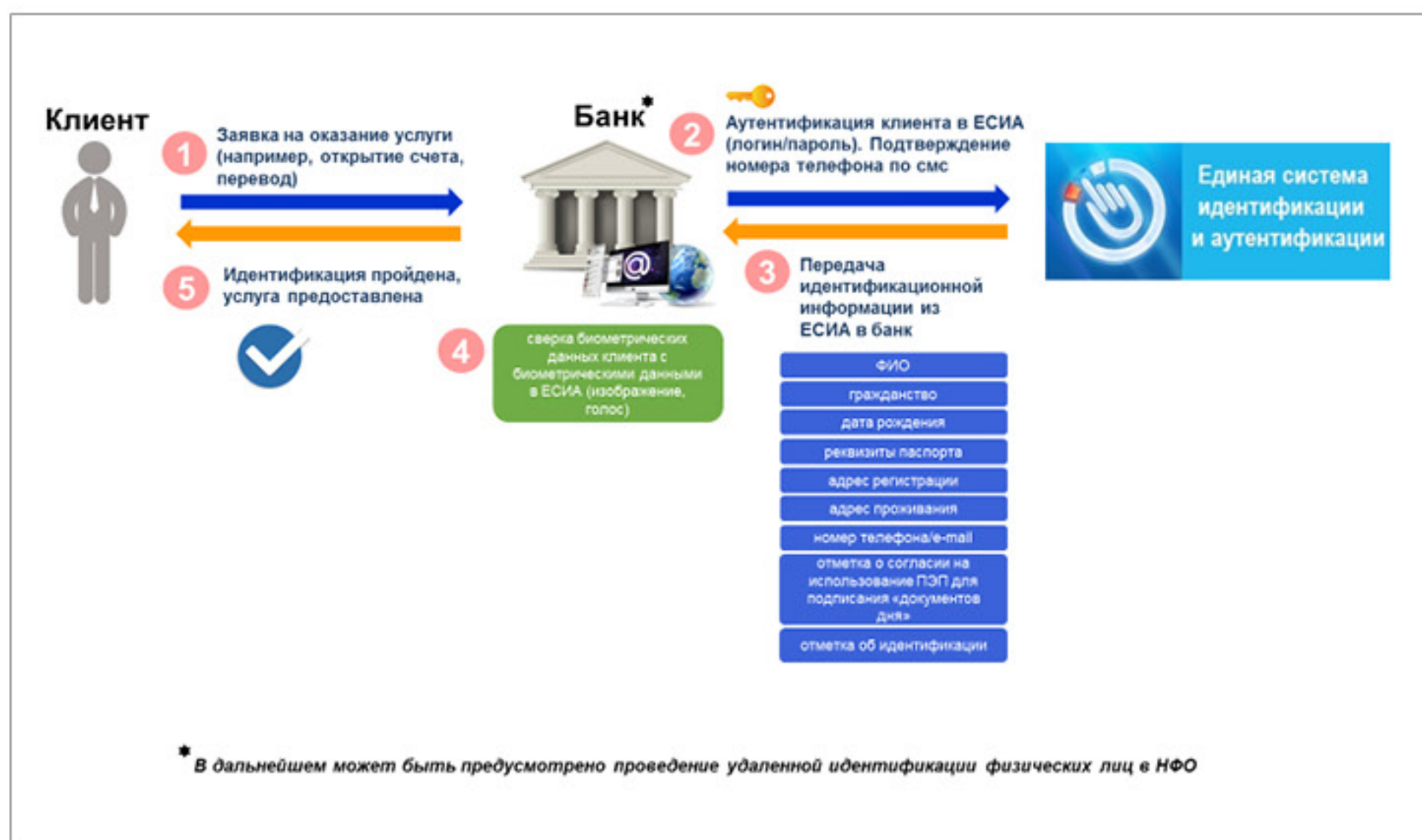


Рисунок 2. Удаленная идентификация

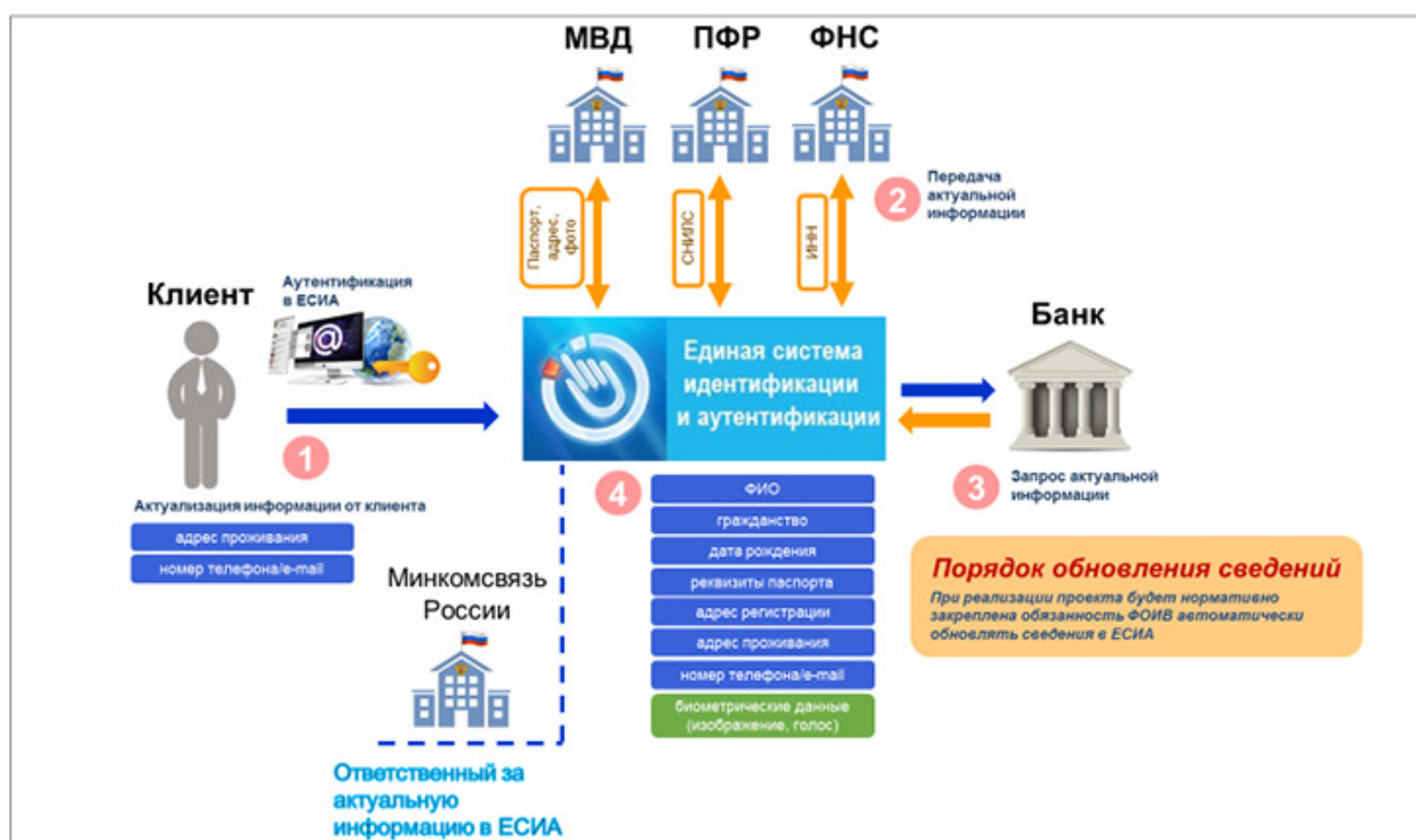


Рисунок 3. Обновление идентификационной информации



Роман ШЕРЕДИН
заместитель руководителя
Федерального агентства
связи (Россвязь)

КТО ЧИСТИТ ТРАФИК?

УСТОЙЧИВОЕ ФУНКЦИОНИРОВАНИЕ
ЕДИНОЙ СЕТИ ЭЛЕКТРОСВЯЗИ
РОССИЙСКОЙ ФЕДЕРАЦИИ – ЗАЛОГ
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
ФИНАНСОВОГО РЫНКА

Всего за несколько столетий технологии связи прошли свой эволюционный путь от сторожевых постов и башен, оптического семафорного телеграфа до сетей электросвязи, ставших основой современного информационного общества. Электронный формат взаимодействия граждан с государством, бизнесом, между собой — это наша сегодняшняя реальность, которая продолжает нас удивлять и стремительно развиваться.

Кроме своей светлой, созидательной стороны информационные технологии имеют и обратную сторону. Как сказано в Доктрине информационной безопасности Российской Федерации: «Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы».

Соответственно, в числе национальных интересов в информационной сфере в доктрине указано «обеспечение устойчивого и безопасного функционирования информационной инфраструктуры, в первую очередь критической, и единой сети электросвязи Российской Федерации». Чем, собственно, наше Федеральное агентство связи, опираясь на свои немалые полномочия и ресурсы, и занимается в ежедневном режиме.

СПЕЦИФИКА ФИНАНСОВОГО СЕКТОРА

Занимаясь обеспечением функционирования и безопасности единой сети электросвязи в целом, мы не можем не учитывать ее сегментированности, то есть отраслевой аспект. В частности, информационная инфраструктура финансового сектора имеет свою довольно выраженную специфику. По сравнению с другими секторами она находится под постоян-

ным прессингом — выдерживает непрекращающееся, стабильно усиливающееся давление со стороны злоумышленников. И безусловно, последствия от этих злонамеренных и вредоносных действий несут в себе как большой материальный ущерб, так и значительные репутационные риски.

ЦНИИС ПРЕДЛАГАЕТ РЕШЕНИЕ

Любая проблема имеет свое решение. В данном случае по заданию Россвязи такое решение подготовил наш подведомственный Центральный научно-исследовательский институт связи (рис. 1). Если коротко, ФГУП ЦНИИС — научная организация первой категории со столетней историей, которая в то же время является стратегическим предприятием оборонно-промышленного комплекса.

Чтобы понять масштаб деятельности ЦНИИСа, достаточно сказать, что именно на его базе действует Центр внедрения СОПМ на сети связи общего пользования. В контексте же решения вопросов информационной безопасности финансовой сферы важно то, что ЦНИИС является базой данных перенесенных номеров мобильных операторов.

После отмены «мобильного рабства» в 2013 году все без исключения мобильные операторы, в том числе и более 150 банков, имеющих такие функции, подключены к базе данных перенесённых номеров, к ЦНИИСу. Такой потенциал позволил институту сформулировать ряд предложений в сфере информационной безопасности банков, которые сейчас активно обсуждаются с руководством ГУБиЗИ Банка России.

А И Б СИДЕЛИ НА ТРУБЕ

На рис. 2 представлено наше видение информационной инфраструктуры финансовой сферы. Также мы выделили две группы угроз по объектам воздействия.



В Федеральном агентстве связи состоялось очередное заседание Президиума НТС, на котором было принято решение о поддержке инициативы ОГО «АДЭ» по созданию под эгидой Россвязи межвузовского учебно-исследовательского центра мониторинга, анализа и расследования инцидентов информационной безопасности с использованием отечественных технических средств.

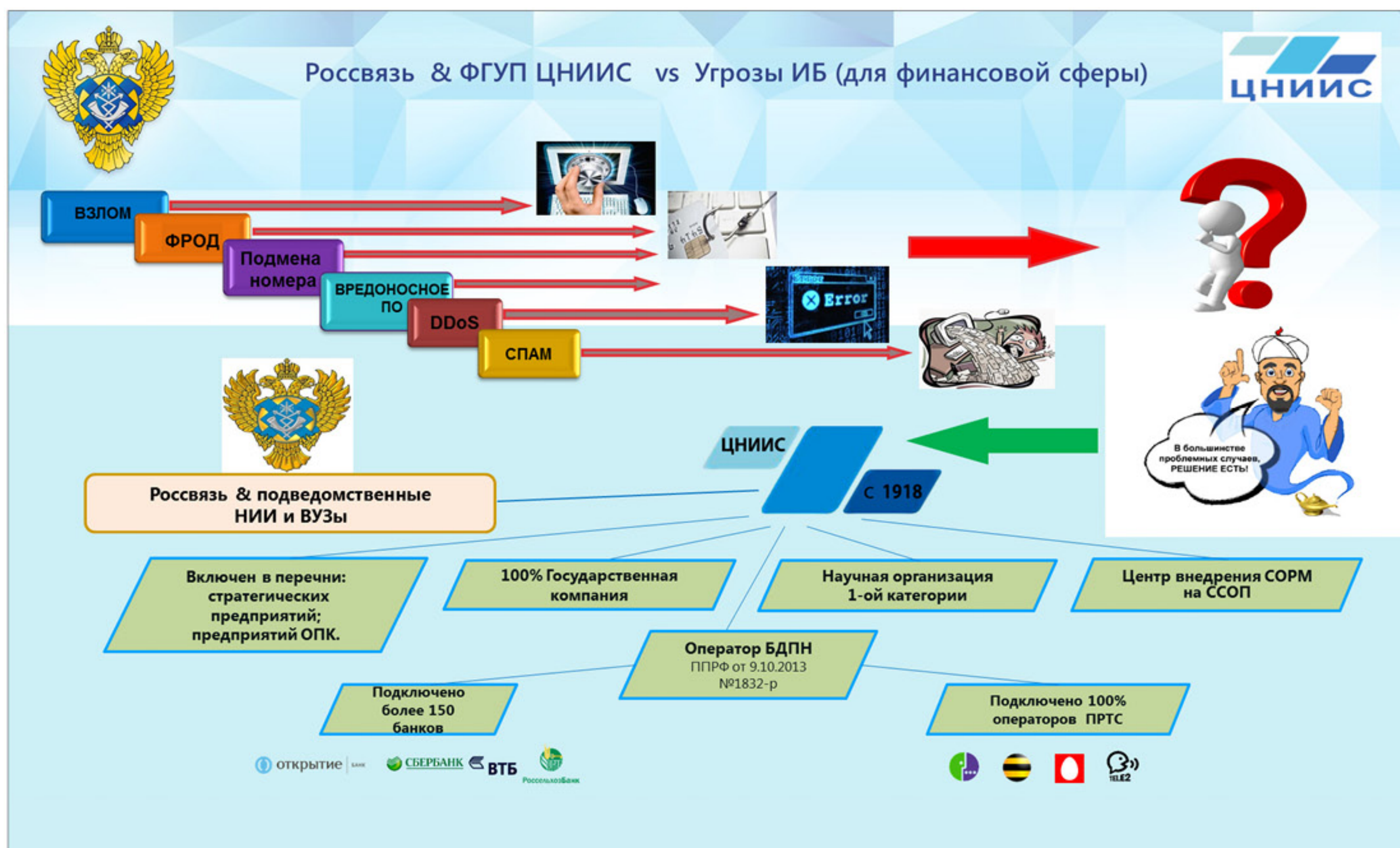


Рисунок 1. Россвязь и ФГУП ЦНИИС



Рисунок 2. Предложения ФГУП ЦНИИС для финансовой сферы



Рисунок 3. Предложения по противодействию угрозам типа «А»



Рисунок 4. Предложения по противодействию угрозам типа «В»



Рисунок 5. Предложения по противодействию угрозам типа «В». Вариант №2 — фильтрация паразитного трафика по запросам

На рис. 3 — предложение по противодействию угрозам типа «А». Соответственно, мы предлагаем создать единую информационную систему. На этом же рисунке показаны роль и место в ней операторов связи ЦНИИС, финансово-кредитных организаций и их пользователей.

Единая информационная система (ЕИС), на наш взгляд, позволит ее участникам запрашивать и получать в режиме реального времени данные о корректной связке международных идентификаторов мобильного абонента и мобильного устройства, получать доступ к архивным данным, данные об операционных системах, используемых пользователями различных удаленных банковских услуг и многое другое. Также ЕИС позволит всем кредитно-финансовым организациям надлежащим образом выполнять требования действующих нормативно правовых актов, как со стороны безопасности транзакций с использованием мобильных устройств, так и со стороны повышения защищенности потребителя услуг и соблюдения требований в области противодействия отмыванию доходов и финансированию терроризма.

Предложение на рис. 4 предполагает создание Межоператорского центра анализа трафика (МЦА). Мы понимаем, что есть и прекрасно работает ФинЦЕРТ — центр мониторинга как подразделение Банка России, но мы также понимаем, что все банки работают между собой и со своими клиентами, используя фактически все связи общего пользования, включая тех или иных операторов связи.

Поэтому работу МЦА мы прорабатываем в двух возможных вариантах.

Первый вариант предусматривает постоянное взаимодействие инфраструктуры кредитно-финансовых организаций с сетью связи общего пользования через МЦА. При такой схеме весь входящий трафик, идущий на инфраструктуру кредитно-финансовых организаций, мониторится, анализируется... Такой подход позволяет решать точечные задачи по ограничению доступа к тем или иным ресурсам, которые являются источником злонамеренных воздействий на отдельных пользователей или инфраструктуру в целом. Соответственно, на выходе в банк поступает уже очищенный полезный трафик. Преимущество такого подхода — практически постоянная защита от DDoS-атак в режиме реального времени.

Второй вариант (рис. 5) можно назвать «вариантом по запросу». В этом случае трафик сети связи общего пользования поступает в банк в штатном режиме. В случае обнаружения сенсорами атак трафик переключается на МЦА и там происходит его фильтрация и очистка.

Оба варианта обеспечивают необходимый информационный обмен между МЦА Россвязи и ФинЦЕРТом Банка России.

ФУНКЦИОНАЛЬНОСТЬ = БЕЗОПАСНОСТЬ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НСПК



**Василий
ОКУЛЕССКИЙ**
начальник Управления
безопасности
АО «НСПК»

Летом 2014 года в ответ на санкции была создана Национальная система платежных карт (НСПК). Целью создания НСПК является обеспечение национальной безопасности России в области операций по банковским картам. Ее создание и развитие — ключевой фактор обеспечения суверенитета национального платежного пространства, который гарантирует безопасность и бесперебойность проведения внутрироссийских транзакций по всем банковским картам всех платежных систем и полную независимость функционирования национального платежного пространства от внешних факторов, в частности, и в условиях действующих санкций.

Уже с 1 апреля 2015 года платежный клиринговый и операционный центр НСПК начал обрабатывать операции по картам крупнейших международных платежных систем, а с 15 декабря 2015 года создал все условия для выпуска банками карт ПС «МИР», к маю 2017 года выпущено более 5 млн карт.

С ПЕРВОГО ДНЯ

С первого дня образования НСПК вопросы обеспечения информационной безопасности решались вместе с задачами построения инфраструктуры компании, формирования ее бизнес-процессов, проектирования и реализации всего спектра услуг.

Это — безопасность каналов связи с участниками, создание системы Удостоверяющего центра (Certificate Authority) для всех банков, безопасность обмена файловыми данными через систему электронного документооборота (СЭДО), это и безопасность данных карты и операций по ней, и безопасность операций электронной коммерции, это и управление расчетными рисками, арбитраж операций, взаимная аутентификация карты и эмитента, безопасность совершения off-line операций, безопасность ПИН, безопасность мобильной коммерции, мониторинг подозрительных операций, система взаимного информирования о подозрительных операциях и еще многое-многое другое.

ТРИ НАПРАВЛЕНИЯ

Очень условно деятельность в сфере безопасности можно разделить на 3 главных направления:

1. Обеспечение катастрофоустойчивости инфраструктуры НСПК.
2. Формирование и контроль выполнения требований по ИБ для участников ПС «МИР».
3. Обеспечение безопасности технологий платежных операций ПС «МИР».

В свою очередь разнообразие уже существующих и разрабатываемых технологий требует развития специализации по направлениям: защита чувствительных данных, развитие контактных и бесконтактных технологий, мобильных и интернет платежей (рис. 1).

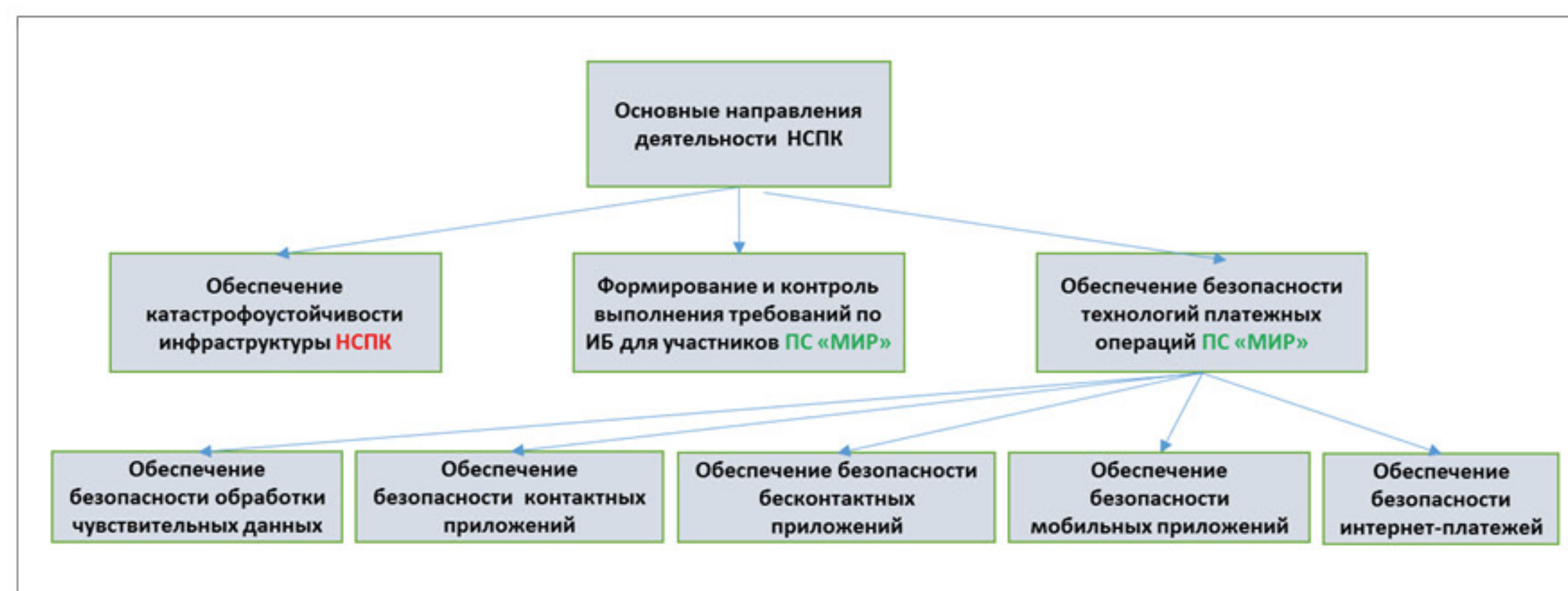


Рисунок 1. Основные направления деятельности НСПК

НАДЕЖНЫЙ ПОДХОД

Катастрофоустойчивость — сравнительно новый термин, который вошел в нашу жизнь и стал весьма актуален в последние годы.

По сути, это хорошо известный всем специалистам комплексный подход к построению инфраструктуры системы, включающий кластеризацию ЦОДов, географическое разнесение их, создание основных и резервных точек доступа, резервирование каналов связи между участниками, канальное шифрование и максимальное использование выделенных каналов, минимальное использование ресурсов публичных сетей, использование программных и технических средств, прошедших процедуру аттестации, использование стандартных архитектурных решений на базе платформы x86.

Реализация этого подхода в 2016 году обеспечила коэффициент готовности НСПК 99,999. Кто знает, тот оценит.

О ФУНДАМЕНТЕ

Как хорошо известно, слабость любой защиты определяется самым слабым звеном. Эта «свежая» идея требует набора базовых «правил игры» в информационную безопасность для всех участников платежной системы. Поскольку все правила нужны здесь и сейчас, то в НСПК пришли к выводу о необходимости ис-

пользования существующего мирового опыта в решении непростой задачи — и присоединились к PCI DSS.

Сразу оговорюсь, PCI DSS — это не «буржуйские» стандарты, а сконцентрированный опыт 30-летнего развития ведущих мировых платежных систем и он не зависит от национальной или государственной принадлежности ПС, это фундаментальные технические и операционные требования, которые разработаны для защиты данных держателей карт, которые были разработаны в целях повышения уровня безопасности данных владельцев платежных карт и содействия процессу повсеместного внедрения единообразных мер по защите данных держателей карт. Кроме того, PCI DSS имеет уже развитую и хорошо организованную систему подготовки профессиональных аудиторов и систему проверки выдвинутых требований. Разработка собственного «параллельного аналога» привело бы к неоправданным затратам на создание такой системы и удвоению затрат банков на проведение сертификации.

Основная задача НСПК в этом направлении обеспечения информационной безопасности — максимально облегчить банкам затраты на совместный аудит соответствия требованиям для ПС «Мир», МПС и 382-П. Задача, прямо сказать, нетривиальная, но тем интереснее ее решать.



> 5 млн

карт ПС «МИР»
выпущено к маю
2017 года

ГРУППЫ ТРЕБОВАНИЙ

Только для того, чтобы напомнить, что это за требования, приведу группы этих требований:

◆ Построение и обслуживание защищенной сети и систем

1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт.
2. Не использовать пароли и другие системные параметры, заданные производителем по умолчанию.

◆ Защита данных держателей карт

3. Обеспечить безопасное хранение данных держателей карт.
4. Обеспечить шифрование данных держателей карт при их передаче через сети общего пользования.

◆ Программа управления уязвимостями

5. Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО.
6. Разрабатывать и поддерживать безопасные системы и приложения.

◆ Внедрение строгих мер контроля доступа

7. Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью.
8. Определять и подтверждать доступ к системным компонентам.
9. Ограничить физический доступ к данным держателей карт.

◆ Регулярный мониторинг и тестирование сети

10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт.
11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности.

◆ Поддержание политики информационной безопасности

12. Разработать и поддерживать политику информационной безопасности для всего персонала организации.

Любому профессионалу от ИБ все эти требования знакомы не только в контексте PCI DSS, но и в повседневной жизни, это наша работа. Если в рамках здравого смысла их выполнять (заменить слова «данные держателя карты» на «платежные» или «персональные» данные) — любые аудиты станут подтверждением вашего профессионализма!

НЕ ПО УЧЕБНИКУ

До сих пор все было, как по учебнику. Классика жанра. Сейчас тоже почти по учебнику, но не всегда ИБ добирается в эти дебри технологий. Известно, что безопасность-«нашлепка», как бы хороша ни была, тормозит бизнес. Безопасность как составная часть бизнеса делает его только привлекательнее. Это становится возможным, когда сами бизнес-технологии одновременно являются технологиями безопасности. Это напрямую относится к «карточным» технологиям.

Привычная платежная карта начинает приобретать бесконтактные свойства, а вместе с ними и новые форм-факторы — в недрах телефонной СИМ-карты, в чипе самого смартфона, в сменной SD-карте, и это все равно остается платежная карта. А значит, ее надо защищать совершенно иными способами, которые реализуются от момента зарождения идеи о новой функциональности.

Основные характеристики контактного приложения «Мир»:

- ◆ полностью соответствует стандарту EMV 4.3;
- ◆ CCD-совместимо и, как следствие, принимается в любом действующем терминале EMV L2;
- ◆ поддерживает базовые функции EMV-приложения, включая ODA, онлайн-взаимную аутентификацию приложения карты и эмитента, скрипт-процессинг, проверку PIN Offline;
- ◆ поддерживает Global PIN;
- ◆ персонализация приложения не зависит от модели микроконтроллера карты (в рамках приложения поддерживается механизм CPS 1.1).

Реализация основных характеристик порождает свои преимущества:

- ◆ выбор профиля обработки транзакции в зависимости от параметров терминала/магазина (terminal type, additional terminal capabilities и т.п.) и карты (бесконтактный/контактный интерфейс);
- ◆ расширенные процедуры управления рисками (таблицы проверки, большое количество кумулятивных счетчиков операций и способов их управления в зависимости от выбранного профиля обработки транзакции, циклические счетчики, MTA, Max offline Days);
- ◆ Non-EMV-функциональность.

ФУНКЦИОНАЛЬНОСТЬ = БЕЗОПАСНОСТЬ

Для тех, кто не понял, зачем нужны предыдущие два абзаца, задам задачку — разделите дефисы на функциональность/безопасность. Даже после первой попытки понятно, что в таких тех-

нологиях функциональность = безопасность. Все это относится и к бесконтактным приложениям «Мир», которые реализуются в рамках версии 1.1 апплета ПП «Мир». Они наследуют все основные свойства контактного приложения, включая выбор профиля обработки транзакции, при этом суммарное время обработки операции на терминале и карте — менее 400 мс. Приложения могут использоваться для оплаты проезда на транспорте в форме как стандартного платежного приложения на карте «Мир» с выбором профиля по типу терминала (например, чтобы всегда отклонять транзакцию в случае провала ODA), так и отдельного пополняемого кошелька, может реализовываться в различных форм-факторах.

ПРО МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

Отдельный разговор про мобильное приложение. Его удобство уже могли оценить многие, карта-телефон всегда под рукой, а технологии взаимной аутентификации участников платежного взаимодействия — еще один пример неразрывного симбиоза безопасность-функциональность-технология. Уже сейчас мобильный сервис реализуется в облачном элементе безопасности (пока для Android 4.4), может использоваться как для бесконтактных, так и удаленных платежей. Все операции токенизируются (до 9 токенов на карту) в зависимости от дате использования токена (бесконтактные операции, удаленные платежи, Card-On-File, ТСП со специальным MCC и т.п.). Все операции обслуживаются в онлайн-режиме с обязательной верификацией держателя карты по ПИН-коду на мобильном устройстве, дополнительно используется fingerprinting (при аутентификации мобильного устройства для реализации, защищенной БД на устройстве), при этом все это технологически полностью соответствует контактному + бесконтактному приложению «Мир» (наследуется формат объектов данных и команд).

ПОД «ПСЕВДОНИМОМ»

Ключевым словом для безопасности здесь является «токенизация».

Токен — цифровой «псевдоним» (его еще принято называть «суррогатным номером») карты «Мир». У одной карты «Мир» может быть много токенов. Он используется вместо истинного номера карты, что позволяет не предъявлять фактический номер карты в токсических средах, а пользоваться его «суррогатом». И этот суррогатный номер действует лишь в определенном канале (например, только лишь в одном вполне определенном приложении на смартфоне), по-



<400 мс

суммарное время
обработки операции
на терминале и карте



этому перехват «токена» лишен всякого смысла, так как в другой канал его предъявить невозможно, ибо платежная система контролирует канал его поступления. Из другого канала данный токен не будет пропущен на дальнейшую обработку. Процесс токенизации/детокенизации, реализуемый в платежной системе «Мир», приведен на рисунке (рис. 2).

НА ПОРОГЕ МАЛЕНЬКОЙ РЕВОЛЮЦИИ

И, наконец, последнее, о чем поговорим в этой статье — безопасность интернет платежей. Сейчас около 10% всех авторизаций — это так называемые CNP (card not present) операции. При этом более двух третей мошенничеств с картами происходит именно при совершении таких транзакций. То есть там, где платеж происходит без самой карты, а только по ее реквизитам. С июня 2016 года в ПС «МИР» доступен сервис MirAssert 1.0 — сервис надежной аутентификации Держателя Карты ПС «Мир» на основе технологии 3D-Secure, правообладателем которой является ПС «VISA».

В настоящее время мы стоим на пороге маленькой революции в обеспечении безопасности, и эта революция называется «MirAssert 2.0». Это сервис надежной аутентификации Держателя Карты ПС «Мир» на основе новой спецификации EMVco 3-D Secure 2.0. Эта новая технология позволяет:

- ♦ проводить аутентификацию держателя карты «Мир» на его смартфоне, планшете или STB (set-top-box) во время операции электронной коммерции, в котором такую процедуру берет на себя загружаемое приложение со встроен-

ным в него компонентом 3DS SDK, сертифицированным EMVco и платежной системой «Мир»;

- ♦ поддерживать Информационный поток проверки держателя карты без непосредственного обращения эмитента к нему (Frictionless Flow) — мировой тренд обслуживания клиентов путем их узнавания дистанционно;

- ♦ поддерживать информационный поток с обращением эмитента к держателю карты (Challenge Flow). Предусматривает весь спектр современных методов аутентификации;

- ♦ Non Payment Authentication. Проверка подлинности личности держателя карты «Мир» системой эмитента при совершении неплатежной операции электронной коммерции. Например, при добавлении карты «Мир» в регистрационную запись клиента в мобильное приложение магазина;

- ♦ ООВ — out-of-band Authentication. Проверка держателя карты любым внешним способом, например, через вызванное из мобильного приложения магазина мобильное приложение банка эмитента.

Более подробное описание этого стандарта и его использования заслуживает отдельной статьи.

Подводя краткие итоги, сформулируем тезис: в наш информационный век безопасность вырастает во все этапы жизненного цикла — от зачатия до надгробного памятника, и без нее нам не жить.

И «Мир» нам в этом поможет.

Рисунок 2. Процесс токенизации/детокенизации, реализуемый в платежной системе «Мир»



Александр ВЕСЕЛОВ
руководитель отдела
технического консалтинга
ООО «С-Терра СиЭсПи»

BIS-КОММЕНТАРИЙ

Одно из ключевых направлений безопасности, обозначенных в статье, — это катастрофоустойчивость. Речь идет о наличии резервного ЦОД, который территориально удален от основного ЦОД и взаимодействует с ним по защищенному каналу связи. Развеем некоторые мифы, касающиеся защиты так называемых «толстых» каналов.

Миф № 1: Оптические каналы связи защищать не требуется. Традиционно считается, что к волоконно-оптической линии связи (ВОЛС) подключиться и перехватить трафик довольно сложно. Но эта информация давно устарела, оборудование для «съема» данных вполне доступно по цене и удобно в использовании. Например, «прищепка» FOD 5503 стоит порядка 35 тысяч рублей.

Защититься от подобных угроз можно организационными и/или техническими мерами. Организационные меры — это постоянный контроль за волокном. Но на практике это применимо только на небольших расстояниях, например, между двумя соседними зданиями в контролируемой зоне. Если речь идет о катастрофоустойчивости, то физическая защита или наблюдение неэффективны с экономической точки зрения, а иногда просто невозмож-

ны, скажем, при использовании городских подземных коммуникаций.

Технические меры — это, в основном, шифрование. Оно может быть реализовано на международных криптоалгоритмах или на отечественных ГОСТ. Если речь идет об информации, подлежащей обязательной защите в соответствии с законодательством, то требуется применять именно криптоалгоритмы ГОСТ. При этом средства криптографической защиты информации (СКЗИ) должны быть сертифицированы ФСБ России.

Реальность № 1: Любые каналы связи, в том числе и оптические, защищать необходимо. Лучше это сделать с применением сертифицированных криптосредств.

Миф № 2: Шифровать канал 10Гб/с ГОСТом невозможно. Поддержка ГОСТ-шифрования, высокая производительность и сертификация — теперь сочетание этих трех понятий стало возможным. Применение комбинированного преобразования ESP_GOST-4M-IMIT в соответствии с рекомендациями ТК26 и оптимизация сетевого стека позволили в новом продукте С-Терра Шлюз 10G получить производительность шифрования 10Гб/с на смешанном трафике. Решение на основе высокопроиз-



Алексей ЦВЕТКОВ
CISM, CISA (ЗАО НИП
«Информзащита»)

BIS-КОММЕНТАРИЙ

Работники НСПК, безусловно, проделали огромную работу, построив в свое время инфраструктуру с нуля в кратчайшие сроки, решили огромное количество организационных вопросов по подключению к себе участников платежных систем, обеспечив тем самым выполнение поставленных перед ними задач.

Если же комментировать описанные в статье направления, то прежде всего здесь также можно поздравить уже конкретно подразделение информационной безопасности АО «НСПК» с теми достижениями, которые, как говорится, на лицо. Но при этом нужно помнить, что обозначенные направления — это не просто успешно оконченные проекты, а непрерывно работающие налаженные процессы.

Обеспечение катастрофоустойчивости (Disaster Recovery Planning) или более широкая сущ-

ность — обеспечение «непрерывности бизнеса», описанное в ГОСТ Р ИСО 22301–2014, подразумевает выстроенные процессы менеджмента непрерывности бизнеса. К процессам системы менеджмента непрерывности бизнеса применяется так называемая PDCA модель, предполагающая циклически повторяющиеся процессы планирования (установления), выполнения (внедрение и работа), проверки (наблюдение и контроль), а также действия (поддержание и совершенствование).

Помня русское выражение «хочешь мира — готовься к войне», нужно периодически проводить тестирование так называемых планов восстановления после чрезвычайных ситуаций, для которых подобные планы и создаются. И чем более приближенные к реальной жизни будут такие проверки, тем легче будет вовлеченным



водительного шлюза многократно проверено как в лаборатории, так и в пилотных проектах заказчиков на различных генераторах трафика.

Реальность № 2: VPN-Шлюз, который шифрует данные в соответствии с ГОСТ со скоростью 10 Гбит/с — это реальность.

Миф № 3: Российские разработки ненадежны. СКЗИ, необходимые для защиты 10G канала, можно разделить на две части — аппаратную и программную. Аппаратные платформы в основном выбираются зарубежные, с наработкой на отказ в десятки тысяч часов. Но стоит обратить внимание и на отечественные устройства (Kraftway, Деро), практически не уступающие по качеству и надежности (справедливости ради, отметим, что компоненты этих аппарат-

ных платформ все же не российского производства).

Программную часть средств защиты лучше предпочесть российскую, которая тщательно проверяется как производителем, так и регулятором ИБ. Во время разработки производитель учитывает задачу связи ЦОДов и закладывает механизмы отказоустойчивости в продукт. В нашем случае, например, это масштабирование с балансировкой нагрузки на любом коммутаторе, поддерживающем агрегированный канал.

Реальность № 3: За последнее время российские компании сделали огромный шаг вперед в сфере надежности и отказоустойчивости сетевых средств защиты и во многом не уступают западным аналогам.

работникам действовать в реальных боевых условиях в случае катастрофы.

Идея задействовать мировой опыт по защите инфраструктуры платежных карт в России кажется очень правильной. Есть множество вопросов, которые предполагается решать с помощью Экспертной рабочей группы Совета PCI SSC Russia. Ее планы работы пока разрабатываются Управлением безопасности АО «НСПК». Один из вопросов, который волнует аудиторов, это то, что не все требования PCI SSC ограничиваются стандартом PCI DSS. Есть дополнительные требования по PIN Security, Card Production и иные направления, которые нужно не забыть, выстраивая систему проверки информационной безопасности платежной системы «МИР». Возможно, с учетом потенциально возрастающего количества специфических прове-

рок, большее число российских компаний-аудиторов смогут их осуществлять.

Данный вопрос также актуален в разрезе третьего направления, описанного в статье, где говорится о встраивании безопасности в жизненный цикл бизнес-процессов, поскольку требования к проверкам платежного программного обеспечения на предмет безопасности, проверки работы ACS серверов уже описаны в действующих международных стандартах и их можно адаптировать под российские требования.

Подытоживая вышесказанное, хочется снова отметить, что в России наконец появилась своя по-настоящему работающая платежная система, отвечающая всем основным требованиям по удобству использования и при этом обеспечивающая высокий уровень безопасности для всех ее участников.



КАК ДОВЕРЯТЬ?



Григорий СТЕПАНОВ
начальник отдела
обеспечения процессов
УЦ Департамента
безопасности
ПАО Сбербанк

ПРОБЛЕМЫ НЕДОВЕРИЯ К СУЩЕСТВУЮЩЕЙ РЕАЛИЗАЦИИ СИСТЕМЫ ЕПД И ВОЗМОЖНЫЕ СПОСОБЫ ИХ ПРЕОДОЛЕНИЯ



Факт наличия недоверия к выстраиваемой в России системе Единого пространства доверия (ЕПД) признан на государственном уровне. В обосновании необходимости внесения значительных изменений в Федеральный закон «Об электронной подписи» № 63-ФЗ (законопроект о полномочных сертификатах) читаем: «...отсутствие возможности у ведомств всецело доверять информации, внесенной в квалифицированный сертификат УЦ...».

Существует множество мнений о том, кто виноват в этой ситуации и как ее можно решить. Они базируются и на имеющемся опыте управления РКІ-инфраструктурой, и на внутренних интересах операторов электронного документооборота (ЭДО), удостоверяющих центров (УЦ), вендоров решений для УЦ и систем ЭДО и мнении основных государственных регуляторов: Минкомсвязи России, ФСБ России, Правительства Российской Федерации.

В этой статье мы попробуем дать оценку некоторым положениям Федерального закона «Об электронной подписи» от 06.04.2011 N 63-ФЗ и выделить основные проблемы в существующем законодательстве, которые требуют доработки.

ЧЕГО СТОИТ ОПАСАТЬСЯ ВЛАДЕЛЬЦУ КЛЮЧА И СЕРТИФИКАТА ЭП?

Во-первых, того, что владелец ЭП без своего волеизъявления может быть признан автором ЭД. Это накладывает на него нежелательные обременения или ответственность. А это может испортить жизнь намного хуже, чем потеря денег.

Такая ситуация теоретически может возникнуть вследствие ряда причин:

- ♦ Несанкционированно создать и сертифицировать ключи ЭП могут сотрудники УЦ (например, под давлением) или атакующие систему УЦ хакеры.
- ♦ Сотрудники УЦ, а также атакующие компьютер владельца ключа хакеры или лица, имеющие доступ к ключевому носителю, могут скопировать и/или несанкционированно использовать ключ ЭП (до его передачи владельцу).

ЧЕГО СТОИТ ОПАСАТЬСЯ ДОВЕРЯЮЩЕЙ СЕРТИФИКАТУ СТОРОНЕ?

В свою очередь, у доверяющей сертификату стороны есть риски вероятных временных, финансовых или имиджевых потерь. Сделка, заключенная удаленно, может быть признана недействительной судебным решением об аннулировании сертификата ЭП субъекта-участника сделки. При этом УЦ может отказаться от компенсации убытков.

Несмотря на то, что риски доверяющей сертификату стороны пока ещё¹ регулируются положениями действующего законодательства, могут иметь место следующие обстоятельства:

- ♦ Договор страхования УЦ может содержать ограничения по количеству страховых случаев.

¹ Законопроектом «о полномочных сертификатах» финансовую ответственность с УЦ предлагается снять в связи с их переводом исключительно в госсектор.

ВЛАДЕЛЕЦ ЭП БЕЗ СВОЕГО ВОЛЕИЗЪЯВЛЕНИЯ МОЖЕТ БЫТЬ ПРИЗНАН АВТОРОМ ЭД. ЭТО НАКЛАДЫВАЕТ НА НЕГО НЕЖЕЛАТЕЛЬНЫЕ ОБРЕМЕНЕНИЯ ИЛИ ОТВЕТСТВЕННОСТЬ. А ЭТО МОЖЕТ ИСПОРТИТЬ ЖИЗНЬ НАМНОГО ХУЖЕ, ЧЕМ ПОТЕРЯ ДЕНЕГ

♦ Договор владельца сертификата с УЦ (Регламент УЦ) может содержать ограничения финансовой ответственности УЦ.

♦ Сертификат ЭП может содержать ограничения, которые не могут быть распознаны системой ЭДО.

ЧЕГО СТОИТ ОПАСАТЬСЯ УЦ?

УЦ должны остерегаться судебной поддержки отказов субъектов от сертификатов ЭП, судебных решений о возмещении ущерба удостоверяющими центрами ущерба в пользу доверившихся таким сертификатам пострадавших сторон, а также судебных решений, связанных с неисполнением обязанностей УЦ.

Риски УЦ могут реализовываться в случаях:

- ♦ Когда у УЦ нет объективного доказательства, что субъект владеет ключом ЭП.
- ♦ Когда УЦ создает сертификат по запросу мошенника, использующего слабости системы УЦ.
- ♦ Когда УЦ создает сертификат по запросу лица, использующего поддельные документы.
- ♦ Когда УЦ создает сертификат представителя юридического лица для не обладающего данными полномочиями лица.
- ♦ Когда УЦ выдает ключ и сертификат ЭП лицу по поддельной доверенности.
- ♦ Когда УЦ несвоевременно аннулирует/прекращает действие сертификата.
- ♦ Когда УЦ использует средства ЭП, не отвечающие требованиям Закона «Об электронной подписи».

ЗАЩИТА ОТ МОШЕННИКОВ

Теперь, когда возможные уязвимости обозначены и понятны риски каждой из сторон, встает вопрос: что делать? Как действующее законодательство и судебная система должны защищать гражданина от мошенника, который получил сертифицированный ключ ЭП на его имя и теперь может применять этот ключ для подписи ЭД в своих интересах.

Для решения этой проблемы УЦ по закону должно доказать, что сертификат ЭП создавался в соответствии с заявлением указанного в нём субъекта и был признан этим субъектом при выдаче ему данного сертификата. Причём это доказательство должно быть таким, чтобы его не могла создать/изменить только одна сторона ЕД. А в случае возникновения спорной ситуации, это доказательство было признано судом.

НЕОПРЕДЕЛЕННОСТЬ № 1

В п.15 N 63-ФЗ в числе основных понятий толкуется выражение «подтверждение владения ключом ЭП». Авторы закона определяют его как получение УЦ доказательств этого владения, без уточнения, каких именно доказательств и, главное, в каком виде они должны приниматься и проверяться судами.

В результате аккредитованные УЦ, пытаясь самостоятельно домыслить суть законного требования, в качестве доказательства владения ключом ЭП демонстрируют самоподписанный запрос на сертификат (pkcs#10). Их логика состоит в том, что раз этот запрос подписан созданным ключом ЭП, значит им владеет тот, кто создал и направил этот запрос, и знает пароль для входа в систему УЦ. Кроме того, что при таком подходе нет защиты от неправомерных действий самих сотрудников УЦ, злоумышленнику для незаконного получения ключа и сертификата ЭП достаточно узнать логин/пароль пользователя системы УЦ. Более продвинутые УЦ для защиты от мошенников реализуют функцию СМС-подтверждения. Это значительно усложняет задачу для взломщика, но не дает 100% гарантии. Кроме троянской программы, ворующей пароли, с компьютера на мобильный телефон жертвы внедряется троянская программа, пересылающая злоумышленнику содержание СМС-сообщений.

НЕОПРЕДЕЛЕННОСТЬ № 2

В ст. 18 ч.3 (63-ФЗ) описано требование, которое могло бы положить конец неопределен-

ности в части объективного доказательства принадлежности квалифицированного сертификата ЭП, если бы не неоднозначность написанного. Итак: «При получении квалифицированного сертификата заявителем он должен быть под расписку ознакомлен аккредитованным удостоверяющим центром с информацией, содержащейся в квалифицированном сертификате». Казалось бы, вот он, тот обязательный и объективный бумажный документ с реквизитами владельца сертификата, составом ключа проверки ЭП, собственноручной подписью и отметкой УЦ, который можно предъявить суду в качестве доказательства, и при отсутствии которого в УЦ суд должен поддержать сторону, отказывающуюся от сертификата ЭП. Однако в законе не указано, что под «распиской» понимается именно собственноручная подпись, а под «заявителем» — указанный в сертификате субъект. Заинтересованные в дешевизне и скорости процедуры сертификации ключей ЭП новаторы быстро сообразили, что расписка вполне может быть подписью электронной и даже не усиленной, а простой — при наличии соглашения с участником ЭДО. В Минкомсвязи подтвердили, что такие действия правомерны.

Некоторые УЦ могут толковать понятие «заявитель» как «доверенное лицо, у которого есть полномочия сделать заявление, забрать носитель ключа ЭП доверяющего ему лица и расписаться в ознакомлении с сертификатом этого ключа».

Реализация простой подписи — это указание на автора ЭД без защиты целостности ЭД посредством секрета, известного только автору ЭД. Следует иметь в виду, что даже если в системе приняты дополнительные меры защиты целостности, то, как правило, владелец (администратор) системы имеет возможность изменить принятую от пользователей «подписанную» простой ЭП информацию.

Таким образом, клиенты многих аккредитованных УЦ могут оказаться беззащитными перед сотрудниками УЦ, которые могут по своей воле создать ключи и выпустить квалифицированные сертификаты ЭП на имена своих клиентов. И уж если в законе предусмотрено ограничение в использовании простой ЭП, то логично было бы также предположить её запрет в процедуре выдачи квалифицированных сертификатов ЭП. В случае подписания договоров, предусматривающих оплату, простую ЭП следует считать аналогом собственноручной подписи только после оплаты клиента.

Такая осторожность оправдана влиянием человеческого фактора: в любой организации, в том числе и в УЦ, найдется сотрудник, ко-

НЕКОТОРЫЕ УЦ МОГУТ ТОЛКОВАТЬ ПОНЯТИЕ «ЗАЯВИТЕЛЬ» КАК «ДОВЕРЕННОЕ ЛИЦО, У КОТОРОГО ЕСТЬ ПОЛНОМОЧИЯ СДЕЛАТЬ ЗАЯВЛЕНИЕ, ЗАБРАТЬ НОСИТЕЛЬ КЛЮЧА ЭП ДОВЕРЯЮЩЕГО ЕМУ ЛИЦА И РАСПИСАТЬСЯ В ОЗНАКОМЛЕНИИ С СЕРТИФИКАТОМ ЭТОГО КЛЮЧА»



торого можно подкупить или припугнуть. Существует множество лазеек, которыми может воспользоваться такой «мотивированный» сотрудник УЦ.

**ПОДВОДНЫЕ КАМНИ
ПРОЦЕССА СОЗДАНИЯ
И СЕРТИФИКАЦИИ КЛЮЧЕЙ.
КАК МОЖНО ИХ ИЗБЕЖАТЬ?**

Для получения ключа ЭП клиент приходит в УЦ с заявлением о создании и сертификации ключей ЭП, документами и квитанцией об оплате. Представитель УЦ после проверки документов в присутствии клиента подключает ключевой носитель, производит необходимые действия и распечатывает бумажные копии созданного сертификата УЦ. Обе стороны подписывают эти бумаги. Где может быть подвох?

♦ Клиент УЦ может расписаться в сертификате под своим именем, а сертификат может содержать ключ проверки от другой ключевой пары. Таким образом, сотрудник УЦ может передать секретный ключ ЭП третьему лицу;

♦ Используя особенности системы УЦ, не выявленные при её сертификации или внесенные после, можно создать копию ключа ЭП.

Чтобы избежать случаев, описанных выше, клиенту стоит создать ключ ЭП и запрос на сертификат самостоятельно на собственном оборудовании.

КЛИЕНТЫ МНОГИХ АККРЕДИТОВАННЫХ УЦ МОГУТ ОКАЗАТЬСЯ БЕЗЗАЩИТНЫМИ ПЕРЕД СОТРУДНИКАМИ УЦ, КОТОРЫЕ МОГУТ ПО СВОЕЙ ВОЛЕ СОЗДАТЬ КЛЮЧИ И ВЫПУСТИТЬ КВАЛИФИЦИРОВАННЫЕ СЕРТИФИКАТЫ ЭП НА ИМЕНА СВОИХ КЛИЕНТОВ

После чего распечатать состав своего ключа проверки и уже в УЦ перед распиской (признанием) в бумажной копии сертификата убедиться в соответствии ключа проверки в составе созданного УЦ сертификата с ключом проверки собственной распечатки.

Именно этот способ создания ЭП должны рекомендовать госрегуляторы в качестве надежного и вызывающего доверие. Однако в требованиях, наоборот, указано об обязанности УЦ создавать ключи ЭП для заявителей, поэтому даже если сам УЦ, не желая попадать под подозрения, захочет исключить функции создания ключей ЭП клиентам, сделать он этого не сможет.



Для доверия квалифицированному сертификату ЭП в Федеральном законе «Об электронной подписи» не хватает положения об объективной процедуре доказательства принадлежности ключа или квалифицированного сертификата ЭП конкретному лицу. В законе должны быть определены требования к объективности «фактора гарантии неотрекаемости от ЭП» — бумажного или электронного документа, создание и изменение которого невозможно без участия УЦ и владельца квалифицированного сертификата ЭП. Этот документ должен связывать ключ проверки ЭП с реквизитами, идентифицирующими владельца ключа. В вопросах доказательства принадлежности ЭП суды должны руководствоваться таким положением закона.

Вторым «столпом доверия» должен быть принцип безусловной ответственности УЦ за внесенную в сертификаты информацию. Сотрудники УЦ должны отвечать за обоснованность создания самого сертификата и гарантировать полное финансовое возмещение в случае доказанных убытков пострадавшей из-за доверия к изданным сертификатам стороне.

Наличие объективного фактора гарантии неотрекаемости от ЭП вместе с гарантией безусловного финансового возмещения доказанных убытков издателями квалифицированных

сертификатов наилучшим образом обеспечивают доверие к сертификатам и делают ненужным государственное регулирование в части правил идентификации субъектов и способов выдачи сертификатов УЦ. Понимая свою ответственность и невозможность подделки фактора гарантии неотрекаемости от ЭП, УЦ могут сами определять необходимые им процедуры для сертификации ключей ЭП, а не действовать строго по назначенной им «сверху» методике.

Отсутствие же вышеуказанных принципов приводит к попыткам удешевления технологии выпуска сертификатов, снижению качества проверки вносимой в них информации, ограничения ответственности, уязвимостям и как следствие — к потере доверия.

Сейчас об упрощенных способах сертификации ключей ЭП можно узнать только из регламентов УЦ. Поэтому при необходимости обработки большого количества ЭД с проверкой ЭП по сертификатам, изданным различными УЦ, могут возникнуть трудности. Особенно, с учетом того, что УЦ могут совмещать различные способы идентификации субъектов и выпуска сертификатов.

Поэтому для регулирования упрощенных способов сертификации было бы полезно законодательно установить три уровня доверия:

♦ Высший уровень доверия — полная и безусловная финансовая ответственность УЦ, гарантия объективного доказательства принадлежности ЭП, надёжный персональный ключевой носитель. Стоимость сертификата — высокая.

♦ Средний уровень доверия — ограниченная финансовая ответственность УЦ, условно-объективная процедура доказательства принадлежности ЭП, защищённость персонального ключевого носителя — по желанию. Стоимость сертификата — средняя.

♦ Начальный уровень доверия — отсутствие финансовой ответственности УЦ, процедура доказательства принадлежности ЭП — условная. Персонального ключевого носителя может не быть вовсе и, соответственно, — низкая стоимость сертификата.

Если законодательно установить единые объектные идентификаторы уровней доверия, то доверяющая сертификату сторона будет иметь возможность самостоятельно определять и декларировать минимально допустимый уровень доверия сертификату в процессах электронного взаимодействия. При правильном определении минимально допустимого уровня доверия владельцами информационных систем можно будет контролировать риски мошеннического вмешательства в ЕПД.

НЕОПРЕДЕЛЕННОСТЬ № 3

Существует возможность внесения ограничений в квалифицированный сертификат. Однако в законе не указано, что это за ограничения и кто их должен регистрировать. Не определено, как должны декларироваться объектные идентификаторы таких ограничений, а также регулироваться методы работы с ними в автоматизированных системах. Таким образом, участники ЕПД рискуют получить риск отказа от обязательств на основании того, что назначение подписанного ЭД противоречит ограничению, указанному в сертификате.

НЕОПРЕДЕЛЕННОСТЬ № 4

Отсутствует определение понятия «аннулирование сертификата» и его отличие от понятия «прекращения действия сертификата». Не указано, должны ли данные сертификаты публиковаться единым списком и как их различать в этом списке (код причины отзыва?). Также не понятно, что делать участнику ЕПД, если он доверился сертификату, который после аннулировали? Положение закона «Использование аннулированного сертификата ключа проверки электронной подписи не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием» как минимум требует пояснений с примерами.

ГОСРЕГУЛЯТОРЫ

В этой статье мы не будем перечислять все недостатки закона «Об электронной подписи», чтобы сделать вывод об основных причинах недоверия к ЕПД. Очевидна необходимость совершенствования государственного регулирования в области применения ЭП и методов объективного по отношению ко всем участникам ЕД судебного разрешения спорных ситуаций, связанных с электронными документами, заверенными ЭП.

Госрегуляторы предлагают монополизировать рынок квалифицированных сертификатов, перенеся функции аккредитованных УЦ исключительно в государственный сектор. При этом полностью отменить обязательства по возмещению убытков, возникающих в результате подрыва доверия к квалифицированным сертификатам. Результат реализации данного сценария неоднозначен: во-первых, придется перестраивать все процессы, во-вторых, риски это никоим образом не компенсирует, в-третьих, в случае реализации риска пострадавшая сторона останется без компенсации.

ПРОФЕССИОНАЛЬНОЕ СООБЩЕСТВО

Профессиональные сообщества в свою очередь предлагают стандартизировать процессы сертификации, чтобы обозначить конкретные методы идентификации и аутентификации субъектов, а также проверки их документов и описания процедур взаимодействия УЦ с субъектом сертификата. Это весьма спорный способ повышения доверия к ЕПД. Если УЦ четко выполнит все требования стандарта процедуры создания и выдачи сертификата, а единственным владельцем ключа ЭП окажется мошенник, действия которого повлекли убытки, не понятен процесс получения финансовой компенсации с УЦ. Ведь по сути дела злоумышленник действует по закону. А доверие к ЕПД пострадавшей стороны будет утрачено.

* * *

Общество заинтересовано в развитии способов удаленной идентификации и аутентификации, а также средств ЭП. Самый эффективный метод для этого, по нашему мнению, — честная конкурентная борьба производителей. Со стороны государства должна быть только поддержка развития и условий конкуренции. Поэтому при внесении изменения в Федеральный закон «Об электронной подписи» № 63-ФЗ должно учитываться мнение государственных и коммерческих компаний.

ТРУДНЫЙ ПУТЬ К УНИВЕРСУМУ

ВОПРОСЫ ОБЛАЧНОГО ХРАНЕНИЯ ЭЛЕКТРОННЫХ
ДОКУМЕНТОВ С ОБЕСПЕЧЕНИЕМ ЮРИДИЧЕСКОЙ СИЛЫ



Андрей КУРИЛО
доцент Финансового
университета при
Правительстве РФ,
председатель Комитета
по информационной
безопасности НП НСФР,
кандидат технических
наук

Мы живем в весьма своеобразное, стремительное время, когда под воздействием новых информационных технологий начинает меняться образ жизни людей — электронные устройства становятся неотъемлемой частью их жизни, одновременно создавая и увеличивая зависимость от них. На эти устройства и сервисы перекладывается все больше функций, которые кажутся нам сейчас достаточно рутинными, однако раньше были неотъемлемой частью личной деятельности человека. Наряду с возникновением новых технологий взаимодействия и обработки информации, прогнозирования поведения личности на основе анализа достаточно простых параметров, этот процесс начинает напоминать некую большую воронку, водоворот, который начинает втягивать и все быстрее закручивать людей, изменяя их ориентиры, сознание и привычный круг ценностей.

Естественно, что на этом фоне изменяется форма взаимодействия субъектов друг с другом и с государственными институтами, происходит адаптация гражданско-правовых отношений к новой форме взаимодействия. Растет число практически используемых людьми электронных документов, объемы электронного взаимодействия.

Наконец, растет число электронных документов, которые нужно хранить.

ДОПОЛНИТЕЛЬНАЯ ФИГУРА

При переходе к использованию электронных документов, классическое право личного владения документом как материальным объектом, а на этом построено все гражданское право, начинает приобретать все более относительный характер, так как гражданин как субъект правоотношений не в состоянии, не может реализовывать самостоятельно, без участия третьей стороны все процедуры, связанные как с обеспечением правильного и надежного хранения электронного документа, так и с сохранением свойств электронного документа, позволяющих ввести его в правовой оборот и использовать по назначению. Иными словами, субъект вынужден все более и более полагаться на некую третью сторону, предоставляющую ему эти сервисы, оставляя за собой лишь право пользования и распоряжения своей собственностью.

За примерами ходить не далеко: паспорт все более напоминает некий аутентификатор, через раз используемый не для удостоверения личности, а для доступа к централизованным системам идентификации и аутентификации. Аналогично дело обстоит с правами на владение автомобилем, полисом ОСАГО. Мы владеем собственностью, платим налоги, получаем предписания, извещения, квитанции, при этом у нас в руках практически нет ничего, кроме кода, с помощью которого мы реализуем свое право доступа к ресурсам, в которых находятся наши документы, в том числе и правоустанавливающие. Таким образом, в классической формуле определения права собственности субъекта как права владения, пользования и распоряжения возникает дополнительная фигура в виде некоей третьей стороны, при участии которой только и возможна реализация упомянутых прав. Более того, без нее, оказывается, в электронном мире реализовать свои права невозможно.

**В СЛУЧАЕ ПЕРЕХОДА
К ЦЕНТРАЛИЗОВАННОМУ
ХРАНЕНИЮ РЯД ПРОБЛЕМ УДАЕТСЯ
РЕШИТЬ, ПРИЧЕМ КАЧЕСТВО
РЕШЕНИЯ ПРОБЛЕМ ВОЗРАСТАЕТ
ПО МЕРЕ ЦЕНТРАЛИЗАЦИИ**

И основополагающий вопрос тут — вопрос доверия к этой третьей стороне. Или точнее — гарантий его обеспечения. Этот вопрос проработан плохо. Не являются исключением и государственные структуры, находящиеся во взаимодействии с гражданами.

ДВЕ СХЕМЫ ХРАНЕНИЯ ЭД

Еще более сложно обстоят дела с хранением электронных документов. Хранение электронных документов по принятой сейчас логике может осуществляться либо централизованно, специализированными операторами, либо децентрализованно, силами самих субъектов, в том числе гражданами.

В случае реализации схемы децентрализованного хранения приходится сталкиваться со следующими серьезными проблемами.

Во-первых, необходимо хранить ЭД таким образом, чтобы обеспечивалась их юридическая сила. А простых способов добиться этого просто нет.

Во-вторых, на протяжении всего времени хранения документов необходимо решать задачу обеспечения их т.н. «миграции» на новые технологии обработки и хранения документов, так как в противном случае со временем нарастают проблемы сохранности и читаемости информации в электронном виде, постепенно перерастая в неразрешаемые, что ведет не только к утрате юридической силы документа, но и к его физической утрате.

В-третьих, для обеспечения свойств юридической силы хранимых документов необходимо выполнять целый набор требований по управлению документами, их метаданными, по обеспечению информационной безопасности систем хранения, конфиденциальности, а также не только выполнять, но представлять соответствующие доказательства выполнения весьма большого числа регламентов по различным направлениям работы системы хранения.

ИЗДЕРЖКИ НЕСОГЛАСОВАННОСТИ

Недооценивается проблема необходимости использования очень большим числом субъектов стандартных форматов, процедур, кодировок, редакторов, визуализаторов, стандартов и протоколов электронной подписи, что на практике неминуемо приводит к тому, что реальное электронное взаимодействие из-за недостаточной согласованности взаимной работы реализовать пока невозможно.

Все это ведет к тому, что издержки при таком подходе становятся неприемлемыми, что демонстрирует левый график на рис. 1.

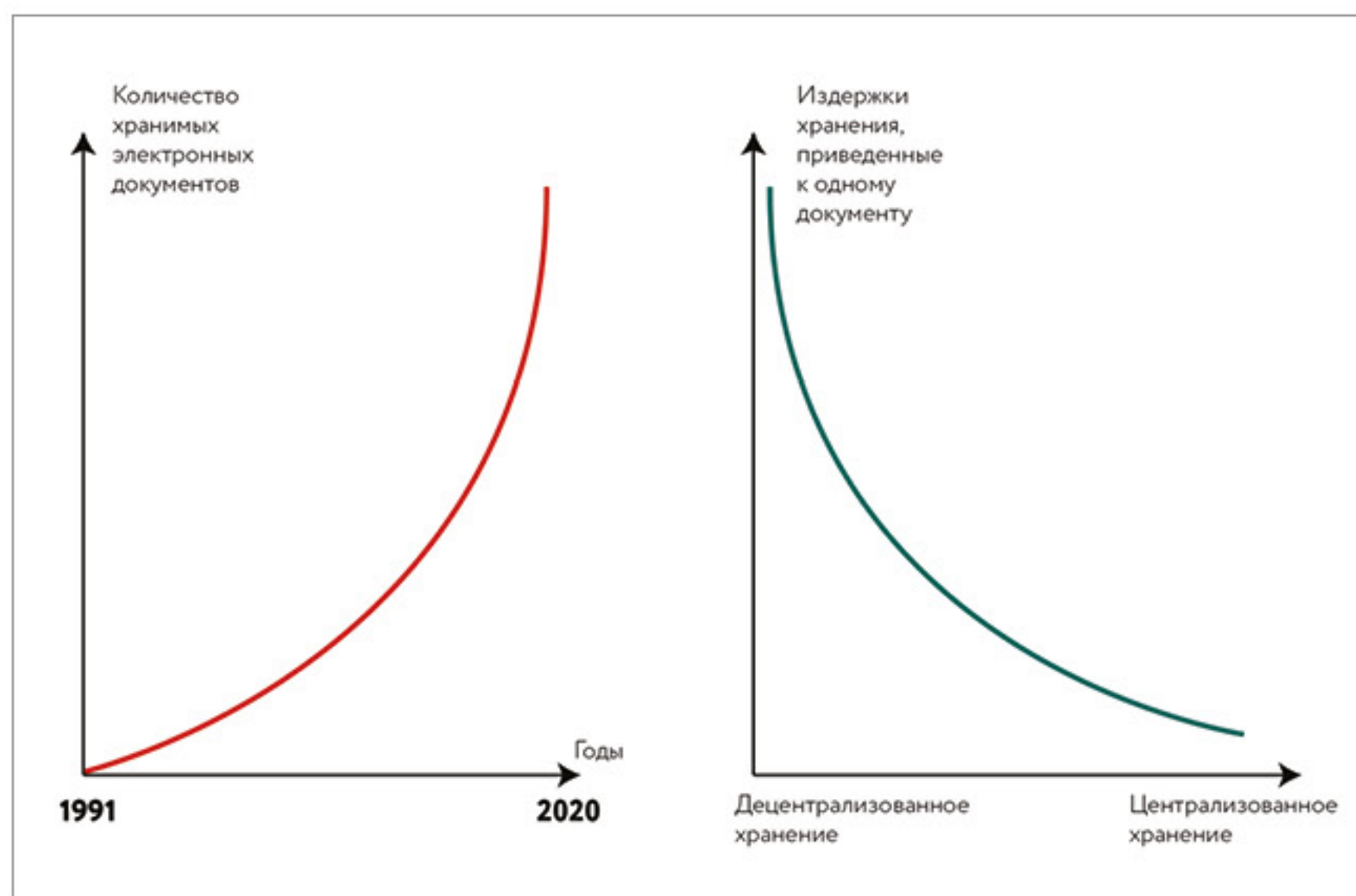


Рисунок 1

Следует отметить, что сложность и масштаб этой проблемы нашим обществом еще не осознаны.

В случае перехода к централизованному хранению ряд проблем удастся решить, причем качество решения проблем возрастает по мере централизации (правый график на рис. 1), однако в этом случае во все большей мере растут значимость вопросов надежности, катастрофостойчивости и безопасности.

СЦИЛЛА И ХАРИБДА

Вопросы безопасности необходимо прокомментировать отдельно, так как в случае централизации обработки данных и их хранения между собой борются две противоположные тенденции: максимальная централизация систем безопасности, что несомненно положительно, так как уменьшается «площадь поверхности атаки» на централизованный аппаратно-программный комплекс и улучшаются условия для контроля состояния средств безопасности и подконтрольных систем. Однако в этом случае одновременно растет размер возможного ущерба в случае нарушения защиты, а также существенно возрастает сложность используемых средств безопасности. Эти обстоятельства приводят к необходимости предъявлять гораздо более жесткие требования к деятельности персонала, причем не только специалистов безопасности и информатизации, но представителей функциональных подразделений.

В последнее время на основании данных о частоте обращения к хранимым документам, принято делить общий жизненный цикл «хранения» электронных документов по срокам: на оперативное хранение (до 5 лет), долговременное хранение (от 5 до 70 лет) и архивное хранение (свыше 70 лет). Технологически это означает на

практике реализацию совершенно разных по принципам работы систем хранения.

Хранение документов пока предполагается осуществлять децентрализованно — в архивах организаций. Порядок передачи ЭД документов в госархивы пока не определен.

СОЗДАНИЕ ДОВЕРИЯ

Вместе с тем, вне зависимости от выбранной формы хранения документов, ключевым вопросом реализации всей задачи обеспечения юридической силы хранимых документов является создание состояния доверия, возникающего в результате соответствия технологий хранения и обработки документов и их метаданных ключевым принципам хранения документов (включая электронные). Согласно ГОСТ Р ИСО 15489-1-2007 «Система стандартов по информации, библиотечному и издательскому делу. Управление документами»:

а) Читаемость на протяжении всего жизненного цикла документа.

Нарушение этого принципа возможно в результате воздействия следующих неблагоприятных факторов:

- ◆ воздействия неблагоприятных условий хранения носителей данных;
- ◆ деградация ключевых параметров носителей данных со временем;
- ◆ моральное устаревание носителей и программных средств, приводящее к их несовместимости с более новыми системами;
- ◆ моральное устаревание форматов представления данных.

b) Интерпретируемость.

c) Идентифицируемость.

d) Доступность.

e) Понятность.

f) Аутентичность.

К этим принципам следует добавить вопросы обеспечения конфиденциальности как каналов связи, так и данных, а также доверия к пользователю (достигается надежной идентификацией, аутентификацией и авторизацией) и доверия к основному инструменту, обеспечивающему равнозначность электронных и бумажных документов: электронной подписи. Вообще, похоже, что перед нами возникает задача сопоставления технических и технологических инструментов обеспечения доверия организационно-правовым, что иллюстрирует рис. 2. Отметим, что в случае использования облачной квалифицированной подписи, что гораздо удобнее, вопросы соответствия средств аутентификации и облачной электронной подписи выглядят следующим образом:

Квалифицированная усиленная облачная ЭП	Сертифицированное криптографическое средство аутентификации
Неквалифицированная усиленная облачная ЭП	Несертифицированное криптографическое средство аутентификации
Простая облачная подпись	Любое некриптографическое средство аутентификации

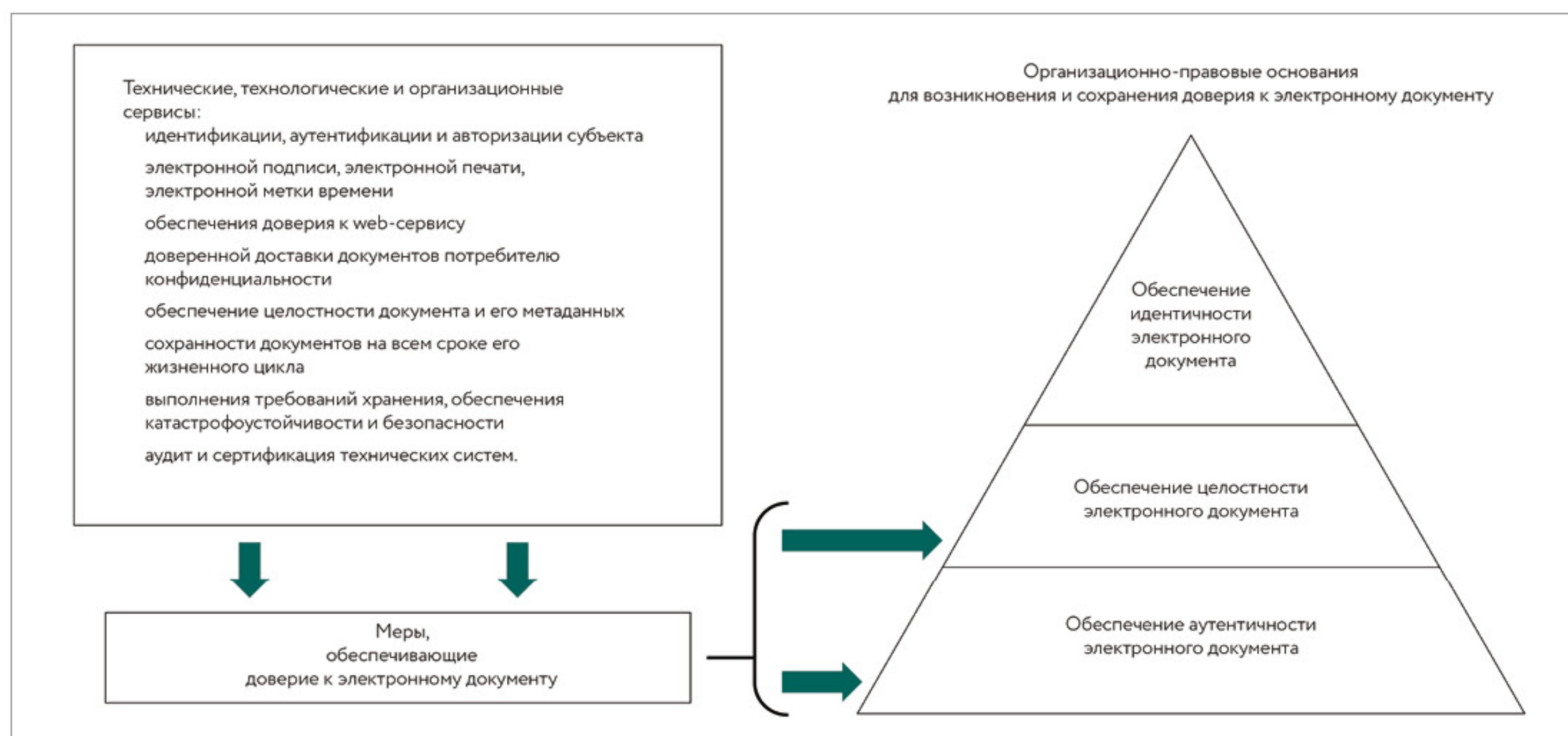


Рисунок 2. Технические, технологические и организационно-правовые основания возникновения и сохранения доверия к электронному документу

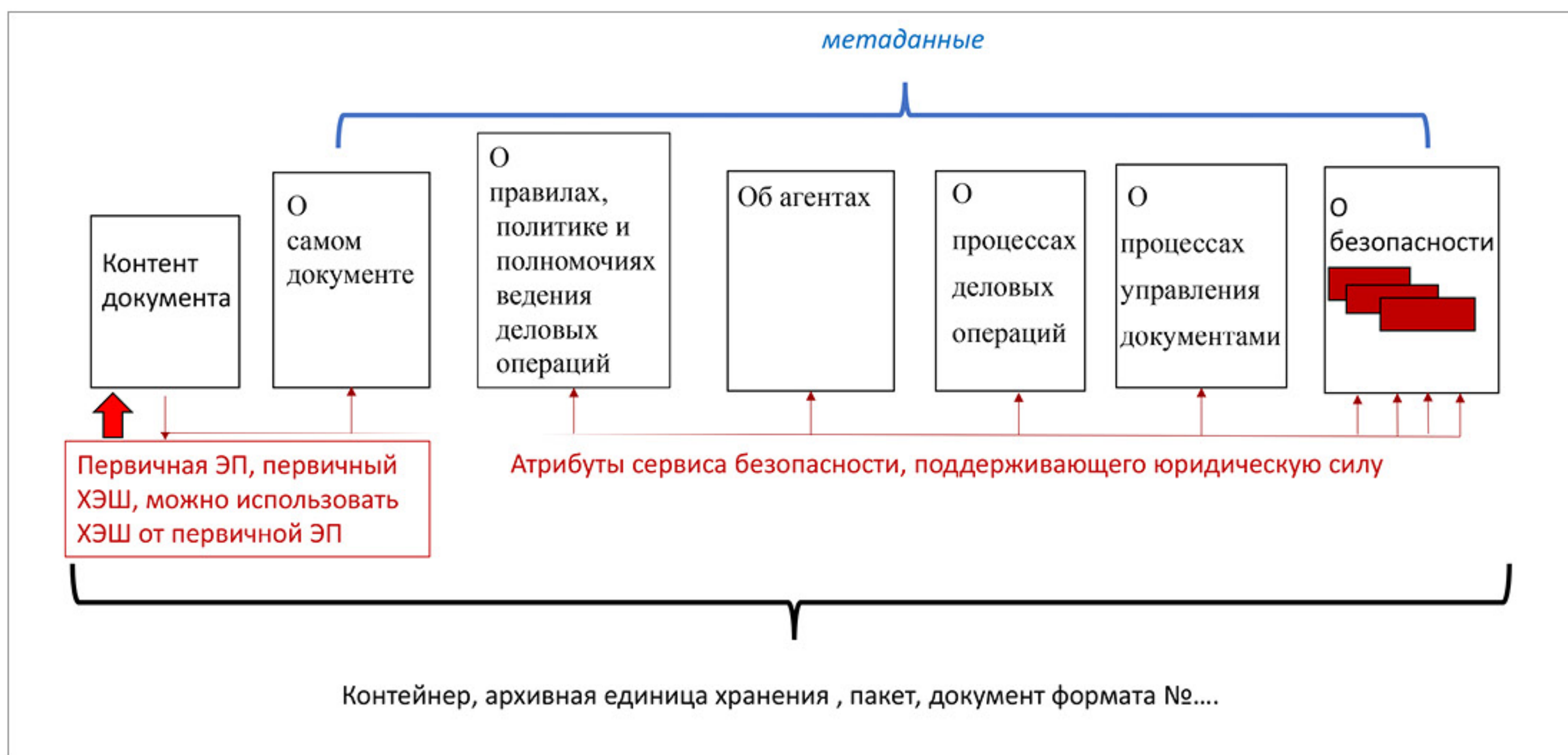


Рисунок 3. Полная структура электронного документа и его метаданных

Необходимо отметить, что организация хранения и обработки электронных документов в целом требует хранения вместе с ним достаточно большого объема принадлежащей ему дополнительной информации (метаданных).

Полная структура электронного документа и его метаданных приведена на рис. 3.

ДОКУМЕНТ И МЕТАДААННЫЕ

Как только мы переходим к предложенной структуре хранения документа, сразу встает вопрос о том, какие данные являются необходимыми для обеспечения юридической силы электронного документа и нужно ли их защищать. Иными словами, если мы используем электронную подпись, что необходимо подписывать: только документ или еще и его метаданные? А если подписываем и документ и метаданные, то как быть с изменениями, которые постоянно в них вносятся, сколько раз нужно подписывать документ и т.д.

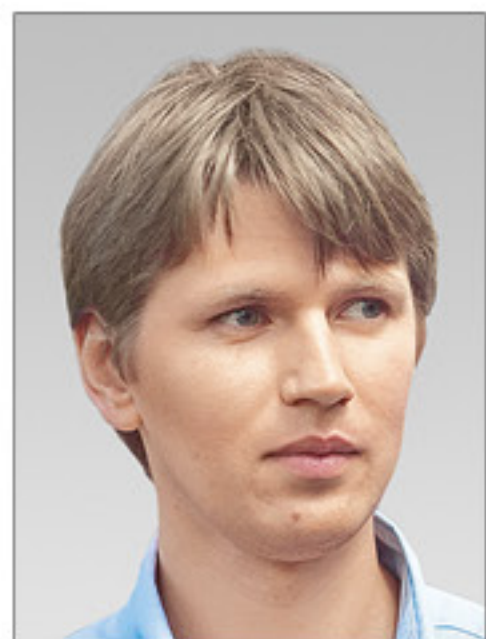
По сложившейся практике в режиме оперативного хранения документов, когда электронные документы как правило хранятся в том виде, в котором были созданы, больше внимания уделяется вопросам, прямо влияющим на сохранение юридической силы электронного документа: легитимности электронной подписи, управлению сертификатами, вопросам ее проверки и т.д. При этом вопросы управления метаданными этого документа в силу вероятно меньшей значимости на этом этапе остаются как бы в тени.

В РЕЖИМЕ АРХИВНОГО ХРАНЕНИЯ

Ситуация радикально меняется при переводе электронного документа в режим долговременного или архивного хранения под действием следующих обстоятельств:

- ◆ количество документов, подлежащих хранению, постоянно увеличивается;
- ◆ число обращений к документам существенно ниже, чем в случае оперативного хранения и снижается со временем;
- ◆ первичная электронная подпись, наличие которой в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи» является обязательным условием признания электронного документа равнозначным бумажному, быстро утрачивает возможность проверки, что требует создания и легитимизации на законодательном уровне специальных сложных технологий, а также привлечения к этой работе третьей стороны — удостоверяющих центров, что в долговременной перспективе объективно снижает надежность работы систем в целом. Следует добавить, что в этой связи вопрос доверия, конечной целью которого является создание и предоставление необходимых и достаточных условий введения электронного документа в правовой оборот, приобретает особое значение, так как процедуры, требования регламентов и результаты их контроля требуют признания как со стороны структур обеспечения информационной безопасности, так и со стороны правоведов и законодателя.

(Окончание в следующем номере)



Антон МИТРОФАНОВ
руководитель проектов,
Департамент
Безопасности
ПАО Сбербанк

«ОБЪЕКТ ОПОЗНАН!»

ИСПОЛЬЗОВАНИЕ БИОМЕТРИИ В БАНКОВСКОЙ СФЕРЕ

Большая часть банковского бизнеса построена на идентификации клиентов. Идентификация — это установление тождественности неизвестного объекта известному, а в более бытовом смысле — как Банк узнает своего клиента. С помощью процедур идентификации банки обеспечивают сохранность средств клиентов и предоставляют доступ к счетам и операциям с деньгами. Для получения 100% гарантии того, что личность имеет права на доступ к счетам, применяется определенная процедура идентификации. Сейчас в основном используется фактор знания определённой информации: пин-кода, пароля, кодового слова, личной информации; либо фактор владения определенным документом или гаджетом, подтверждающим личность: банковской картой, лич-

ным мобильным телефоном, паспортом. Оба этих фактора имеют существенный недостаток — пароль можно забыть или потерять бумажку, на которой он записан, а паспорт, банковскую карту и телефон можно подделать либо украсть.

По этой причине интерес к альтернативным методам идентификации, которые позволяют банкам с большей степенью достоверности подтверждать личность клиента, очень высок.

СТАТИЧЕСКИЕ И ДИНАМИЧЕСКИЕ

Биометрические технологии представляют принципиально новый подход к идентификации — распознаются уникальные биофизические особенности человека, которые неотъемлемы от самого человека. В общем смысле



биометрия — это измерение физических или поведенческих параметров человека. Их нельзя потерять или украсть, и сложно подделать — цена подделки существенно выше, чем в случае с паспортом или картой.

Биометрические технологии — это инструмент для измерения и сравнения биометрических характеристик человека.

Встречаются люди, похожие друг на друга (близнецы, люди с похожими голосами), однако современный уровень технологий в большинстве случаев позволяет распознавать минимальные различия между такими людьми. Точность распознавания как раз и является показателем эффективности биометрических технологий — это количество верно распознанных людей от общего количества попыток.

Сейчас на мировом рынке представлено несколько ключевых биометрических технологий. Их можно условно разделить на два класса: статические и динамические.

К статическим относятся такие технологии, как распознавание лица, отпечатка пальцев, рисунка вен — физиологические особенности, которые не изменяются со временем, либо изменяются медленно и незначительно.

К динамическим относятся технологии анализа поведенческих особенностей человека, например, почерк (в том числе и подпись документов), голос, поведение при работе с компьютером/мобильным устройством.

Статические биометрические технологии обладают намного более высокой точностью распознавания, но не всегда применимы, потому что требуют применения отдельных сканеров для получения биометрического образца.

ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ

Нельзя однозначно сказать, какая из двух технологий более перспективна — все зависит от целей использования. Мы в Сбербанке провели массу исследований и пилотных внедрений для анализа применимости технологий в различных условиях. По нашему мнению, универсальной «волшебной палочки», которая решит все проблемы идентификации личности, сейчас не существует. Все технологии имеют как преимущества, так и недостатки, и оказываются эффективными только в определенных условиях.

Так, для контактного центра распознавание голоса — отличный дополнительный фактор подтверждения личности клиента. В совокупности с традиционными методами идентификации он помогает повысить уровень доверия к этому каналу обслуживания.

Наиболее универсальной, с точки зрения возможностей использования, выступает технология распознавания лица. Решения этого класса позволяют достаточно точно идентифицировать людей и не требуют специального сканирующего оборудования: видеокамера есть в любом персональном устройстве — смартфоне, ноутбуке, планшете.

Для отдельных задач, таких, как обеспечение доступа в помещение, лучше подходят технологии распознавания рисунка вен ладони — они требуют от пользователя активного действия, и не работают в фоновом режиме, если человек

**СТАТИЧЕСКИЕ БИОМЕТРИЧЕСКИЕ
ТЕХНОЛОГИИ ОБЛАДАЮТ
НАМНОГО БОЛЕЕ ВЫСОКОЙ
ТОЧНОСТЬЮ РАСПОЗНАВАНИЯ,
НО НЕ ВСЕГДА ПРИМЕНИМЫ,
ПОТОМУ ЧТО ТРЕБУЮТ ОТДЕЛЬНЫХ
СКАНЕРОВ ДЛЯ ПОЛУЧЕНИЯ
БИОМЕТРИЧЕСКОГО ОБРАЗЦА**



просто прошел мимо. Однако их использование требует установки дополнительных сканеров.

ТЕНДЕНЦИИ ПРИМЕНЕНИЯ

Биометрические технологии не стоят на месте, вендоры развивают алгоритмы распознавания, повышают их точность и скорость поиска. Однако ключевым фактором для перехода технологии из стадии инновации в стадию промышленного использования являются сценарии применения этой технологии для решения конкретных бизнес-задач.

Сейчас можно выделить две основные тенденции применения биометрической идентификации в мире. Первая — это мультимодальная биометрия, когда используется не одна биометрическая технология, а сразу несколько.

Как говорилось выше, отсутствие 100% точности распознавания — один из ключевых недостатков биометрических технологий. Они основаны на распознавании особенностей человека и поэтому могут допускать ошибки. Например, если лица людей похожи под определенным углом, то система может их перепутать. Вероятность такой ошибки очень мала — сотые доли процента. Однако при решении финансовых вопросов даже один такой инцидент может быть критичным для всей системы и дискредитировать весь класс технологий. Для того, чтобы исключить возможность такой ошибки, используется несколько биометрических модальностей — различных особенностей человека, которые проверяются одновременно. Например, использовать проверку лица совместно с проверкой голоса: если лица двух человек по-

хожи, то голоса у них различаются, и двойник не пройдет такую проверку. Такой подход называется мультимодальной биометрией.

Второй тенденцией применения биометрии выступает использование персонального устройства как биометрического токена доступа. Все современные смартфоны оснащены камерой и микрофоном, многие имеют сканер отпечатка пальца, Samsung встроил во флагманское устройство сканер радужной оболочки глаза, а также анонсировал сканер рисунка вен в умных часах. С помощью этих возможностей пользователь получает доступ к ИТ-системам, используя биометрический сканер на устройстве, которое потом передает результаты в систему предоставления доступа.

МОШЕННИЧЕСТВО В БИОМЕТРИИ

Специалисты Службы кибербезопасности Сбербанка активно изучают вопросы, связанные с возможностью мошенничества при использовании биометрии, ведь, если Вас взломали, физиологические параметры сменить сложнее, чем пароль.

И тут возникает больше вопросов к реализации технологического решения сканера биометрических данных, чем к самой технологии распознавания.

Для примера рассмотрим технологию распознавания лица. Если система просто получает фотографию с камеры и анализирует, на кого похож человек, то похитить биометрические данные можно с помощью обычного смартфона — фото лица заменит пароль и позволит получить доступ к вашим счетам.

Для решения этой проблемы используются специальные алгоритмы и технические средства, с помощью которых можно тем или иным способом определить, что перед камерой находится живой человек, а не фото или видеозапись. К таким методам относятся анализ мимики, движения зрачков, выполнения пользователем определенных действий, случайным образом генерируемых системой, либо построения 3D-модели лица с использованием дополнительной камеры.

Способ похитить отпечатки пальцев тоже известен из множества детективных романов. Можно получить их с поверхности стакана или любого другого предмета личного пользования. Поэтому современные сканеры отпечатков пальцев могут проверять множество дополнительных параметров, таких, как пульс, температура, состав жиров на коже.

Специалисты Службы кибербезопасности Сбербанка ожидают и готовятся к тому, что после массового внедрения биометрических технологий в банковской сфере, настанет период активных попыток так или иначе обойти биометрическую идентификацию.

Тем не менее, потребность внедрения биометрической идентификации в банках неоспорима. Мошенники уже научились подделывать паспорта с высоким качеством, воровать банковские карты, использовать методы социальной инженерии. Внедрение биометрии создаст еще один барьер для борьбы с преступным сообществом, а также повысит сложность и стоимость атак для злоумышленников. Уже сейчас многие люди пользуются биометрией на личных устройствах, например, сканером отпечатков пальцев на устройствах Apple. По результатам наших исследований большая часть клиентов банков готова к использованию биометрии при обслуживании.

Банки от поставщиков решений по биометрической идентификации, в первую очередь, ожидают законченных решений, которые можно внедрить в эксплуатацию без больших накладных расходов. Сейчас в каждом виде биометрической идентификации есть свои лидеры. Это касается и разработчиков программного обеспечения, и производителей оборудования. Российские производители занимают на этом рынке не последнее место. Есть технологии, которые входят в перечень лучших на мировом рынке.

В Сбербанке биометрическая идентификация применяется уже сейчас, но пока в ограниченных объемах. Одной из наиболее известных технологий является доступ к мобильному приложению нашего банка по отпечатку пальца, с использованием технологии Apple TouchID.

ПО РЕЗУЛЬТАТАМ НАШИХ ИССЛЕДОВАНИЙ БОЛЬШАЯ ЧАСТЬ КЛИЕНТОВ БАНКОВ ГОТОВА К ИСПОЛЬЗОВАНИЮ БИОМЕТРИИ ПРИ ОБСЛУЖИВАНИИ

Кроме того, за последние два года мы провели несколько пилотных проектов по применению биометрии. Варианты системы оплаты по отпечаткам пальца действуют в магазинах — партнёрах банка. Несколько филиалов банка в тестовом режиме были оснащены биометрическими системами распознавания лица и распознавания рисунка вен.

В недавнем прошлом в Сбербанке стартовал проект по оснащению контактного центра системой распознавания голоса клиента, а в ближайшее время запускается проект по оснащению офисов обслуживания клиентов системой распознавания лица.

Особого внимания заслуживает социальный проект банка — «Ладшки». Его суть заключается в оснащении школьных столовых терминалами для оплаты обедов. Изначально предполагалось, что оплата будет производиться по карточкам, однако дети их часто теряли, поэтому в терминалы внедрили систему распознавания рисунка вен. Проект получил положительные отзывы. Пользователи отметили удобство его использования и точности распознавания. Сейчас идёт массовое внедрение этой технологии в школах России.

* * *

Технологии надежной и удобной идентификации чрезвычайно важны для успешности банковского бизнеса. Использование биометрических технологий является одним из направлений развития технологий идентификации, которое позволит существенно повысить удобство использования банковских сервисов.

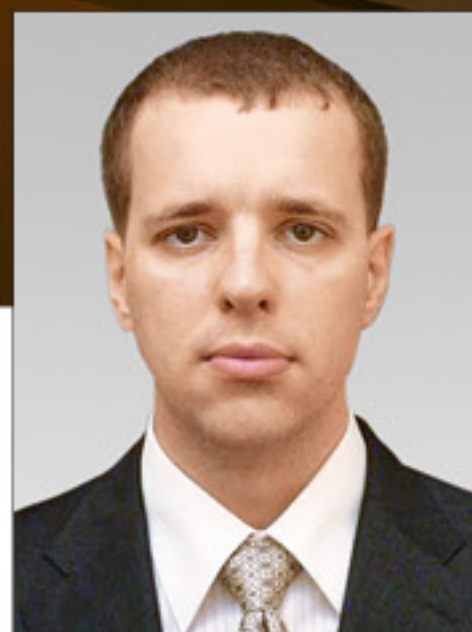
При этом необходимо помнить, что сами по себе биометрические технологии не являются гарантом безопасности, биометрические данные можно похитить так же, как любые другие. При внедрении биометрических технологий нельзя забывать об обеспечении безопасности их применения.

Ключевыми тенденциями применения биометрии сейчас является использование нескольких биометрических модальностей и комбинация биометрических факторов с традиционными методами идентификации для повышения надежности.

КИБЕРВИМОГАТЕЛЬНОСТЬ. НОВЫЙ ТРЕНД КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ



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



Александр ПАЛЬЦЕВ
IT Security Manager at Savoy Development Ltd,
The Republic of Seychelles

Ransomware («ransom» — выкуп + «software» — программное обеспечение) — вирус-вымогатель, вредоносное программное обеспечение, требующее выкуп за возврат доступа к данным жертвы, — похоже, имеет все шансы поработить компьютерных пользователей.

Майская массированная атака червя WannaCry, поразившая сотни частных и государственных компаний, привлекла внимание мировых масс-медиа к ransomware-вредоносам. Тема в тренде и интересна теперь не только специалистам ИБ. Как известно, червь WannaCry за неполные две недели поразил более 300 тысяч компьютеров по всему миру. Суммарный ущерб в мировом масштабе оценивается в 1 млрд долларов. Для распространения была использована закрытая еще в марте уязвимость EternalBlue и бэкдор DoublePulsar.

Стабильный рост в данном криминальном сегменте наблюдался давно, как минимум на протяжении последних двух лет. Последняя массовая атака, выполненная на весьма качественном уровне, означает, что рост продолжится и дальше.

Основой для роста ransomware-сектора киберпреступности стали два фактора — развитие анонимных систем онлайн-платежей (в особенности bitcoin) и новая ступень организации киберпреступности — децентрализация и предоставление вредоносного ПО как сервиса (RaaS).

Основная цель преступников остается прежней — максимальная нажива, схема же, в сравнении с привычными «Локерами», слегка меняется.

Вредоносная программа получает доступ к данным своей жертвы, а затем шифрует их. Далее с помощью этой же программы или другим способом

злоумышленник предлагает владельцу данных приобрести инструмент для расшифровки за плату, которую необходимо перевести по указанному адресу. Шифрование без возможности восстановления при этом равноценно потере данных.

Принципиальный экономический момент состоит в том, что инструмент восстановления зашифрованных данных для владельца дешевле, чем стоимость потери этих данных.

ЭКОНОМИКА ПРЕСТУПЛЕНИЯ

Большинством хакеров движет именно жадность, стремление обогатиться, а вовсе не злоба или идеологические мотивы. По всей видимости, при массовом употреблении этот вид преступлений экономически гораздо более привлекателен, чем продажа украденной у кого-то информации.

Зачем сбывать краденую информацию по сниженным ценам в условиях конкуренции между хакерами? Вымогательство проще и, похоже, надежнее.

Каждая конкретная жертва имеет свою личную границу цены, которую она готова заплатить за восстановление своих данных и нормальное продолжение своей деятельности. Хакеру, в свою очередь, надо угадать эту цену.

Попробуем встать на место хакера. Предположим, что у него есть средства обхода защиты средств безопасности жертвы. Получив доступ, он может украсть критическую для жертвы информацию и постараться потом ее кому-то продать. Эта операция обладает сравнительно низкой доходностью в силу высокой конкуренции между хакерами. Кроме того, хакер может безвозвратно уничтожить эту информацию.

Альтернативный подход состоит в следующем: зашифровать эти данные и потребовать выкуп. Моральная ответственность хакера при таком преступлении невелика. Никто не умрет, никто не потеряет свои сбережения. И даже информация не крадется и не разглашается. Как только осуществляется перевод денег из рук в руки, жертва восстанавливает свои данные. Очень рациональная стратегия: «заплатите, получите ключ для восстановления и работайте дальше».

Ключевым вопросом является цена, при которой жертва соглашается заплатить и не сообщать в правоохранительные органы. Для определения стоимости выкупа могут быть использованы предположения о роде деятельности жертвы, либо конкретная информация о жертве, собранная вредоносной программой. Например, при проведении целевой атаки по списку адресов, хакер может заранее предположить потенциальную важность данных. Список адресатов может быть сформирован по закрытой (утекшие базы, взломанные сайты и т.д.) либо открытой информации (социальные сети, сайты поиска работы).

По данным отчета Symantec «Ransomware and Business 2016», в 2016 году было обнаружено более 100 новых семейств ransomware-программ, при этом средний размер выкупа, запрашиваемого программами, составил \$679 по сравнению с \$294 в 2015 году.

КНУТ И ПРЯНИК. «ПРИВЕДИ ДРУГА!»

Кроме цены для жертвы также немаловажным может быть риск разглашения информации. Итак, «кнут» — это угроза удаления и/или разглашения информации.

Может существовать и своеобразный «пряник». Например, ransomware-программа Porcorn Time в своем требовании выкупа объясняет действия хакера тяжелым положением «сирийских студентов», вынужденных таким способом собирать пожертвования.

Чтобы пользователь был поговорчивей, используются и классические средства вирусписателей: удаление части данных по таймеру, сообщения о якобы незаконных действиях (со ссыл-

**ПРИНЦИПИАЛЬНЫЙ ЭКОНОМИЧЕСКИЙ
МОМЕНТ СОСТОИТ В ТОМ, ЧТО
ИНСТРУМЕНТ ВОССТАНОВЛЕНИЯ
ЗАШИФРОВАННЫХ ДАННЫХ
ДЛЯ ВЛАДЕЛЬЦА ДЕШЕВЛЕ, ЧЕМ
СТОИМОСТЬ ПОТЕРИ ЭТИХ ДАННЫХ**

ками на статьи УК) и иные трюки. Например, упомянутая выше ransomware-программа Popcorn Time в числе прочего предлагает пользователю вместо платежа разослать специально подготовленные ссылки своим друзьям. В случае, если хотя бы двое из них заплатят, пользователь получит ключ расшифровки бесплатно.

Если же пользователь оказался несговорчивым и предпочел понести потери информации вместо потери денег, то у хакера может иметься инструмент анализа результативности кампании, позволяющий скорректировать работу ПО. Так, по данным отчета McAfee Labs "Understanding Ransomware and Strategies to Defeat it", некоторые ransomware-программы, предоставляемые в качестве сервиса, и, таким образом, доступные даже новичкам, имеют в комплекте инструменты оценки до-

ПРИМЕР ИЗ ЖИЗНИ

Несмотря на некоторую сложность системного вредоносного ПО, практическая его реализация не представляет особых проблем для программиста средней руки или даже студента.

Например, не так давно один наш коллега после открытия «левого» письма в электронной почте столкнулся с вымогателем Ransom: Win32/Simlosap.A (другие названия: Trojan.Encoder.567; Win32/Filecoder.CQ). Анализ кода зловреда показал, что распространение трояна происходит в упакованном виде. Использовался самодельный упаковщик, написанный на Visual Basic. Сам ransomware-вымогатель был разработан с использованием компилятора Delphi 6.0–7.0. Для реализации основной задачи — шифрования трояна применяет трехступенчатое шифрование RSA (768 бит), которое также было



Рисунок 1. Скриншот программы с запросом денег за расшифровку

реализовано на Delphi. Для функционала работы с многоразрядной арифметикой привлекались сторонние библиотеки.

Шифрование файла устроено следующим образом. Первые 30 000 байт содержимого шифруются сложением по модулю 256 с гаммой, для генерации которой используется алгоритм хеширования MD5. Если длина содержимого больше 30 000 байт, в нем на случайных позициях находятся три блока длиной 1024 байт, которые шифруются алгоритмом RSA на сгенерированном в начале работы открытом ключе. Формируется определенная служебная информация, которая записывается в конец зашифрованного файла.

ВЫВОДЫ И ПЕРСПЕКТИВЫ

Как известно, даже идеально построенная система ИБ предприятия, к сожалению, не гарантирует 100% безо-

пасности. Что уж говорить о рядовых пользователях, которые в большинстве случаев не имеют даже актуального антивирусного софта.

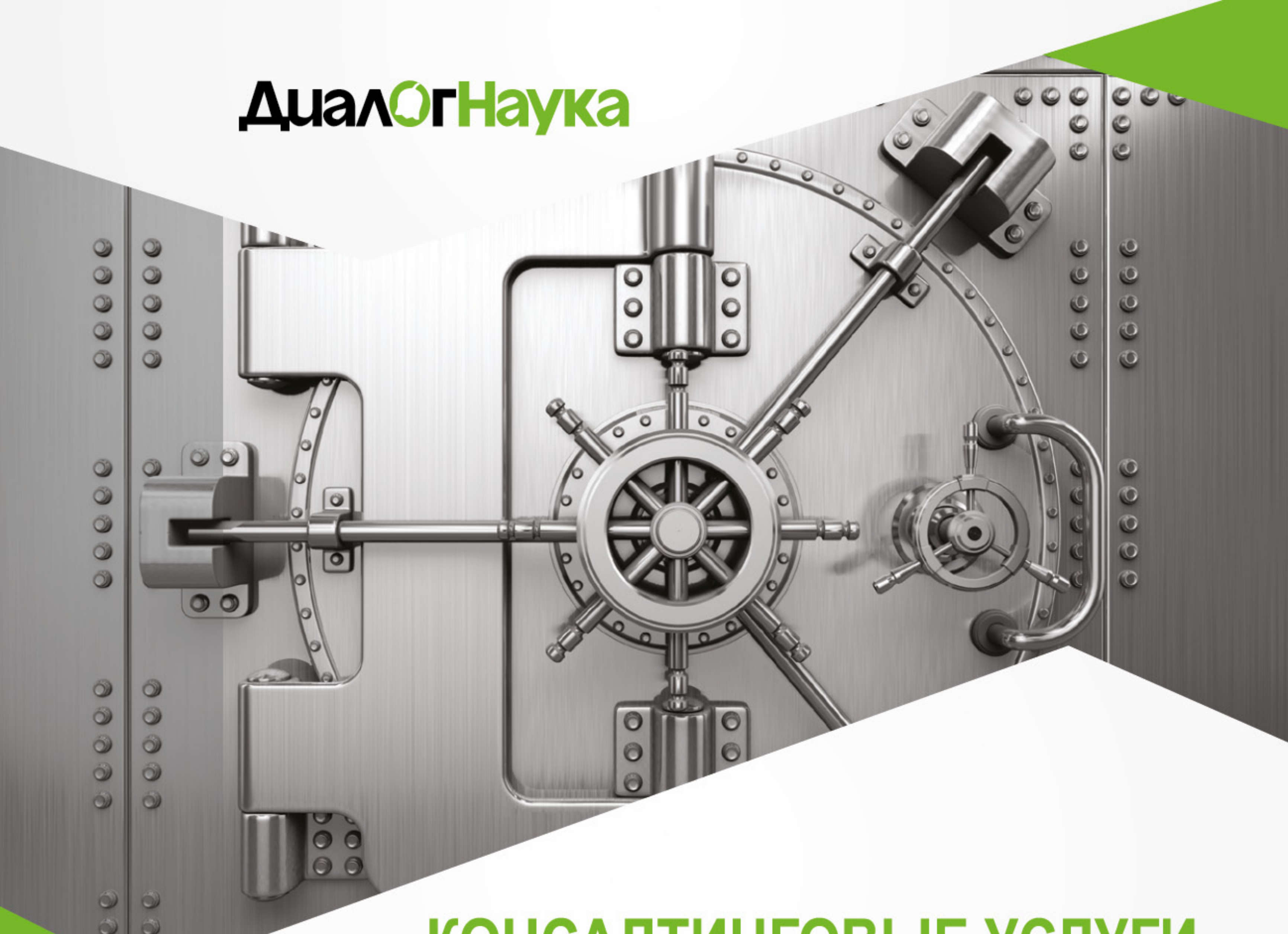
Если шифрование в коде ransomware-программы организовано правильно, то дешифрование данных оказывается крайне сложным и требует анализа кода и вскрытия алгоритма. Единственным надежным средством обезопасить данные от работы ransomware-вирусов остается грамотно построенное резервное копирование.

* * *

Можно прогнозировать бурный рост преступлений с использованием Ransomware, поскольку это и в самом деле весьма удобный и доходный способ криминального обогащения.

ССЫЛКИ

1. www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
2. <https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/>
3. www.mcafee.com/it/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf



КОНСАЛТИНГОВЫЕ УСЛУГИ ДЛЯ КРЕДИТНО-ФИНАНСОВЫХ ОГРАНИЗАЦИЙ

- Оценка соответствия требованиям стандарта Банка России СТО БР ИББС
- Проведение аудита на соответствие требованиям стандарта PCI DSS
- Оценка соответствия требованиям Положения Банка России №382-П
- Тесты на проникновение и инструментальный аудит безопасности
- Защита персональных данных

Дополнительная информация:
+7 495 980 67 76
www.dialognauka.ru



Андрей ШПАКОВ
ведущий инженер отдела
технического консалтинга
ООО «С-Терра СиЭсПи»

КАКОЙ VPN ВЫБРАТЬ?

СРАВНЕНИЕ ТЕХНОЛОГИЙ И ПРОТОКОЛОВ ЗАЩИЩЕННОГО ДОСТУПА

VPN является неотъемлемой частью всех систем информационной безопасности, в том числе тех, которые обеспечивают защиту информационных систем финансовых организаций. Эта технология является самым простым, понятным и доступным способом безопасно объединить территориально распределенные площадки и надежно защитить информацию при передаче по сетям общего пользования.

Существует множество сценариев применения VPN: организация взаимодействия между удаленными офисами, подключение удаленных сотрудников или клиентов, подключение банкоматов, доступ к ЦОД-ам, в которых сосредоточены ресурсы информационных систем банка. Кроме задачи обеспечения взаимодействия, в ряде случаев, VPN позволяет сформировать четкий периметр защиты и обеспечить доступность сегментов информационной системы.

Однако, прежде чем приступить к выбору конкретного поставщика решения, нужно и важно понимать, какие технологии VPN существуют и каково различие между ними.

ПРОПРИЕТАРНЫЕ ПРОТОКОЛЫ

Все протоколы для передачи данных разделяются на две категории.

Первая категория, о которой пойдет речь — проприетарные (закрытые) протоколы и технологии, являющиеся интеллектуальной собственностью отдельных компаний. Преимущества такого подхода в том, что технология может быть относительно быстро до-

работана под требования производителя оборудования или желание конкретного заказчика. Однако, есть и ряд минусов.

Во-первых, для заказчика велика вероятность стать объектом исследований и технических доработок за свои же деньги. Для того, чтобы снизить риск появления архитектурных ошибок, необходимо максимально полно отработать новую технологию с привлечением как можно более широкого круга экспертов. К сожалению, база заказчиков российских вендоров, использующих проприетарные протоколы, не всегда позволяет это сделать. К слову, зарубежные лидеры ИТ-рынка не идут путем создания проприетарных протоколов. Они развивают функциональные возможности общепринятых протоколов, открывают доступ к своей технологии и делают ее публичной, доступной для других производителей.

Во-вторых, существенным недостатком является то, что нестандартный дизайн продукта и недокументированное поведение устройств могут поставить заказчика в зависимость от поставщика продуктов. Если качество сервиса или услуг перестанет устраивать заказчика, переход с проприетарного протокола на другой может быть крайне затратным, либо вообще невозможным без полной перестройки

системы безопасности. В лучшем случае заказчик сможет рассчитывать на использование б/у аппаратных платформ, на которые можно будет поставить новое программное обеспечение. Специалисты компании «С-Терра СиЭсПи» уже имели опыт установки своего VPN-шлюза на платформы компании Stonesoft (которая хоть и использовала стандартные протоколы, но, как известно, прекратила активную деятельность на рынке сетевой безопасности в России).

В-третьих, любой нестандартный дизайн создает проблемы при поиске неисправности или неправильной работе устройств. Необходимо иметь в штате людей, знающих особенности поведения как стандартного оборудования, так и специфику работы технологий конкретного производителя.

И, в-четвертых, нужно учитывать тот факт, что проприетарный протокол имеет минимальные шансы для получения совместимости с другими производителями.

ПУБЛИЧНЫЕ ПРОТОКОЛЫ

Вторая категория — это публичные (или стандартные) протоколы, которые могут применяться в оборудовании, произведенном различными вендорами. Описание этих технологий приводится в специальных докумен-

**НУЖНО УЧИТЫВАТЬ ТОТ ФАКТ,
ЧТО ПРОПРИЕТАРНЫЙ ПРОТОКОЛ
ИМЕЕТ МИНИМАЛЬНЫЕ ШАНСЫ
ДЛЯ ПОЛУЧЕНИЯ СОВМЕСТИМОСТИ
С ДРУГИМИ ПРОИЗВОДИТЕЛЯМИ**

РЯД РОССИЙСКИХ ПРОИЗВОДИТЕЛЕЙ, В ТОМ ЧИСЛЕ КОМПАНИЯ «С-ТЕРРА СИЭСПИ», ОБЕСПЕЧИЛИ СОВМЕСТИМОСТЬ СВОИХ СЕРТИФИЦИРОВАННЫХ РЕШЕНИЙ ПРИ ИСПОЛЬЗОВАНИИ ПРОТОКОЛА IPsec

тах (Request for Comments, RFC) организации инженерного совета Интернета (Internet Engineering Task Force, IETF). Их создают и дополняют лучшие эксперты отрасли. Для VPN из публичных протоколов наиболее часто используются IPsec и SSL в различных вариациях.

SSL (TLS)

Это семейство протоколов предназначено для обеспечения удаленного клиентского доступа и ориентировано на конкретные пользовательские приложения. Существует несколько вариантов использования SSL (TLS):

Бесклиентский режим. В этом режиме используется односторонняя аутентификация сервера на клиентской стороне. При этом пользователю не требуется устанавливать специализированное клиентское ПО для защиты трафика, а достаточно иметь на АРМ-е только криптопровайдер. Работа в таком режиме возможна только с Web-приложениями, причем в российских реалиях есть привязка к не самому популярному браузеру Internet Explorer. Такой режим работы подходит, например, для ограниченного перечня сценариев защищенного доступа к web-порталу.

Клиентский режим. Если требуется обеспечить доступ к какому-либо другому приложению, используется специальный SSL (TLS)-клиент. В этом режиме есть возможность использовать двухстороннюю аутентификацию.

Одним из главных преимуществ протокола является отсутствие или минимальная необходимость персональной настройки клиента. Однако, в случае, если на рабочую станцию будет установлено новое ПО или появится новый сервис, к которому требуется доступ, пользователь должен будет

добавить эти параметры в настройки клиента.

Также нужно учитывать особенность, что стандартный SSL работает на уровне приложения и не может защитить трафик от сетевого оборудования или от сегментов сети. Решить эту задачу может протокол DTLS, но он тоже имеет клиент-серверную модель и слабо распространен среди российских производителей.

IPsec

IPsec работает на более низком уровне модели OSI, и для его работы не требуется поддержка со стороны приложений. Он отлично подходит для создания защищенных соединений как между филиалами в территориально распределенной сети, так и для организации защищенного удаленного доступа.

За счет работы протокола на сетевом уровне, для работы VPN не требуется вносить изменения в ПО на рабочих местах. Все пользовательские приложения работают «прозрачно» и не знают про существование VPN. Протокол всегда осуществляет двухстороннюю аутентификацию.

При реализации удаленного доступа требуется персонализированная настройка клиента для каждой конкретной рабочей станции. При этом клиент защищает все сетевые взаимодействия между АРМ-ом и удаленной сетью. Следовательно, необходимость наличия на рабочих местах пользователей средств защиты от несанкционированного доступа к АРМ является более актуальной, чем в случае SSL.

IPsec является самым известным протоколом для построения VPN и продолжает развиваться. Появилась вторая версия протокола распространения ключей IKE, стек протоколов является частью стандарта IPv6.

Кроме вышеперечисленного, у стандартных протоколов IPsec и SSL (TLS) есть определенные преимущества именно в российских реалиях. Речь идет про деятельность технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) в области выработки рекомендаций по использованию единообразных узлов замены и параметров эллиптических кривых в российских ГОСТах по криптографии, а также их использование в протоколах передачи данных. Эта деятельность уже принесла свои плоды — ряд российских производителей, в том числе компания «С-Терра СиЭсПи», обеспечили совместимость своих сертифицированных решений при использовании протокола IPsec. Безусловно, если бы применялись проприетарные протоколы, таких результатов невозможно было бы достичь. Хотя такие процессы не происходят быстро, у заказчиков появляется перспектива исполнения заветной мечты — появления технической совместимости различных сертифицированных VPN-решений между собой.

Использование стандартных протоколов в разных областях (Syslog, SNMP, Netflow и т.д.) позволяет объединять продукты в единую систему. Например, такая практика является общепринятой при решении задач мониторинга и построения SIEM-систем.

ДЕЛАЕМ ВЫВООДЫ

При выборе стандартного протокола заказчик должен определиться с желаемым сценарием использования. Если ему достаточно защиты лишь отдельных сервисов и важна простота настройки — SSL (TLS), при необходимости полной сетевой связности между объектами — его выбор IPsec.

* * *

Вместе с тем, необходимо помнить, что помимо протокола передачи данных, в каждом решении есть большое количество разных технологий и особенностей. Поэтому стоит оценивать и сравнивать продукты в целом, в зависимости от поставленной задачи.



**Антон
СВИНЦИЦКИЙ**
руководитель
отдела консалтинга
АО «ДиалогНаука»



**Виктор
СЕРДЮК**
генеральный
директор
АО «ДиалогНаука»

ОСНОВНЫЕ ВЕКТОРЫ АТАК НА БАНКИ

СОВРЕМЕННЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

На сегодняшний день банки все чаще становятся мишенью для атак со стороны злоумышленников, поскольку проникновение в автоматизированные системы банка позволяет нарушителям получить прямой доступ к финансовым ресурсам. Именно поэтому банковская сфера одной из первых попала в лидеры по количеству целенаправленных атак и уровню понесенного ущерба, который в реальности может превышать официальные данные в разы. В рамках данной статьи будут рассмотрены основные векторы для потенциальных атак на кредитно-финансовые организации, а также возможные пути защиты от них.

АТАКИ НА АБС

Для проникновения в корпоративную сеть банка и последующего получения доступа к АБС злоумышленники чаще всего используют два вектора атак — это рассылка фишинговых сообщений электронной почты с вредоносным содержанием либо привлечение банковских сотрудников на сайты с вредоносным содержанием или фишинговым интерфейсом, имитирующим внутренние системы банка. В обоих случаях важным элементом проникновения внутрь корпоративной сети является преодоление периметровых средств защиты. Для этого используются специальные вредоносные программы, которые оптимизированы для преодоления стандартных средств за-

щиты, таких как антивирусы и системы обнаружения атак.

Отличительной особенностью таких целенаправленных атак (APT) является постоянное совершенствование методов атаки, адресность используемых экземпляров вредоносного кода и контролируемость самого процесса атаки с последующим уничтожением следов проникновения. В современных условиях это означает использование сложных методов упаковки вредоносных программ, адресный фишинг, который сложно отличить от легитимного информационного ресурса или письма, скрытые протоколы коммуникации между злоумышленником и инфицированными компьютерами и, в результате, длительный период присутствия нарушителя в системе. Так, по данным компании Hewlett Packard Enterprise, среднее время между проникновением злоумышленников в систему и их обнаружением составляет 243 дня, то есть практически 8 месяцев.

Основными инструментами для защиты от целенаправленных атак являются средства углубленного анализа передаваемых файлов с возможностью их запуска в виртуальных машинах — этот инструмент в простонародье называется «песочница» (sandbox). Она позволяет обнаруживать хорошо замаскированные вредоносные программы и блокировать их дальнейшее распространение в корпоративной сети банка. Одним из примеров такого рода систем является решение FireEye, которое хо-

рошо зарекомендовало себя в ряде ведущих российских банков.

Еще одним инструментом защиты являются системы обработки и корреляции событий информационной безопасности (SIEM). Правда, для ее эффективного функционирования требуется установка и правильная настройка правил корреляции, а также наличие внедренных процессов управления инцидентами безопасности. При этом для расширения возможностей SIEM-систем необходимо использовать различные классы средств защиты информации, которые будут являться поставщиками событий безопасности, например, системы выявления аномалий в поведении пользователей (UEBA). Интеграция с UEBA позволяет выявлять нелегитимное использование учетных записей пользователей злоумышленниками, получившими доступ к АБС путем перехвата идентификационной и аутентификационной информации. В большинстве случаев поведение такого пользователя будет сильно отличаться от будничных действий обычного сотрудника или пользователя, назначенного на такую же роль в АБС.

АТАКИ НА СИСТЕМЫ ДБО

Если собственную информационную систему банк еще может контролировать, то защиту клиента обеспечить значительно сложнее. Поэтому часто целенаправленные атаки организуются не на сам банк, а на его клиентов. Здесь могут использоваться целена-

правленный фишинг якобы от имени банка, фальшивые мобильные приложения, вредоносные модули браузера, перенаправляющие запросы пользователя на подставные сайты, и многое другое.

Системы ДБО в вопросах обеспечения безопасности финансовых транзакций очень сильно зависят от трех аспектов: доверенной аутентификации клиента и подтверждения проводимых операций, безопасной среды исполнения приложения и защищенного канала взаимодействия между системой клиента и банком в рамках системы ДБО. Хакеры могут целенаправленно атаковать все три элемента. Например, для получения паролей от веб-приложения создать фиктивный интерфейс банка и послать на него ссылку клиентам или для атаки на коммуникационную составляющую внедрить в браузер модуль, который будет перенаправлять запросы на специальный посреднический сайт злоумышленников. При заражении вредоносной программой рабочей станции, с которой происходит взаимодействие с системой ДБО, злоумышленники могут перехватывать весь трафик и подменять реквизиты платежей.

Для каждого из трех указанных ключевых компонентов разработаны средства противодействия целенаправленным мошенническим действиям. Для защиты аутентификации — одноразовые пароли, средства двухфакторной аутентификации или аппаратные устройства с электронной подписью документов. Для защиты от вредоносного кода — антивирусы с встроенными функциями контроля поведения приложений (HIPS). Для защиты коммуникаций — взаимная аутентификация сторон и шифрование канала связи между клиентским приложением и сервером банка, например, с помощью TLS. Однако целенаправленные атаки характерны тем, что стандартные методы могут не сработать, поэтому банк должен также контролировать логику происходящих событий с помощью систем защиты от мошенничества или антифрод-систем, адаптированных под требования банка. Такие системы позволяют обнаруживать аномальное поведение клиентов и блокировать

ПО ДАННЫМ КОМПАНИИ HEWLETT PACKARD ENTERPRISE, СРЕДНЕЕ ВРЕМЯ МЕЖДУ ПРОНИКНОВЕНИЕМ ЗЛОУМЫШЛЕННИКОВ В СИСТЕМУ И ИХ ОБНАРУЖЕНИЕМ СОСТАВЛЯЕТ 243 ДНЯ, ТО ЕСТЬ ПРАКТИЧЕСКИ 8 МЕСЯЦЕВ

подозрительные транзакции. В ряде случаев есть возможность создавать антифрод-системы на базе уже установленных в банке SIEM-систем. Так, например, такая возможность есть у продуктов HPE ArcSight, на базе которых можно создать дополнительный набор правил корреляции и отчетов, выявляющих признаки мошенничества в банковских транзакциях.

АТАКИ НА СИСТЕМЫ МЕЖБАНКОВСКОГО ОБМЕНА

Переводы денежных средств осуществляются как с помощью платежных систем, таких как Visa, MasterCard или НСПК, так и с помощью системы межбанковских расчетов SWIFT и/или Банка России. В данном случае атака может быть направлена на подделку реквизитов платежей в транзакции или поручении, чтобы деньги были переведены не на счет требуемого получателя, а на счет злоумышленника. Так, например, в этом году была опубликована информация об успешной атаке на SWIFT, в результате которой злоумышленникам удалось похитить средства национального банка Бангладеш на десятки миллионов долларов. К сожалению, успешные атаки на АРМ КБР (автоматизированное рабочее место клиента Банка России) также не являются редкостью. Именно поэтому Банк России выпустил целый ряд документов, направленных на повышение уровня защиты кредитно-финансовых организаций от такого рода атак, в частности, Положение Банка России от 24 августа 2016 г. № 552-П «О требованиях к защите информации в платежной системе Банка России». Для защиты данных платежных карт клиентов банков активно используется международный стандарт PCI DSS, который является обязательным для банков, обрабатываю-

щих карточные данные, в том числе, имеющие собственные процессинговые центры.

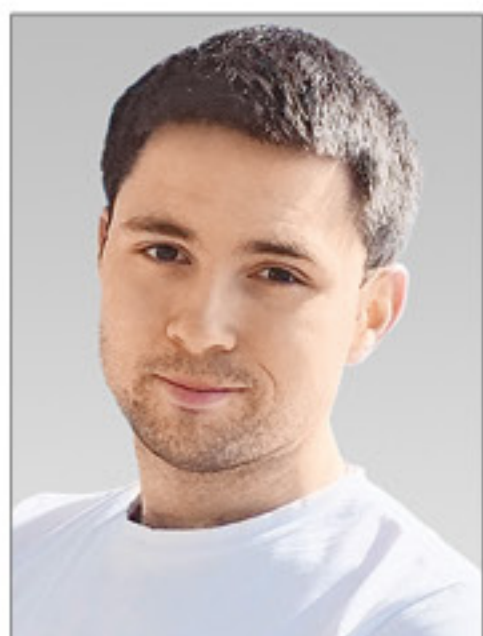
АТАКИ НА БАНКОМАТНЫЕ СЕТИ

Еще одним вектором для потенциальных атак злоумышленников являются банкоматные сети. По сути, современный банкомат представляет собой тот же компьютер, подключенный к сети банка. При этом в качестве операционной системы чаще всего используется общесистемное ПО Microsoft Windows, в том числе Windows XP, а также, в силу аппаратных и/или программных ограничений, не используются даже простейшие средства защиты информации — антивирусы и средства мониторинга. Злоумышленник может атаковать банкомат посредством как локального, так и удаленного доступа, используя уязвимости в общесистемном и прикладном ПО банкомата. Для защиты от такого рода угроз необходимо использовать специализированные средства защиты, предназначенные для защиты самого банкомата, а также каналов взаимодействия между ним и корпоративной сетью банка.

* * *

В настоящее время существует достаточно большое количество векторов, по которым злоумышленник может атаковать банк. Для эффективной защиты от такого рода угроз необходимо использовать комплексный подход, предусматривающий применение как организационных, так и технических мер защиты. Именно такой подход предусмотрен в положениях нового ГОСТа по защите информации, разработанного Центральным банком России, принятие которого ожидается в текущем году.

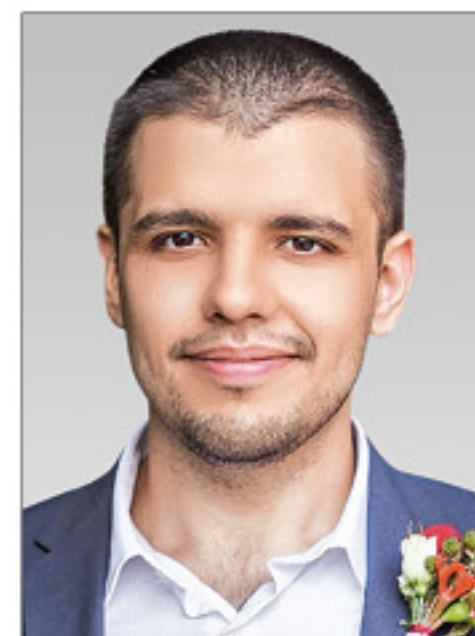
НЕИЗВЛЕКАЕМЫЕ КЛЮЧИ В ОБЛАКЕ — ПУТЬ ЧЕРЕЗ КРИПТОПРОВАЙДЕР



Станислав СМЫШЛЯЕВ
начальник отдела защиты информации
компании КристоПро, к.ф.-м.н.



Павел СМЕРНОВ
заместитель начальника отдела разработки
компании КристоПро, к.т.н.



Сергей АГАФЬИН
ведущий инженер-программист компании
КристоПро

Одной из важнейших задач прикладной криптографии, бесспорно, является задача хранения секретных ключей. Для этого применяется множество средств, которые имеют как достоинства, так и недостатки. В рамках данной статьи авторы на основе своего опыта в области разработки криптографиче-

ских систем опишут существующие подходы к решению данной задачи и проведут их краткое сравнение.

ПРОГРАММНЫЕ И ПРОГРАММНО- АППАРАТНЫЕ ХРАНИЛИЩА

Исторически первым распространенным методом хранения ключей

в компьютерных системах прикладной криптографии стало использование обычной файловой системы. Этот подход имел много достоинств. Прежде всего, чтобы поместить ключевой контейнер (ключевую пару с дополнительной информацией) в файловую систему, не нужны дополнительные устройства. Разграничение доступа

к контейнерам осуществляется исключительно штатными механизмами операционной системы. Модификацией данного подхода является использование съемных дисковых накопителей: раньше — дискет, сейчас — USB-флешек и смартфонов.

Основными криптографическими системами, использующими данный подход с самого начала своего существования, являются криптографические провайдеры — модули, реализующие интерфейс Microsoft CryptoAPI. Данный интерфейс оказался настолько удобным для использования в прикладных приложениях Windows, что до сих пор значительное количество приложений полагаются именно на него, а сам интерфейс даже портирован компанией КриптоПро на Unix-платформы. В России первой системой, которая его предоставляла, стал криптографический провайдер «КриптоПро CSP», появившийся в 2001 году.

Со временем стало ясно, что хранение ключей в постоянной памяти компьютера или на дискете хоть и является удобным подходом, но имеет ряд недостатков с точки зрения устойчивости к моделям нарушителя, предполагающим возможность кратковременной компрометации системы. Таким образом, следующим шагом стало использование в качестве хранилища ключей пассивных смарт-карт и USB-токенов. В отличие от дискет (напомним, что речь всё еще идет о начале 2000-х), смарт-карты предоставили возможность хранения ключевого контейнера в защищенной памяти, доступ к которой разграничивался микроконтроллером самого устройства. Тем не менее, данные устройства всё еще не умели самостоятельно выполнять криптографические преобразования, так что основным путем их использования стало подключение к программным криптопровайдерам, которые использовали токены только для одной задачи: считать ключ из их памяти в оперативную память компьютера.

В связи с отсутствием альтернатив в течение долгого времени использование программных провайдеров в связке с пассивными токенами было де-факто стандартом в нашей стране. Тем не менее, прогресс не стоял на ме-

ПОДХОД DSS ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО ВСЕ КЛЮЧИ ПОЛЬЗОВАТЕЛЕЙ ХРАНЯТСЯ В ЗАЩИЩЕННОМ ХРАНИЛИЩЕ HSM, А ДОСТУП К КЛЮЧАМ ОСУЩЕСТВЛЯЕТСЯ ЧЕРЕЗ WEB-ИНТЕРФЕЙС

сте, и к концу 2000-х годов появился новый класс устройств: токены с неизвлекаемыми закрытыми ключами (активные токены, функциональные ключевые носители). В отличие от пассивных устройств, которые только хранят закрытые ключи, данные токены уже умеют самостоятельно формировать и проверять электронную подпись, шифровать и хэшировать небольшие сообщения.

Несмотря на то, что данные устройства могут встраиваться в автоматизированные системы через независимые библиотеки, бесшовный переход на их использование возможен только через соответствующие криптопровайдеры. Одним из них стал, например, «КриптоПро Рутокен ФКН», который в связке с «Актив Рутокен ЭЦП» мог легко заменить связку «КриптоПро CSP» с «Актив Рутокен Лайт», если пользователи хотели начать использовать неизвлекаемые ключи.

Однако, несмотря на большое количество преимуществ, которыми на первый взгляд обладает токен с неизвлекаемыми ключами, у него, помимо высокой цены и низкой производительности, есть еще ряд недостатков по сравнению с другими методами хранения ключей. Прежде всего, самое очевидное — поломка или потеря токена автоматически приводят к нарушению рабочих процессов. Если извлекаемые ключи могут быть заархивированы в некоем защищенном хранилище компании, то неизвлекаемые ключи всегда существуют ровно в одном экземпляре.

С повышением уровня безопасности при использовании данных токенов также всё не совсем просто: если раньше нарушитель мог «встать посередине» между токеном и криптопровайдером и украсть ключ, то теперь

его задачей стала кража ПИН-кода, который в большинстве случаев представляется либо в открытом виде, либо с использованием тривиального алгоритма, который легко может быть восстановлен опытным злоумышленником. Конечно, есть защищенные протоколы аутентификации на токенах, например, протокол SESPake (Рекомендации по стандартизации Р 50.1.115–2016), но они начали распространяться только недавно, а реализующие их носители еще не доступны для продажи.

УДАЛЕННЫЕ И ОБЛАЧНЫЕ ХРАНИЛИЩА

Еще одним распространенным видом ключевых хранилищ являются HSM (Hardware Security Module) — защищенные программно-аппаратные комплексы. По сути они представляют собой полноценные защищенные ЭВМ (уровень безопасности вплоть до KB2), доступ к которым осуществляется по защищенным сетевым протоколам. Несмотря на то, что они обеспечивают практически предельную степень безопасности ключей, их удобство использования оставляет желать лучшего: размещение HSM возможно только в защищенных помещениях внутри компании, а для доступа используются специальные утилиты.

Развитием идеи HSM стало появление удобных удаленных сервисов электронной подписи (Digital Signature Server — DSS). Подход DSS заключается в том, что все ключи пользователей находятся в безопасном хранилище HSM, который может принадлежать как компании-работодателю, так и независимой доверенной организации, например, удостоверяющему центру, а доступ к ключам осуществляется по защищенному каналу через

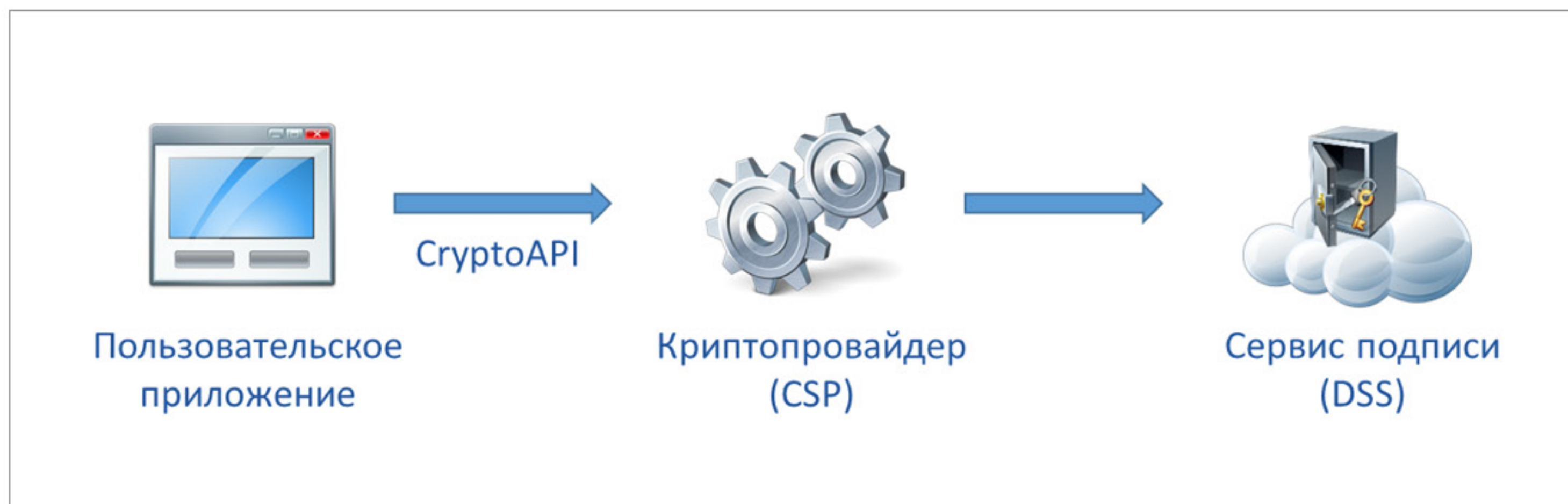


Рисунок 1. Принципиальная схема системы использования «облачного токена»

Web-интерфейс. Одним из таких комплексов является, например, «Крипто-Про DSS», на который было получено положительное заключение на соответствие уровню КСЗ.

Данный подход позволил расширить использование HSM с одной небольшой выделенной локальной сети до крупной сети компании и даже сети Интернет. При использовании DSS пользователи могут подписывать документы с любой точки земного шара, будучи полностью уверенными, что их ключи находятся в безопасности, а доступ к ним может быть осуществлен любым удобным защищенным способом. Переход на удаленное использование ключей также позволяет перевести систему из разряда дорогих программно-аппаратных комплексов в дешевую массовую услугу.

Разумеется, у DSS остается существенный недостаток — сложность встраивания в существующие системы. Web-интерфейс — это хорошо, но что делать компаниям, которые хотят повысить безопасность своей автоматизированной системы без серьезных затрат в разработку нового прикладного ПО взамен существующего, которое уже много лет использует CryptoAPI?

Как нам видится, естественным путем решения данной проблемы является встраивание поддержки DSS в существующие криптопровайдеры. Если подключение такого «облачного токена» будет не сложнее подключения физического токена, то единственным, что нужно будет сделать пользователю, чтобы начать работать с данными защищенными ключами

в рамках своей системы, — обновить криптопровайдер. Принципиальная схема подобной системы представлена на рисунке 1.

Этот подход обладает всеми преимуществами остальных подходов и практически лишен недостатков. Единственное, пожалуй, чего он не в состоянии обеспечить — спокойствие людей, которые в силу каких-либо причин предпочитают не передавать свои данные на удаленный сервис. Однако, как показывает опыт других сфер информационных технологий, адекватных альтернатив переходу к облачным сервисам с каждым днем остаётся всё меньше.

Кратко содержание нашей статьи можно представить в виде следующей сравнительной таблицы:

Способ хранения	Высокая скорость	Низкая цена	Использование пользовательского ключа на удаленном рабочем месте	Встраивание в существующие системы через CryptoAPI	Защита ключа от кражи или утери	Защищенный канал доступа к ключам
CSP + HDD	+	+	-	+	+	+
CSP и пассивный токен	+	-	+	+	-	-
Активный токен	-	-	+	-	-	-
CSP + активный токен	-	-	+	+	-	-
HSM	+	-	-	+	+	+
HSM + DSS	+	+	+	-	+	+
«Облачный токен»: HSM + DSS + CSP	+	+	+	+	+	+

KASPERSKY®



Kaspersky® DDoS Prevention

Противодействие
DDoS-атакам
для непрерывной
работы вашего бизнеса

- Гибкий подход к построению системы защиты
- Уникальные технологии фильтрации трафика
- Обнаружение атак на ранних стадиях
- Собственная сеть центров очистки трафика
- Детальный анализ и подробные отчеты
- Круглосуточная экспертная поддержка

kaspersky.ru/ddos-prevention

© АО «Лаборатория Касперского», 2016.
Зарегистрированные товарные знаки и знаки обслуживания
являются собственностью их правообладателей

ARinteg®

+7 (495) 221 21 41 Москва • +7 (343) 247 83 68 Екатеринбург • +7 (812) 407 34 71 Санкт-Петербург

ARinteg (зарегистрированная торговая марка ООО «АРинтег») -
Platinum Partner «Лаборатории Касперского».
Компания ARinteg предоставляет полный комплекс услуг в области защиты информационных ресурсов.

www.ARinteg.ru





**Алексей
ЛУКАЦКИЙ**
эксперт
информационной
безопасности

К СОСУ ГОТОВ? ПОДУМАЙ!

ОБМЕН ОПЫТОМ СТРОИТЕЛЬСТВА
ЦЕНТРОВ МОНИТОРИНГА ИБ
НА SOC FORUM В КАЗАХСТАНЕ

В конце апреля в Астане (Казахстан) состоялся SOC Forum — мероприятие, уже дважды прошедшее в Москве, и вот вырвавшееся на просторы СНГ. Я не раз высказывался о данном мероприятии в позитивных тонах, считая, что за фокусными мероприятиями будущее, и Медиа Группа «Авангард» смогла оседлать одну из самых живых и «горячих» тем, о которой думают многие специалисты по кибербезопасности в России и других странах. На астанинском форуме мне довелось модерировать пленарную секцию

и выступать на секции «Опыт построения SOC». Поэтому мне бы хотелось поделиться своим взглядом на происходящее в Казахстане. Тем более, что мне есть с чем сравнивать — Cisco имеет свой собственный внутренний SOC (о нем я и рассказывал), предлагает аутсорсинговый SOC для своих клиентов, а также помогает им строить свои центры мониторинга, если по каким-то причинам они не готовы обращаться к аутсорсингу данных услуг. Именно это дает мне основания для оценки множества докладов и того, насколько они соот-

носятся с лучшими мировыми практиками (в 2015–2016-м годах у меня было два «турне» по SO Сам в разных странах мира, где я мог почерпнуть много интересного).

МОЖЕТ ЛИ NOC ПРЕВРАТИТЬСЯ В SOC?

В пленарной секции, которую мне довелось модерировать, прозвучала фраза: «У нас уже есть NOC (Network Operations Center — авт.), поэтому мы можем легко на его базе сформировать SOC». Это классическое заблуждение, которое часто можно слышать от опе-



раторов связи, давно имеющих у себя центры управления сетью и которые решили выйти на новые для себя рынки. И хотя в обоих центрах занимаются мониторингом, это совершенно разные задачи. Да, эти команды могут и должны работать вместе, но все-таки они занимаются разными вещами: у них разные приоритеты. Задача NOC обеспечить непрерывное функционирование сетевой инфраструктуры и быстро восстанавливать сеть в исходное состояние. Задача SOC — реагировать на инциденты безопасности.

Согласно 5 моделям функционирования SOC по версии Gartner, объединение SOC и NOC все-таки возможно, но только в небольших и низкорискованных организациях, где функции управления сетью и ИБ уже реализуются одними и теми же людьми. По сути речь идет о классическом малом и, иногда, среднем бизнесе, где функции ИБ возложены на ИТ-департамент. В таких ситуациях «не до жиру». Но у данного подхода есть и проблемы. У SOC/NOС разные политики, процессы, процедуры и зачастую инструменты (хотя сбор событий, управление событиями и инцидентами, оркестрация, анализ Netflow и другие могут реализовываться одним и тем же ПО). Будут ли сотрудники NOC концентрироваться на угрозах? А на проблемах, выходящих за рамки текущей сетевой инфраструктуры? А будут ли они заниматься Threat Hunting и Threat Intelligence? Все это маловероятно, а значит идея возложить на NOC еще и функции SOC обречена на неудачу.

ОТ SIEM К ТРИАДЕ SIEM+NTA+EDR

Еще одна классическая ошибка, которая явно и неявно звучала на SOC Forum, — построение SOC вокруг какого-либо SIEM. Исторически в России самым популярным SIEM-решением считается ArcSight ESM. Его используют и заказчики и поставщики аутсорсинговых услуг (например, он применяется компаниями Solar Security и ISSP, выступавшими на форуме). Завбавно, на прошедшей в июне в США конференции Gartner по информационной безопасности и управлению рисками по опросу среди потребите-



лей призовая тройка была распределена между совсем иными компаниями — LogRhythm, LogPoint и Splunk. Кроме последнего имени, остальные два практически не известны на территории постсоветского пространства. Но дело даже не в том, какой продукт используется в качестве SIEM. Фокус на SIEM, как ядре SOC, — это всего лишь первый уровень зрелости SOC по версии Gartner. В выступлении компании Palo Alto прозвучал тезис, что «миссия SOC — отслеживать, обнаруживать и эскалировать важные события ИБ для гарантии конфиденциальности, целостности и доступности во всей компании». В такой постановке задачи, действительно, средство управления событиями ИБ становится ядром SOC. Но центр мониторинга ИБ не занимается событиями ИБ. Его основное предназначение в ином — обеспечение централизованного и консолидированного предотвращения, обнаружения и реагирования на инциденты ИБ.

В Cisco наш SOC построен вокруг трех основных элементов, занимающихся мониторингом логов, сетевых потоков, конечных устройств и поведения, — SIEM (на базе Splunk), NTA или Network Traffic Analysis (на базе Cisco Stealthwatch), EDR или Endpoint Detection & Response (на базе Cisco AMP for Endpoints). И если до 2010-го года львиная доля инцидентов в Cisco обнаруживалась за счет анализа журналов регистрации с помощью SIEM, то се-

годня на SIEM у нас приходится около 20% всех обнаруженных инцидентов ИБ. Еще 20% мы ловим за счет анализа Netflow с помощью технологий NTA (раньше их еще называли NBAD, Network-based Anomaly Detection или Network Behavior Anomaly Detection). Третьи 20% обнаруживаются с помощью анализа поведения и, наконец, оставшиеся 40% являются заслугой сервисов Threat Intelligence.

Компания Gartner, активно исследующая тему SOC, также считает, что современный SOC в своем ядре использует тройку технологий — SIEM, NTA (иногда еще добавляя NTF, Network Traffic Forensics) и EDR, позволяющих собирать события безопасности из сетевого трафика, с конечных устройств и с журналов регистрации. В столице Казахстана про решения EDR и NTA практически никто не упомянул, что отражает ситуацию, когда отечественные SOCи находятся на самом начальном этапе своего развития. Исключением стало выступление компании МТС, рассказавшей о своем опыте построения SOC — анализом Netflow они занялись еще в начале этого десятилетия. Если подождать пару-тройку лет, то многие упомянутые технологии (исключая EDR) войдут в те же SIEMы. Но тут стоит добавить, что до России с ее курсом на изоляционизм и импортозапрещение (а большинство технологий к нам все-таки приходит оттуда) этот прогноз может и не сбыться вовсе.

Компании Positive Technologies и Solar Security, предоставляющие внешние услуги SOC и для SOC, много говорили о необходимости инвентаризации ИТ-активов. Интересно, что опрос клиентов Gartner показал, что на Западе эта технология как раз не входит в число обязательных для SOC, мотивируя это не самым удачным опытом внедрения такого рода продуктов (сложно и неочевидная эффективность). И действительно, в условиях динамично изменяющейся ИТ-инфраструктуры современного предприятия (и чем оно больше, тем динамичнее картина) поддерживать в актуальном состоянии карту сетевых ресурсов превращается в очень неочевидную задачу. Даже при использовании специализированного инструментария (Positive Technologies использует собственное решение на базе MaxPatrol, Solar Security использует Skybox Security, Cisco применяет RedSeal).

Последний, пятый уровень зрелости SOC по версии Gartner подразумевает под собой применение не только SIEM, NTA/NFT, EDR, но и UEBA (User Entity Behavior Analytics), средств оркестрации и даже обманных решений. С необходимостью последней технологии для SOC я бы поспорил (хотя в мире за последнее время появилось около десятка стартапов по теме обмана в ИБ), а вот остальные упомянутые решения очень важны. Про оркестра-



Игорь Ляпунов, генеральный директор Solar Security

цию на SOC Forum KZ говорила компания R-Vision, но только применительно к автоматизации управления инцидентами. Остальные задачи SOC, которые можно и нужно автоматизировать, рассмотрены не были (возможно, по причине нехватки времени).

THREAT INTELLIGENCE И THREAT HUNTING

Одной из обязательных задач современного SOC является Threat Intelligence и Threat Hunting. Первое — это базирующееся на доказательствах знание (включая процесс его получения) о текущих или предполагаемых угро-

зах и нарушителях, обеспечивающее понимание методов, используемых злоумышленниками для нанесения ущерба, и способов противодействия им, где в качестве доказательств могут быть использованы индикаторы компрометации, контекст, предположения и т.п. Второе — это поиск следов нарушителей, которые остаются незамеченными технологиями предотвращения и обнаружения угроз. В качестве исходных данных для Threat Hunting могут использоваться и данные Threat Intelligence. Тема Threat Hunting была обойдена вниманием выступающих, что было обусловлено нехваткой владения темой и неготовностью к ней многих присутствующих, пока только размышляющих о том, нужен им SOC или нет, а не о том, как выявлять следы нарушителей в множестве внутренних и внешних источников информации.

Про Threat Intelligence говорили многие участники SOC Forum, которые используют источники Open Source, репутационные базы вендоров, а также платные подписи, среди которых упоминались российские «Лаборатория Касперского» и Group-IB, а также иностранные Cisco Threat Grid, Payload Security, VirusTotal, Cisco OpenDNS и другие. Для консолидации получаемых извне или созданных самостоятельно индикаторов компрометации применяются различные платформы — от open source MISF



Алексей Качалин, заместитель директора по развитию бизнеса компании Positive Technologies

(используется ISSP) или CRiTs (используется Cisco) до коммерческих или вообще самописных. Компания МТС пока только планирует внедрять Threat Intelligence в своем SOC, в том числе и в виде взаимодействия с национальной системой обнаружения, предотвращения и ликвидации последствий компьютерных атак ГосСОПКА. В Cisco пошли еще дальше и разработали собственную платформу Cisco TIP (Threat Intelligence Platform), которая предназначена для решения множества внутренних задач службы ИБ и в т.ч. SOC.

SOC — это люди, процессы и технологии

Взяв за основу классическую триаду «люди, процессы и технологии», почти все выступающие отмечали, что SOC — это прежде всего люди, и люди квалифицированные. Как сказал недель позже на мероприятии Gartner Антон Чувакин: «лучше плохой SIEM с хорошей командой, чем офигенный SIEM с плохой командой». И вот в этом вопросе большинство заказчиков столкнется с классической проблемой — людей нет.

Представители Solar Security рекомендуют начинать с 2–3 человек первой линии, 1 аналитика и 1 руководителя (то есть 4–5 человек). Именно с таких цифр начинался JSOC, работающий в режиме 5x8. Сейчас, при режиме работы 24x7, в JSOC трудится уже 54 человека. По оценкам Cisco, минимальное количество специалистов, которые могли бы обеспечивать круглосуточный режим работы SOC, составляет около 20 человек. Например, в Microsoft Cyber Defense Operations Center работает 50 человек, в Cisco CSIRT — 103, в Ростелекоме — 25 и идет еще набор, в Solar JSOC — около 60 и также идет набор, Сбербанк озвучивает цифру в 400 человек, у Лаборатории Касперского — 14 человек. При этом у тех же Microsoft, Cisco, ЛК есть отдельные подразделения Threat Intelligence, которые в озвученные выше цифры не включены (например, Cisco Talos, занимающийся анализом угроз и создающий сигнатуры, описывающие репутации узлов и т.п., насчитывает 250 человек). Готовы ли вы к та-

ПОЧТИ ВСЕ ВЫСТУПАЮЩИЕ ОТМЕЧАЛИ, ЧТО SOC — ЭТО ПРЕЖДЕ ВСЕГО ЛЮДИ, И ЛЮДИ КВАЛИФИЦИРОВАННЫЕ

кому расширению штата или все-таки стоит смотреть на внешние центры мониторинга?

Тема процессов была практически обойдена вниманием на SOC Forum, а вот про технологии говорили много. Оно и понятно — многие выступающие представляли «продуктовые» компании, желающие продать свои решения. И если кто-то пытался увязать свои решения с SOC, то некоторые производители даже не удосуживались сделать хотя бы такую небольшую работу и никак не объясняли место своих NGFW, сканеров кода и других решений в деятельности SOC.

Интересная ситуация возникла с анализом защищенности. Некоторые поставщики услуг упоминали про необходимость сканирования уязвимостей, как части SOC. При этом на прошедшем в Москве несколькими днями позже закрытом мероприятии Gartner ее представитель Антон Чувакин рассказывал, что на Западе в последнее время многие компании не то, чтобы совсем отказываются от устранения уязвимостей и выстраивания патч-менеджмента, но и не ставят эти процессы во главу угла. При среднем времени устранения уязвимостей в 30 дней и более (по исследованиям Cisco, устранение заказчиками уязвимостей в сетевом оборудовании или серверном ПО может длиться до пяти лет) говорить об оперативности не приходится. Отсюда и исключение этого процесса из списка ключевых для SOC. Нередко клиенты мирятся с наличием дыры и поэтому не имеют выстроенного процесса устранения уязвимостей. Тем интереснее сравнивать этот взгляд с российским, где только совсем недавно регуляторы обратили внимание на анализ защищенности и сделали его обязательной частью любой системы защиты (по требованиям ФСТЭК, ЦБ, ФСБ), а также частью обязательных требований при получении лицензии ФСТЭК на деятельность SOC.

В КАЧЕСТВЕ ЗАКЛЮЧЕНИЯ

На форуме было представлено несколько аутсорсинговых SOC, и у многих заказчиков звучал классический вопрос: «Что лучше — свой SOC или аутсорсинговый?» Представители аутсорсинговых центров, разумеется, утверждали, что отдать на аутсорсинг лучше всего. Представители многих заказчиков наоборот считали, что «своя рубашка ближе к телу» и надо постепенно наращивать свои компетенции. Например, у МТС первоначально SOC работал в режиме 8x5 и только сейчас перешел на режим 24x7. Истина, как известно, где-то посередине — часть функций можно попробовать (при наличии людей) реализовать самостоятельно, а часть (те же Threat Intelligence, расследование инцидентов, сканирование защищенности и другие) отдать во внешние руки.

* * *

Но гораздо интереснее вопроса, должен быть SOC внешним или внутренним, является другой вопрос, которого на форуме почти не коснулись. Кому нужен SOC (именно кому, а не зачем)? Дело в том, что внедрение собственного SOC или переход на аутсорсинговую модель требуют определенного, и немалого, уровня зрелости. Сегодня только ленивый не задумывается о том, чтобы назвать купленный ArcSight или скачанный OSSIM SOCом, но... повторюсь, SOC — это люди, процессы и только потом технологии. Если в компании нет процессов (или они приобретены у крупного консалтера без понимания их сути) — к SOCу компания не готова. Если в компании есть только межсетевой экран на периметре и антивирус на персоналках — к SOCу компания не готова. Нужно дозреть, и только наткнувшись на невозможность решить возникающие проблемы текущими средствами, можно задумываться о переходе на новый уровень под названием Security Operations Center.



УРОКИ ЛЕТНЕЙ СЕССИИ

В МОСКВЕ СОСТОЯЛАСЬ ЛЕТНЯЯ СЕССИЯ
УРАЛЬСКОГО ФОРУМА – КОНФЕРЕНЦИЯ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВОЙ
СФЕРЫ. PCI DSS RUSSIA 2017»

Ежегодно в феврале на ключевом мероприятии отрасли ИБ Уральском форуме «Информационная безопасность финансовой сферы» при участии всех регуляторов и представителей отрасли обсуждаются самые важные темы и проблемы противодействия киберпреступности и защиты российских банков от компьютерных угроз. Но из-за высокой загруженности деловой программы за её рамками остается часть вопросов, требующих своевременного обсуждения и решения. Именно эти, наиболее острые и насущные, вопросы традиционно выносятся на Летнюю сессию Уральского форума. В этом году конференция «Информационная безопасность финансовой сферы. PCI DSS Russia 2017» состоялось 31 мая в Москве, в конференц-зале гостиницы «Золотое кольцо». В ней приняли участие более 150 представителей регуляторов, руководителей и ведущих сотрудников российских банков, телеком-компа-

ний, разработчиков и поставщиков решений в области ИБ, аудиторов безопасности информационных систем и других специалистов отрасли.

Среди основных тем, обсуждавшихся на Летней сессии, — применение актуальных версий стандартов ИБ международных платёжных систем, взаимодействие организаций финансовой сферы в деле противодействия DDoS-атакам, а также вопросы идентификации и аутентификации клиентов кредитно-финансовых организаций в контексте использования ЕСИА.

«МИР», ТЕСТ, СТАНДАРТ!

В сессии «Информационная безопасность платежных систем», посвященной в основном стандарту PCI DSS, Максим Фомичев, начальник отдела сопровождения ИБ НСПК, рассказал, что в соответствии с Правилами платежной системы «Мир» основными нормативными документами, регламентирующими выполнение требований по обеспечению информационной безопасности,

для всех субъектов платежной системы «Мир» являются Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» и международный стандарт безопасности данных индустрии платежных карт PCI DSS (Payment Card Industry Data Security Standard).

Проведение тестирования автоматизированных систем на проникновение является обязательным, в том числе и в соответствии с требованиями PCI DSS, поэтому в рамках этой же сессии рассматривались основные принципы и методики такого тестирования. Эта тема привлекла всеобщее внимание, поскольку на Уральском форуме в Магнитогорске ее обсуждение хоть и было бурным, но затронуло только частные аспекты. Обобщающий до-



Алексей Плешков, независимый эксперт



Иван Янсон, Сбербанк России



Дмитрий Федоров, Банк ВТБ

клад в исполнении Алексея Плешкова, позиционировавшего себя как независимого эксперта, прозвучал именно на Летней сессии.

Обсуждалась и мотивация для выполнения требований стандартов информационной безопасности. Итоги дискуссии вкратце таковы. Целью должно быть обеспечение защищенности ресурсов организации, а не формальное исполнение требований под угрозой санкций. Если организация уделяет адекватное внимание информационной безопасности, то основная часть требований стандартов будет ею выполнена автоматически. Стандарт — это памятка, по которой специалисты проверяют, все ли моменты, связанные с обеспечением безопасности, учтены в процессе работы.

ИДЕИ ВТБ ОБСУДИЛИ С ЭНТУЗИАЗМОМ

На следующей сессии, посвященной противодействию DDoS-атакам, были рассмотрены основные тенденции в данной области. Докладчики приводили статистику и делились опытом. Например, самая мощная атака в мире достигала 1.1 Тбит/с, в России (по данным Ростелеком) — 214 Гбит/с. Рассматривались также плюсы и минусы двух подходов противодействия DDoS: аутсорсинга и построения своей защиты.

Кульминацией всей конференции — с активным противостоянием сторон и бурной дискуссией, охватившей весь зал, — стала сессия, посвященная использованию новых решений в целях идентификации и аутентификации пользователей финансовых услуг. Рассматривалось несколько смежных вопросов.

Иван Янсон, бизнес-партнер по информационной безопасности ПАО «Сбербанк России», рассказал

о целях и ходе эксперимента по удаленной регистрации бизнеса. В свою очередь Алексей Александров, технический директор 1С-СП, сообщил о новой отечественной разработке, поддерживаемой Банком ВТБ, по реализации усиленной электронной подписи на сим-картах телефонов. Тут возникло много вопросов о перспективах сертификации и зависимости от безопасности операционных систем, но в целом оба доклада были восприняты аудиторией положительно.

Дмитрий Федоров, представитель Банка ВТБ, рассказал о новых идеях использования Единой системы идентификации и аутентификации и Национальной Биометрической платформы для предоставления финансовых услуг населению. Указанный подход должен решить одну из важнейших банковских проблем — сделать доступными банковские услуги для всех граждан России независимо от наличия поблизости банковских офисов. Сам подход был принят с большим энтузиазмом, что повлекло за собой трудноостановимое обсуждение множества частных специальных вопросов.

БИОМЕТРИЮ ПОСТАВИЛИ НА МЕСТО

Завершилась Летняя сессия Уральского форума большой дискуссией, которую вел руководитель подразделения информационной безопасности Банка ВТБ Сергей Пазизин. В ходе дискуссии, местами переходившей в яростные дебаты, обсуждались пути решения проблем ИБ в части борьбы с DDoS-атаками, а также вопросы надежности современных методов идентификации и аутентификации.

Споры оказались весьма плодотворными. Например, обсуждение обяза-

тельности услуги по очистке трафика для мобильных операторов привело к выводу, что все должен решить рынок — спрос своим давлением заставит операторов обеспечивать клиентов такими услугами. С другой стороны, нет необходимости принудительно удалять с рынка операторов, которые не обеспечивают защиту клиентов от DDoS-атак, так как эта угроза не для всех актуальна. По крайней мере, не более актуальна, чем для самих операторов, поскольку такие атаки на их клиентов не позволят нормально функционировать каналам связи самих операторов.

В части нормативной базы обсудили и констатировали необходимость доработки Уголовного кодекса. Потребность в строгом, юридически обоснованном наказании за организацию DDoS-атак давно уже видится в фельетонной плоскости — кого все-таки защищает Закон: мирных граждан или злоумышленников?

По поводу применения биометрических методов участники дискуссии отметили их полезность как дополнительного фактора при аутентификации пользователя, что может снизить количество случаев мошенничества в системах дистанционного банковского обслуживания. Также биометрия будет эффективна, если ее использовать при открытии пользовательских счетов, но при условии разработки достаточно сложной и трудоемкой процедуры первичного подтверждения личности при приеме клиента на обслуживание. Вместе с тем, основным способом аутентификации пользователей при проведении платежей — и на этом участники дискуссии решили остановиться — в ближайшее время останутся такие проверенные методы, как электронная подпись и разовые пароли.

БЕЛАРУСЬ — РОССИЯ: БЕЗОПАСНОСТЬ — ЗАДАЧА ОБЩАЯ

С 16 по 19 мая 2017 г. в Полоцке состоялась XXII научно-практическая конференция «Комплексная защита информации» как мероприятие Союзного государства. Организаторы конференции: Парламентское собрание Союза Беларуси и России, Постоянный комитет Союзного государства, аппарат Совета безопасности Российской Федерации. Организационную поддержку мероприятию оказали: Медиа Группа «Авангард» и Государственное предприятие «Научно-исследовательский институт технической защиты информации».

На конференции были рассмотрены актуальные вопросы безопасности информационного пространства государств-участников Союзного государства. В работе научного форума приняли участие свыше 100 представителей Беларуси и России. Среди них — 2 академика, 3 член-корреспондента (различных академий), 15 докторов наук, 18 кандидатов наук, в том числе 9 профессоров, более десяти доцентов и старших научных сотрудников, а также специалисты-практики, руководители государственных и коммерческих организаций, специализирующихся на вопросах выработки практических ре-

шений в сфере информационной безопасности.

На пленарных и секционных заседаниях было заслушано и обсуждено более 75 докладов ученых, специалистов, представителей государственных органов России, Беларуси и Союзного государства по широкому спектру научных и практических направлений в области информационной безопасности, в том числе 12 докладов в рамках «Школы молодых ученых». Осуществлялся обмен опытом по вопросам использования защищенных информационных технологий в различных сферах жизни общества и государства.





ИЗ РЕЗОЛЮЦИИ XXII НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»

На конференции были обсуждены следующие темы:

- ◆ технические средства защиты информации;
- ◆ средства криптографической защиты информации;
- ◆ проблемы противодействия киберпреступности;
- ◆ проблемы подготовки кадров в области информационной безопасности;
- ◆ формирование трансграничного пространства доверия Союзного государства;
- ◆ перспективные направления информационной безопасности;
- ◆ проблемы стандартизации в области информационной безопасности.

Конференция отмечает актуальность:

- ◆ решения проблемы обеспечения защищенности персональных данных с использованием перспективных высоких технологий;
- ◆ разработки системы сертификации специалистов как объективной основы подбора и расстановки кадров, включая разработку методик оценки лояльности и профессиональных компетенций кадров в отрасли информационной безопасности;
- ◆ дальнейшего развития совместных работ научных коллективов России и Беларуси по развитию современных информационных технологий в интересах создания новых защищенных импортозамещающих платформ;
- ◆ приоритет использования средств защиты информации, разработанных в Союзном государстве России и Беларуси;
- ◆ развития профильного образования и популяризации профессий в области информационной безопасности;
- ◆ создания и развития трансграничного пространства доверия Беларуси и России.

Отдельно отмечается вклад молодых ученых и специалистов в научную деятельность в сфере защиты общих информационных ресурсов Союзного государства.

Положительной оценки заслуживает практика проведения в рамках Конференции «Школы молодых ученых» как одной из форм продвижения и поддержки перспективных специалистов, укрепления их интереса к научной работе в области информационной безопасности.

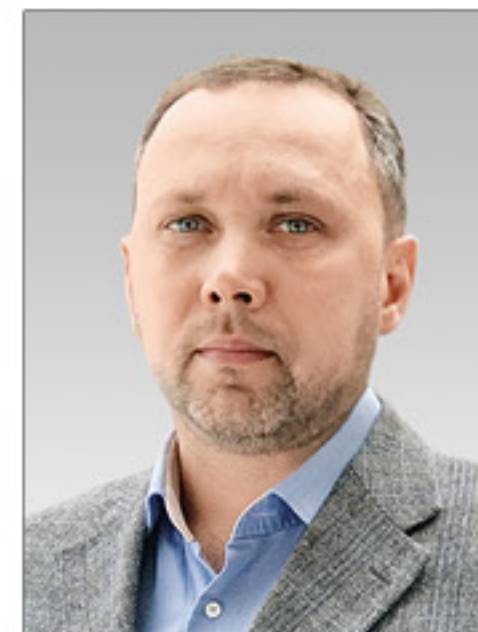
Конференция считает необходимым организовать публикацию материалов конференции в научном журнале с целью привлечения широкого внимания к затронутым проблемным вопросам.

Участники конференции считают, что состоялся плодотворный обмен опытом в области исследований, разработки и внедрения теоретических, методологических, нормативных, организационно-технических, правовых и гуманитарных вопросов обеспечения информационной безопасности.

Участники конференции постановили:

- ◆ Одобрить работу XXII научно-практической конференции.
- ◆ Поддержать предложение по рассмотрению и одобрению Концепции программы «Совершенствование системы защиты информационных ресурсов Союзного государства и государств-участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» в максимально сжатые сроки.
- ◆ Провести XXIII научно-практическую конференцию «Комплексная защита информации» в 2018 г. в Российской Федерации. Просить Постоянный Комитет Союзного государства сформировать рабочую группу для подготовки и осуществления организационных мероприятий.
- ◆ Проинформировать руководство Постоянного Комитета Союзного государства и Парламентского Собрания Союза Беларуси и России об итогах XXII научно-практической конференции «Комплексная защита информации» и ее предложениях.
- ◆ Организовать публикацию материалов конференции в третьем квартале 2017 года.

НОВЫЙ ИСТОЧНИК ЭНЕРГИИ



Артем ЗУБКОВ
директор Фонда
содействия развитию
безопасных
информационных
технологий (ФСРБИТ)

На научно-практической конференции «Комплексная защита информации» состоялось представление нового общественного фонда — Фонда содействия развитию безопасных информационных технологий. Возникновение новой общественной структуры — всегда событие, тем более, в такой достаточно узкой и закрытой сфере, как информационная безопасность. Вдвойне неожиданно и приятно, когда оказывается, что созданная всего полгода назад организация уже активно, продуктивно работает. На научно-практической конференции «Комплексная защита информации» в Полоцке в рамках доклада А. Н. Зубкова прозвучала информация о новом общественном Фонде содействию безопасных информационных технологий. Публикуем доклад в сокращенном виде, ту его часть, где речь идет непосредственно о Фонде.

ПРЕДПОСЫЛКИ ВОЗНИКНОВЕНИЯ ФОНДА

Мы с вами работаем в сфере информационной безопасности — на границе хаоса и порядка, и одними из первых ощущаем на себе, как стремительно меняется время. Наша отрасль — наряду с отраслью ИТ — также стремительно развивается и меняется на глазах. Не так давно сформировалось ядро отрасли — ее цели и задачи, государственный регулирующий аппарат, научная база, система образования, — и казалось бы, этого достаточно, чтобы разумно и стабильно управлять развитием сравнительно небольшой, камерной сферы, в которой работает всего несколько десятков тысяч человек.

Но время бросает вызовы. И главный из них — масштаб. Доктрина информационной безопасности Российской Федерации (от 5 декабря 2016 г.) говорит об этом прямо и просто: «Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества. Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации».

Напомню также красноречивые количественные данные, приведенные в «Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года»: «В России сегодня насчитывается около 300 тыс. программистов <...>. Вместе с тем к 2019 году в мире будет насчитываться более 26 млн программистов, из них в Индии — более 5 млн человек, в США — более 4,5 млн человек, в Китае — около 2 млн человек».

Эти цифры — не новость. Я привел их не для того, чтобы рассказать о проблеме высококвалифицированных кадров в России, эта проблема активно решается, а для того, чтобы показать, как пропорционально потребностям ИТ в ближайшее времякратно увеличится и отрасль информационной безопасности. В такой ситуации перед отраслью, безусловно, встанут проблемы роста, которые невозможно решить одним только государственным регулированием.

Таким образом, в действие должны вступить механизмы саморегулирования и общественной поддержки.



В конце прошлого года по инициативе заслуженных специалистов в сфере информационной безопасности был создан Фонд содействия развитию безопасных информационных технологий.

Цель деятельности Фонда сформулирована так: «Содействие интеграции отраслей информационной безопасности и информационных технологий, развитию их научного и кадрового потенциала, распространение лучших отечественных практик в области безопасных информационных технологий».

ЧЕМ ЗАНИМАЕТСЯ

Чем занимается фонд конкретно? Направлений несколько. Поделюсь опытом только трех из них, тех, к организации которых я имею непосредственное отношение.

Во-первых, организация научных и научно-практических конференций, выставок.

Фонд создан не на пустом месте и, конечно, мы собираемся категорично вторгаться в сложившийся ландшафт отраслевых конференций и выставок. Наше дело — чтобы те выставки и конференции, которые мы проводим или курируем, были стабильно лучшими, служили образцами и по содержанию и по форме. Приведу свежий пример.

В этом году на IX Уральском форуме — одном из ключевых мероприятий отрасли — мы впервые заметили проявление различий между поколениями безопасников. Если раньше разница между условно 50-летними и условно 30-летними была не особенно заметна, то теперь разрыв в полтора-два десятилетия стал явственным. Он выразился не столько внешне, сколько внутренне: «старшие» и «младшие» предпочитали разные доклады, участвовали в разных дискуссиях, их интересовали разные темы, спикеры, форматы и направления, а там, где они оказывались за одним «круглым столом», выражали явно полярные позиции.

Они были совершенно разными! О чем это говорит? О том, что наша отрасль растет, развивается и... множится.

Процесс отрадный, но «Отцы и дети» — тема вечная, и давно известно, если не начать ее вовремя обсуждать, держать под контролем, она превращается в проблему. Чтобы этого не случилось мы, не откладывая дело в долгий ящик, на ближайшем мероприятии — Форуме АЗИ — организовали так называемую Дуэль поколений. Чтобы, как говорится, клин клином.

Как это выглядело? На сцене в интеллектуальной схватке сошлись три мэтра-практика информационной безопасности против трех молодых (27–30 лет), но достаточно опытных безопасников. Тему дуэли сформулировали так: «Как сохранить и приумножить опыт ИБ-поколений?»



Форум АЗИ (12 апреля 2017 года, г. Москва)



Симпозиум СТС Групп (5–7 июня 2017 года, Репино, Санкт-Петербург)

Вы удивитесь, зал был очень активен, всем хотелось поучаствовать, сказать свое слово. То есть мы попали в точку. Но самое интересное, что расхождение во взглядах у разных поколений оказалось исключительно внешним. Да, в деталях, которые часто в нашей профессии выходят на первый план, в частности, в вопросах бизнеса, расхождений было много. А вот в фундаментальных позициях противоречий не оказалось.

Какой сделали вывод? Безопасникам как воздух требуется понимание и философское осмысление своей деятельности. Вопросы «Куда идет профессия?», «Какое место она занимает среди прочих?», «Чем отличается от других?», «Каков ее общественный статус?» совсем не праздные, а очень даже важные,

причем, как среди старшего поколения, так и среди молодежи.

Стоит сказать, что мы активно расширяем практику международных мероприятий. В конце апреля, например, впервые провели SOC Форум в Астане, используем новые формы для традиционных мероприятий: PCI DSS Russia (Летняя сессия Уральского форума) в Москве и STS Group в Санкт-Петербурге.

ФОРМИРОВАНИЕ ЭЛИТЫ ОТРАСЛИ

Организация и повышение уровня мероприятий и выставок — это только одно из направлений нашей деятельности. Другое направление — поддержка интеллектуальных соревнований и обучающих мероприятий для молодежи.

В этом году Фонд продолжил традицию торжественного закрытия Межрегиональной олимпиады школьников по математике и криптографии и Межрегиональной олимпиады по информатике и компьютерной безопасности. Чтобы ребятам это событие запомнилось надолго и, возможно, повлияло на их выбор профессии, мы провели награждение победителей и призеров в легендарном МИАНе — Математическом институте им. В.А. Стеклова. Перед школьниками, их учителями и родителями выступили ведущие деятели науки, в том числе и вице-президент Академии криптографии РФ В.Н. Сачков, а также была прочитана захватывающая, больше похожая на шоу, лекция «Математическая составляющая» с демонстрацией удивительных фактов и опытов из мира геометрии и физики. Это событие школьникам уж точно запомнится.

Репортажи с таких мероприятий опубликованы в отраслевых СМИ, а также показаны по телевидению.

Тема профориентации, популяризации профессии в контексте кадрового обеспечения отрасли особенно волнует руководство Фонда. Проблема государственного масштаба, многофакторная и требует комплексного подхода. Тут мы пропагандируем концепцию сквозного образования: Школьник — Студент профильного вуза — Молодой специалист. За тот небольшой срок, что работает Фонд, мы сделали заметные шаги в этом направлении: привлекли специалистов и организовали социологическое исследование «Кадровая ситуация в ИБ: Россия». Его результаты были опубликованы в специальной брошюре, распространены и обсуждены на IX Уральском форуме. Кроме того, мы организовали подготовку и регулярную публикацию квалифицированных тематических обзоров, в частности, обзоров отечественных и зарубежных вузов, готовящих специалистов в сфере ИБ, обзоров рейтингов по трудоустройству выпускников, обзоров, посвященных самообразованию в сфере ИБ и других.

МЕДИА-ИНСТРУМЕНТАРИЙ

Третье направление нашей деятельности — медийное сопровождение развития безопасных информационных технологий. Поскольку, работая в Фон-



Смотрите выпуски ИБ-лектория на tv.ib-bank.ru

де, я одновременно являюсь и генеральным директором Медиа Группы «Авангард», то деятельность этих двух организаций во многом переплетена. Вкратце напомним, что Медиа Группа «Авангард» обладает полноценным медийным инструментарием, вполне достаточным, чтобы влиять на общественное мнение в отраслевом, и даже шире, масштабе. Мы выпускаем в бумажной и интернет-версиях авторитетный (лучший на сегодняшний день!) профессиональный журнал «BIS Journal — Информационная безопасность банков», поддерживаем популярный отраслевой интернет-портал, развиваем отраслевое телевидение BIS TV.

Именно по инициативе Фонда в этом году мы сделали акцент на развитие телевидения — расширили спектр программ. И вот почему. Нам показалось, что в сфере информационной безопасности появился ряд новых тем, например, agile, интернет вещей, блокчейн и т.д., которые будоражат умы профессионального сообщества, но еще плохо им осмыслены. От этого возникает такая интеллектуальная неразбериха с понятиями, их неправильное понимание, что в совокупности затуманивает горизонт событий.

И тут свое слово должны сказать медийные технологии, потому что, с нашей точки зрения, одна из главных задач медиа — это просвещение. В текущем году наше BIS TV занялось именно этим. Была создана программа

«ИБ-лекторий», в которой авторитетные в профессии люди, по долгу службы имеющие дело с тем или иным новым явлением, компетентно рассказывают о нем телезрителям. Да, спорные интерпретации возможны, но на первый план в таких передачах выходят уже не домыслы и интерпретации, а практический опыт и конкретные факты.

Если вы войдете на нашем портале ib-bank.ru в раздел ТВ, то наряду с другими программами и видеосюжетами перед вами откроются выпуски ИБ-лектория. В последних выпусках, например, Рустэм Хайретдинов (InfoWatch) читает лекцию «Agile и безопасность», Алексей Лукацкий (Cisco) рассказывает о серьезных трансформациях рынка киберпреступности, Алексей Качалин (Positive Technologies) с неожиданной стороны представляет модный нынче пентест и т.д.

Подводя итоги, можно сделать вывод, что Фонд содействия развитию безопасных информационных технологий только на начальной стадии своей деятельности уже активно воздействует на жизнь профессионального сообщества, актуализирует ее по разным направлениям, обогащает новым эффективным опытом и способствует повышению общего уровня и консолидации отрасли информационной безопасности России.

СКОВАННЫЕ ОДНОЙ ЦЕПЬЮ



Марина БРОДСКАЯ
обозреватель
BIS Journal



СПОРИТЬ О БЛОКЧЕЙНЕ, ПОХОЖЕ,
БУДУТ ДОЛЬШЕ, ЧЕМ ВНЕДРЯТЬ

В 2019 году будут приняты все нормативно-правовые акты, которые обеспечат использование технологии блокчейн в России. Об этом говорится в проекте программы «Цифровая экономика Российской Федерации», который разработало Министерство связи и массовых коммуникаций России. Минэкономики и Минкомсвязи рассматривают возможность использования технологии блокчейн в сфере госуправления и экономики, соответствующее поручение дал премьер-министр России Дмитрий Медведев.

А ТЕМ ВРЕМЕНЕМ...

Тем временем, пока в России только рассматривают законодательные основы использования технологии блокчейн на отдельных участках, власти Дубая, крупнейшего города ОАЭ, начали выстраивать свою экономику на основе технологии блочных цепей и уже осуществляют большинство операций, связанных с госструктурами, при помощи цепочки цифровых блоков. Считается, что это повысит эффективность взаимодействия органов власти и поможет привлечь в город бизнес.

Объединенные Арабские Эмираты далеко не первая страна, в которой те-

стируют технологию блокчейн. Присматриваются к ней и Еврокомиссия, и Европейский Центробанк, в Швеции на основе блокчейн хотят организовать работу базы данных Шведского земельного реестра, на основе этой технологии уже организована работа ряда криптовалют и системы Qiwi. С апреля криптовалюта, созданная на основе блокчейна — биткойн — вошла в список законных платежных средств в Японии.

КАК НАЧИНАЛОСЬ

Впервые о блокчейне (англ. Blockchain или block chain) стало широко известно как о технологии, которая использует-



ся для создания и пополнения кошельков виртуальной валюты — биткойна. Блокчейн — это система защиты и управления базами данных, которая поддерживает постоянно растущий список упорядоченных записей, называемых блоками. Каждый блок этой распределенной базы данных содержит метку времени и ссылку на предыдущий (родительский) блок. Считается, что по своей природе такая система устойчива к модификации данных — после записи данные в блоке не могут быть изменены задним числом.

В представлении обывателя, блокчейн — новая технология, которая связана с документооборотом и позволяет исключить посредников при проведении определенных операций, тем самым сокращая материальные и временные затраты. Технология удобна для хранения сведений об операциях с недвижимостью, о записях актов

гражданского состояния, финансовых операциях, штрафах и пр. По мнению специалистов — сторонников внедрения технологии в жизнь, она предоставляет неограниченные возможности для работы с данными вне зависимости от физического местонахождения пользователя и одновременно обеспечивает надежную защиту блоков цепочки от подделки.

БЛОКЧЕЙН. ЧТО ЭТО ТАКОЕ?

Выстроенная по определенным математическим правилам, технология блокчейн — это постоянно формируемая цепочка, которая представляет собой сложную структуру и состоит из отдельных блоков транзакций. Каждый блок содержит подтвержденную информацию о группе транзакции и о предыдущем блоке, за счет чего достоверность информации в блоках можно быстро перепроверить. Вся цепочка блоков

содержит сведения обо всех совершённых когда-либо операциях в базе данных. Исключение составляет первый блок в цепочке, у которого отсутствует родительский блок.

Отдельный блок цепочки состоит из заголовка и списка транзакций. Заголовок блока включает в себя свой хеш, хеш предыдущего блока, хеши транзакций и дополнительную служебную информацию, в том числе сведения со ссылками на транзакции с предыдущими состояниями данных. Комиссионные транзакции могут содержать в атрибуте любую информацию и не имеют родительских транзакций.

Вновь созданный блок цепочки будет принят остальными пользователями, если числовое значение хеша заголовка равно или ниже определённого числа, величина которого периодически корректируется. Жесткого алгоритма получения желаемого результата хеша нет, поэтому применяется метод случайного перебора. Обычно требуется большое количество пересчётов. Как только вариант найден, узел рассылает полученный блок другим подключенным узлам, которые проверяют блок и, в случае отсутствия ошибок, он считается добавленным в цепочку и следующий блок должен включить в себя его хеш.

**СЧИТАЕТСЯ, ЧТО ПО СВОЕЙ ПРИРОДЕ
ТАКАЯ СИСТЕМА УСТОЙЧИВА
К МОДИФИКАЦИИ ДАННЫХ— ПОСЛЕ
ЗАПИСИ ДАННЫЕ В БЛОКЕ НЕ МОГУТ
БЫТЬ ИЗМЕНЕНЫ ЗАДНИМ ЧИСЛОМ**

Распределенная база данных блокчейн формируется как непрерывно растущая цепочка блоков с записями обо всех транзакциях. Копии базы или её части одновременно хранятся на множестве компьютеров и синхронизируются согласно формальным правилам построения цепочки блоков. Информация в блоках не зашифрована и доступна в открытом виде, но защищена от изменений криптографически через хеш-цепочки с помощью асимметричного шифрования.

БИТКОИН КАК ПРИМЕР

В системе биткоин, где технология блокчейн отработана наиболее четко, величина целевого числа, с которым сравнивается хеш, корректируется через каждые 2016 блоков. Запланировано, что вся сеть системы биткоин должна тратить на генерацию одного блока примерно 10 минут, на 2016 блоков — около двух недель. Если 2016 блоков сформированы быстрее, то цель уменьшается и достичь её становится труднее, в противном случае цель увеличивается. Изменение сложности вычислений не влияет на надёжность сети биткоин и требуется лишь для того, чтобы система генерировала блоки почти с постоянной скоростью, не зависящей от вычислительной мощности участников сети.

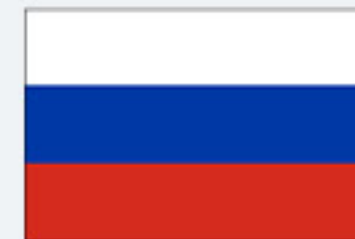
Для предотвращения многократной траты одной и той же суммы используются метки времени, реализованные путём разбиения БД на цепочку специальных блоков, каждый из которых, в числе прочего, содержит в себе хеш предыдущего блока и свой порядковый номер. Считается, что благодаря технологии наследования информации в блоке, повторная трата ранее израсходованных средств маловероятна. Также не учитывается умышленное изменение информации в любой из копий базы или в большом количестве копий, поскольку это не соответствует правилам. Однако некоторые изменения могут быть приняты и внесены во все копии базы, если при формировании нескольких последних блоков возникли ошибки.

При создании новых блоков часто возникают ситуации, когда у одного родительского звена появляется не-

БЛОКЧЕЙН FOREVER!

ЗА ЧЕСТНЫЕ ВЫБОРЫ!

Бизнес-омбудсмен Борис Титов предложил ЦИК использовать при голосованиях технологию блокчейн. По его мнению, можно продублировать классическую «бумажную» процедуру выборов электронной уже в ходе выборов Президента России в марте 2018 г. В ЦИК сообщили, что это предложение может быть реализовано в тестовом режиме в нескольких регионах, но только в случае, если не придется менять закон — необходимо совместить заложенный в Конституции принцип тайного голосования с верификацией каждого конкретного голоса. Новая технология позволит голосовать миллионам людей, которые работают вдали от места постоянной регистрации и де-факто лишены избирательного права. По мнению бизнес-омбудсмана, регистрация результатов голосования в блокчейн-системе закроет возможность манипуляций на выборах и полностью исключит из повестки дня проблему их возможной фальсификации.



ЕВРОПА ГОТОВИТСЯ ОСНОВАТЕЛЬНО

Европейская комиссия планирует создать обсерваторию и форум по вопросам технологии блокчейна, чтобы понять, какую роль государственные органы должны играть при её разработке и какое содействие оказывать для её освоения. Европарламент призвал Комиссию создать экспериментальный проект по наращиванию технических знаний и потенциала регулирования, говорится в сообщении Комиссии. Планируется провести конкурс по контракту на оказание услуг для создания обсерватории и форума, который соберёт комментарии по поводу использования технологии блокчейн. Предполагаемый бюджет проекта, который рассчитан на два года, составляет 500 тыс евро.



США. В РЯДУ ПРОЧИХ

В США подписан законопроект, запрещающий использование блокчейна для отслеживания происхождения оружия. Исключения составят случаи, когда сотрудник правоохранительных органов получает соответствующий ордер в ходе криминального расследования.



«Технология электронного отслеживания огнестрельного оружия означает платформу, систему или группу систем или устройств, использующих совместный реестр, распределенный реестр, технологию блокчейн или другую подобную технологию или электронную базу данных для децентрализованного, либо централизованного хранения информации. Такие системы не принадлежат и не контролируются каким-либо одним лицом или организацией и используются для отслеживания и контроля над использованием огнестрельного оружия», — уточняется в законопроекте 2216.

НЕ ОТСТАЕТ И УКРАИНА

Министерство юстиции Украины проводит консультации с компанией Bitfury (США) по внедрению технологии блокчейн в работу ведомства и госпредприятия «Система электронных торгов арестованным имуществом». Минюст как содержатель 17 государственных реестров заинтересован во внедрении новых технологий и подходов к защите информации и управлению информацией.



... И КАМБОДЖА

Национальный банк Камбоджи, при поддержке стартапа Soramitsu, разрабатывает новый прототип платежной инфраструктуры на базе технологии блокчейн.

Основанный в 2016 году, стартап Soramitsu является одним из создателей проекта Iroha, который присоединился к Hyperledger. По словам представителей Soramitsu, Национальный банк Камбоджи будет вносить свой вклад в разрабатываемые проектом программы на основе блокчейна.

**В СФЕРЕ АВТОРСКОГО ПРАВА**

Фонд «Сколково», Российское авторское общество, Российский союз правообладателей, Всероссийская организация интеллектуальной собственности, Высшая школа экономики, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Научно-исследовательский институт экономических стратегий и банк «Новый век» создают ассоциацию, цель которой — запустить в России единую платформу управления объектами интеллектуальной собственности IP-CHAIN. Будет создан Национальный координационный центр обработки транзакций с интеллектуальной собственностью. На основе единой платформы IPHub, которая будет работать на базе технологии блокчейн, будет создан сервис. Он позволит получить информацию о различных объектах интеллектуальной собственности — объектах авторских и смежных прав, патентах, товарных знаках и пр. Авторы и владельцы прав смогут размещать в базе данных свои объекты и определять пределы и способы их использования. Также будет разработан стандарт обмена информацией, чтобы к платформе могли подключать свои системы другие владельцы прав, сообщает газета «Ведомости».

**ИЩУ ЧЕЛОВЕКА!**

Европейский центробанк планирует нанять на руководящую должность специалиста в области технологий распределенного реестра, сообщается на сайте ЕЦБ. Основные требования к кандидату — не менее трех лет практического опыта в сфере технологий распределенного реестра и опыт управления проектами. Новый работник возглавит структурное подразделение ЕЦБ, которое будет предоставлять IT-услуги для таких направлений, как денежно-кредитная политика, инфраструктура банка и платежи.

ЕЦБ уже сформировал небольшую группу экспертов в области IT, которая будет изучать возможности использования технологии распределенного реестра (DLT) и реализации финтех-инноваций.



рам пользователей, на которых хранятся копии каждого из блоков. Вывести такую распределенную систему из строя нереально, если только не произойдет глобальный обвал сети и одновременное уничтожение всех носителей информации.

Открытость системы и возможность изучить каждый блок в отдельности позволяет отследить цепочку изменений информации и корректность представленных в блоке данных. При этом система шифрования надежно скрывает персональную информацию о пользователях системы. Для подтверждения пользователя сети блокчейн применяется специальный ключ, который, однако, не дает пользователю полный доступ к системе.

СТРОИТЕЛИ И РЯДОВЫЕ

Работают с блокчейн два типа пользователей: строители, которые отвечают за создание новых блоков, и рядовые участники, которые формируют простые записи о транзакциях. В задачи строителей входит сбор записей пользователей, формирование из них готовых блоков и рассылка информации по сети пользователям для дальнейшего хранения и проверки данных. За свою работу строители получают комиссионные.

ДОСТОИНСТВА И НЕДОСТАТКИ

Сторонники блокчейн полагают, что эта технология станет новым словом в области информационных технологий и обработки информации. Они утверждают, что у системы блокчейн есть неоспоримые преимущества — безупречная надежность и абсолютная безопасность, а также возможность проверки всей цепочки от момента ее создания до блока икс.

К недостаткам технологии относят низкую скорость работы, зависящую от трафика. Этот факт оказывает влияние на скорость внедрения технологии блокчейн в финансовой сфере, но никак не влияет на надежность сети блокчейн, считают поклонники технологии. Например, конкуренты банковской системы SWIFT рассматривают технологию блокчейн, чтобы совсем вытеснить банки из области проведения международных платежей. Мировой рынок денежных переводов оценивается сегодня в \$552 млрд.

сколько дочерних блоков и цель разветвляется. В таком случае возможно параллельное наращивание различных ветвей, например, в локальной сети. При ретрансляции блоков в глобальную сеть автоматически будет считаться основной более длинная цепочка, при равенстве длины параллельная работа продлится до создания нового блока. Приоритет отдается той части цепи, в которой блок появится раньше

и ветвь станет длиннее соседней. Работа над параллельной цепочкой прекращается, а транзакции, вошедшие в такую ветку, будут поставлены в очередь для включения в очередной блок.

УСТОЙЧИВОСТЬ И ОТКРЫТОСТЬ

Принято считать, что устойчивость сети блокчейн обеспечивается за счет распределения данных по компьюте-

ГЛАВНОЙ ПРОБЛЕМОЙ КРИПТОВАЛЮТ, ПОСТРОЕННЫХ ПО ТЕХНОЛОГИИ БЛОКЧЕЙН, ЯВЛЯЕТСЯ БЕЗОПАСНОСТЬ КОНЕЧНЫХ ТОЧЕК— УСТРОЙСТВ, КОТОРЫЕ ХРАНЯТ ЛИЧНЫЕ КЛЮЧИ ДЛЯ КОНТРОЛЯ ВИРТУАЛЬНОЙ НАЛИЧНОСТИ

МНОГИЕ СОМНЕВАЮТСЯ

Однако многие исследователи не разделяют столь радостных ожиданий в отношении блокчейн. С ними согласны и финансисты. Не поняли технологию блокчейн и ее преимуществ в компании PayPal — там продолжают использовать традиционные базы данных.

Международная межбанковская система передачи информации и финансовых транзакций SWIFT заявила об опасности нереалистичных ожиданий в отношении технологий цепочки блоков и распределённых реестров в банковской среде. Новая платформа международных платежей SWIFT построена без использования технологии блокчейн. При этом SWIFT готова использовать блокчейн в других направлениях и совместно с группой банков выведет на рынок стартапы, которые используют эту технологию.

ВАЖНЫЙ ЭКСПЕРИМЕНТ

В январе SWIFT объявила, что начала работу над приложением Proof-of-concept (PoC) для тестирования механизма оптимизации корреспондентских отношений между банками при помощи блокчейн-проекта Hyperledger. Блокчейн-приложение будет протестировано в закрытой банковской группе при жестком контроле профилей пользователей, их данных и привилегий. Для определения успешности PoC SWIFT проанализирует безопасность и конфиденциальность транзакций, а также возможность использования новых и более глубоких типов данных ликвидности счетов. Результаты тестирования нового решения на базе блокчейна будут представлены в октябре 2017 года в Торонто (Канада). В случае успешного испытания и внедрения решения, к нему присоединятся новые банки. Финансовые

организации смогут оптимизировать свою ликвидность и снизить операционные издержки.

А КАК С КОНФИДЕНЦИАЛЬНОСТЬЮ?

Группа американских исследователей поставила под сомнение утверждение об анонимности и конфиденциальности технологии блокчейн. По утверждению экспертов, применение методов эвристического анализа транзакций открытой информации в сети блокчейн позволяет отследить все транзакции одного и того же лица, даже если оно работает анонимно и создает несколько адресов для каждой новой сделки, выявить его денежные потоки и уточнить финансовые подробности.

Один из способов сокрытия информации из блока цепочки, за исключением самого факта существования сделки, — криптографический протокол электронной наличности, лежащий в основе криптовалюты Zerocash. Это альтернативная конструкция криптовалюты, которая использует передовую криптографию. Каждая сделка с криптовалютой сопровождается криптографическим публично проверяемым доказательством своей собственной действительности и подтверждает тот факт, что тратится сумма, не превышающая доступный лимит с этого адреса. Как утверждают создатели метода шифрования, в основе их математических допущений содержится много новых криптографических подходов.

ПРОБЛЕМА КОНЕЧНОЙ ТОЧКИ

Однако главной проблемой криптовалют, построенных по технологии блокчейн, является безопасность конечных точек — устройств, которые хранят личные ключи для контроля виртуальной наличности. Возможны потери из-

за физического повреждения жесткого диска или утраты (кражи) устройства с диском, а также кражи криптовалют вредоносными программами или путем целевых вторжений. В отличие от фиатных валют, кража криптовалют мгновенна и необратима.

И МНОГО ДРУГИХ ПРОБЛЕМ

Несколько лет назад группа американских исследователей рассмотрела различные способы хранения и шифрования личных ключей к биткоин-кошелькам и оценила их по 10 критериям, в числе которых были безопасность, удобство и скорость развертывания. Самым надежным признан способ хранения средств в виде наличных, он удовлетворял 9 критериям. Все виртуальные варианты хранения криптовалюты и ключей к ней имели те или иные изъяны.

Уже известны случаи краха бирж криптовалют, последовавших в результате хакерских атак. Например, крупнейшая в мире площадка для обмена биткоинов — биржа Mt.Gox — обанкротилась в 2014 году в результате хакерских атак. Ряд экспертов оценивали рынок биржи в \$300 млн, владельцы виртуальной валюты не смогли вывести свои средства.

* * *

Технология блокчейн имеет множество достоинств, в том числе возможность проведения операций без многочисленных посредников с одновременным ведением истории операции. Предприниматели и исследователи находят все больше областей для применения этой технологии, однако предсказанная технологическая блокчейн-революция до сих пор не свершилась. Вместо этого идет долгая и тяжелая работа по интеграции технологий в инфраструктуру интернета, компаний и сервисов. Цифровая идиллия натывается на многочисленные подводные камни, в числе которых конфиденциальность, безопасность и взаимодействие с реальным миром. И работы по дальнейшему исследованию, развитию и внедрению технологии хватит на ближайшие годы.



Александр БОДРИК
директор по развитию
бизнеса и консалтингу
ГК Иридис, CISA,
CCSK, ITIL Expert

ГОРОД КАК ПРОСТРАНСТВО ДОВЕРИЯ

КОНЦЕПЦИЯ ПЕРСПЕКТИВНОЙ СИСТЕМЫ
КИБЕРБЕЗОПАСНОСТИ ПРАВИТЕЛЬСТВА
МОСКВЫ

Современное государственное управление во многом полагается на цифровые технологии. Выработка государственной и муниципальной политики, подготовка и принятие решений, планирование и контроль бюджетных средств, организация госуслуг гражданам — все это сферы, в которых сегодня без цифровых технологий никуда.

Соответственно по мере «оцифровки» городских процессов все больше возрастает значимость кибербезопасности как предпосылки качества и доверия к результатам городского управления. Нельзя полагаться на аналитические сводки или мониторинг эффективности муниципальных проектов, сфер образования, здравоохранения и других, не имея уверенности в достоверности полученной информации, а значит, в том, что она обрабатывается, хранится и передается надлежащим — защищенным — образом.

Но обеспечение кибербезопасности государственной структуры коренным образом отличается от практик коммерческого сектора. С одной стороны, больший вес имеют нормативные требования регуляторов, с другой, государственные организации опере-

дили не одну коммерческую отрасль в автоматизации взаимодействия с клиентами (гражданами), с третьей, у государственных организаций принципиально шире набор заинтересованных в кибербезопасности сторон, ведь они хранят очень (очень!) много данных о физических и юридических лицах.

С учетом сложности задачи, а также имея в виду довольно частые обращения за консультациями коллег из госсектора, автор задался целью выработать гибкий и масштабируемый подход к управлению кибербезопасностью для государственной организации. Его основные контуры представлены на примере Правительства Москвы.

МАСШТАБ ЗАДАЧИ

Москва — центр политической и экономической жизни страны, а значит, обеспечение кибербезопасности процессов управления столицей и кибербезопасность ее жителей — задача не менее важная, чем кибербезопасность, скажем, Вооруженных Сил или ФСБ. С другой стороны, практики кибербезопасности силовых структур не применимы «в лоб» к гражданским процессам и проектам.

Периметр Правительства Москвы поражает воображение — более 2500 учреждений и сотни тысяч пользователей, повседневная деятельность которых влияет на жизнь более 12 млн человек.

Статья содержит анализ специфичных вызовов, высокоуровневое проектирование системы кибербезопасности Москвы, и будет полезна как специалистам столичного правительства, так и схожим по сути организациям — правительствам других субъектов федерации и стран, а также диверсифицированным и вертикально-интегрированным корпорациям.

СЕМЬ СПЕЦИФИЧЕСКИХ ВЫЗОВОВ

Однако впечатляющие цифры не полностью отражают сложность задачи обеспечения кибербезопасности большого города.

Во-первых, Правительство Москвы — это 6 подразделений прямого подчинения, 7 вертикалей Заместителей Мэра, что состоит из десятков департаментов, инспекций, управлений и комитетов и 11 префектур (включающих 125 управ), каждая из которых по экономическому потенциалу и масштабам социальных задач может потягаться с не самой маленькой европейской страной (например, Кипром или Эстонией). Каждое из этих подразделений может потенциально торпедировать реализацию эффективной «сквозной» системы в том случае, если возможности влиять на кибербезопасность у него будут меньше, чем его обычные политические возможности внутри Правительства Москвы. Управление любой «сквозной» функцией в таких условиях

**ПЕРИМЕТР ПРАВИТЕЛЬСТВА МОСКВЫ
ПОРАЖАЕТ ВОООБРАЖЕНИЕ — БОЛЕЕ
2500 УЧРЕЖДЕНИЙ И СОТНИ ТЫСЯЧ
ПОЛЬЗОВАТЕЛЕЙ, ПОВСЕДНЕВНАЯ
ДЕЯТЕЛЬНОСТЬ КОТОРЫХ ВЛИЯЕТ
НА ЖИЗНЬ БОЛЕЕ 12 МЛН ЧЕЛОВЕК**

должно быть выстроено с учетом интересов всех ключевых задач и структур Правительства Москвы. И кибербезопасность тут не исключение.

Во-вторых, Правительство управляет и/или поддерживает целый спектр отраслей социальных услуг и народного хозяйства, а также районов Москвы с их экономическим, социальным, этническим и культурным разнообразием. Это значит, что полностью централизованное управление не может быть эффективным и как следствие — эффективное управление рисками, в том числе рисками кибербезопасности, должно быть во многом децентрализованным и находиться в зоне ответственности руководителей вертикалей и префектур.

В-третьих, Правительство представляет из себя уникальную сервисную организацию, перед которой Мэром поставлены задачи радикального улучшения стандартов обслуживания клиентов — жителей Москвы. Правительство предприняло ряд шагов по централизации клиентского сервиса и уже оказывает услуги по трехуровневой модели (рис. 1). При этом концентрация деятельности влечет и концентрацию рисков.

В-четвертых, текущая экономическая ситуация стимулирует повышать эффективность расходования бюджетных средств, а значит, как минимум, для ряда активностей системы кибербезопасности будет необходима экономия на масштабе (economy on scale).

В-пятых, в отличие от многих других крупных и сервисных по своей сути организаций Правительство не относится ни к силовым структурам, ни к высокотехнологичным организациям, а значит, кибербезопасность нерационально рассматривать как отдельный риск. Для Правительства основными задачами есть и будут социально-экономическое развитие Москвы, а также поддержка жителей на выборах (политическая лояльность). В итоге кибербезопасность настолько полезна, насколько она может защитить выполнение задач Правительства от неопределенности в киберпространстве — будь то кибер-атаки или банальные сбои в работе сервисов. Соответственно, эффективной кибербезопасность может быть только при



Рисунок 1. Операционная модель обслуживания жителей Москвы

условии интеграции в процессы организации — интеграции на всех этапах: от поддержки принятия решений при постановке целей до обеспечения достоверности управленческой информации и гарантировании качественной обратной информационной связи от проектов и сервисов организации.

В-шестых, перед Правительством стоят гражданские задачи социально-экономической сферы, а значит, регуляторный компонент кибербезопасности априори не может быть ключевым, ведь главное — не формальное соответствие требованиям регуляторов (часто 20-летней давности), а предсказуемость реализации стратегического плана Правительства и повседневная безопасность жителей.

В-седьмых, в зависимости от Вертикали и отрасли необходимая для реализации стратегического плана Правительства скорость оцифровки городских сервисов и изменений существенно разнятся, что должно найти свое отражение в управлении кибербезопасностью. Ведь для цифровых сервисов кибербезопасность выполняет роль сцепления, без нее устойчивое развитие и предоставление цифровых сервисов просто невозможно.

ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ СИСТЕМЫ

Для проектирования системы кибербезопасности соответствующей размерам и специфике периметра Правительства

Москвы предлагается основываться на 5 ключевых принципах.

В силу большого числа влиятельных заинтересованных сторон важен принцип Прозрачности: Мэр и руководство Правительства, жители и регуляторы должны видеть направления и результаты деятельности системы кибербезопасности. Ведь именно для удовлетворения требований заинтересованных сторон существует функция кибербезопасности как таковая.

Прозрачная система кибербезопасности высветит необходимость реализации принципа Справедливости — учета всего комплекса интересов заинтересованных сторон — отсутствия однозначного навязывания требований кибербезопасности Вертикалям и префектурам.

Учитывающая интересы ключевых заинтересованных сторон система кибербезопасности («справедливая») будет встречать минимум организационного сопротивления и в целях эффективности сможет реализовать принцип Интегрированности, когда практики и меры кибербезопасности будут интегрированы как в повседневные процессы, так и в проекты развития.

Интегрированная в процессы и проекты система кибербезопасности неминуемо потребует реализации принципа Гибкости — возможности разрабатывать, устанавливать и внедрять практики кибербезопасности сообразно степени и скорости оцифровки процессов

и услуг того или иного сегмента Правительства.

Прозрачная, справедливая, интегрированная и гибкая система позволяет реализовать принцип Масштабируемости, что сократит влияние кибербезопасности на сроки ТТМ (time-to-market) / сроки вывода государственных цифровых сервисов и сроки реализации муниципальных программ и проектов.

ЧЕТЫРЕ КОНТУРА СИСТЕМЫ

Несмотря на то, что детальная структура системы кибербезопасности может быть выработана лишь в ходе отдельного значимого проекта, уже сейчас возможно выделить 4 взаимодополняющих контура системы кибербезопасности Москвы: централизованного планирования и контроля, централизованных сервисов, кибербезопасности Вертикалей и кибербезопасности префектур.

Контур централизованного планирования и контроля кибербезопасности призван разработать и предложить к утверждению руководству Правительства общие для всех учреждений в периметре Правительства «правила игры» (модельные политики и регламенты процессов безопасности). Главная задача контура — удостовериться, что каждое, существенным образом влияющее на кибербезопасность, управленческое решение достаточно проработано и принято на надлежащем уровне (Комитете / совещании), в том числе — что существуют механизмы эскалации и согласования исключений из правил. Второстепенная задача — внедрение культуры ответственности руководства структурных подразделений Правительства за их решения в сфере кибербезопасности, ведь последствия от этих решений могут существенным образом повлиять на достижение стратегических целей Вертикалей/префектур и Правительства в целом. Кибербезопасность сама по себе может быть только советником в рамках Вертикалей/префектур и независимым мониторинговым и координирующим органом в рамках Правительства в целом.

После определения необходимо удостовериться в выполнении политик

УЖЕ СЕЙЧАС МОЖНО ВЫДЕЛИТЬ 4 ВЗАИМОДОПОЛНЯЮЩИХ КОНТУРА СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ МОСКВЫ: ЦЕНТРАЛИЗОВАННОГО ПЛАНИРОВАНИЯ И КОНТРОЛЯ, ЦЕНТРАЛИЗОВАННЫХ СЕРВИСОВ, КИБЕРБЕЗОПАСНОСТИ ВЕРТИКАЛЕЙ И КИБЕРБЕЗОПАСНОСТИ ПРЕФЕКТУР

и регламентов безопасности — реализовать программу аудитов кибербезопасности на регулярной основе с применением риск-ориентированного планирования. Аудиты могут распространяться на Вертикали, префектуры и ключевые подведомственные учреждения. Согласно Международным стандартам внутреннего аудита аудиты в специфичных областях (в том числе кибербезопасности) может проводить и служба внутреннего аудита (ГлавКРУ) — но в случае наличия необходимых компетенций.

Контур централизованных сервисов кибербезопасности призван обеспечить единый уровень качества и минимальные затраты на реализацию общих сервисов безопасности. Среди таких обычно — проектно-архитектурный сервис, сервис сопровождения проверок регуляторов, сетевая безопасность, противодействие вредоносному коду, Anti-DDoS, мониторинг событий и уязвимостей сетевой безопасности, а также выявление целевых атак. Ключевой принцип создания этого контура фундаментально справедлив — Вертикали и префектуры, что желают получить доступ к общим сервисам, должны выполнять и/или потреблять установленные для пользователей общих сервисов требования кибербезопасности — как в части информационных систем так и в части поведения сотрудников. Контур планирования и централизованных сервисов логично организационно должны входить в вертикаль операционного директора (руководителя аппарата) Правительства.

Контур кибербезопасности Вертикалей призван защитить интересы Вертикалей в общих процессах ки-

бербезопасности, адаптировать общие политики и процедуры под их специфичные потребности и выявить специфичные для них проблемные места в сфере кибербезопасности (в первую очередь в области специфичных для отраслей Вертикали приложений и сервисов для граждан), не отрываясь при этом от «полей». С другой стороны, контур разгружает централизованные процессы планирования, проводит контрольные мероприятия в отношении структурных подразделений и подведомственных учреждений Вертикали, а также реализует фундаментально «близкие к земле» процессы повышения осведомленности, управления доступом и расследования инцидентов.

Контур кибербезопасности префектур функционирует аналогично контуру кибербезопасности Вертикалей, но фокусируется на «полевых» процессах — управлении доступом (определение ролей, согласование доступов, управление исключениями, ведение каталога информационных ресурсов и их владельцев, аудит доступов), повышении осведомленности (security awareness — тренинги и экзамены), расследовании связанных с сотрудниками инцидентов, представлении интересов префектуры в общих совещаниях и процессах кибербезопасности, и во вторую очередь, на обеспечении безопасности локальных информационных ресурсов. Организационно контуры для префектур и Вертикалей могут быть реализованы в виде отдельных должностей в рамках префектур и Вертикалей или в виде отделов кибербезопасности префектур и Вертикалей в рамках централизованного подраз-

деления кибербезопасности. Возможен и смешанный вариант: Вертикали и префектуры с существенной потребностью в кибербезопасности создают собственные структуры по кибербезопасности, другие — обслуживаются из централизованного подразделения. Крупные подведомственные учреждения обслуживаются по типу префектур, небольшие могут обслуживаться контуром кибербезопасности Вертикалей или префектур.

В первом приближении взаимодействие между контурами системы кибербезопасности может выглядеть как на рис. 2.

РАСПРЕДЕЛЕНИЕ ПОЛНОМОЧИЙ В СИСТЕМЕ

Столь развитая и диверсифицированная система кибербезопасности требует примеров для иллюстрации, как такие системы обычно работают в реальной жизни.

В управлении доступом ведущая роль принадлежит префектурам или подведомственным организациям (подведам). Доступы всегда согласовываются и аудируются в контуре кибербезопасности префектур или даже подведах, согласование или аудит доступов со стороны Вертикалей или централизованной кибербезопасности необходимо лишь при доступе сотрудников префектур к информационным ресурсам Вертикалей или общегородским ресурсам.

При обеспечении Безопасности в ИТ-проектах обязанности разделены — централизованная кибербезопасность организует конвейер контроля (аудита) безопасности в проектах (с четкими критериями и SLA), организует обучение и продвигает нормы функционирования конвейера как минимум среди Вертикалей и префектур.

Возможно создание и общего сервиса безопасности в проектах — архитектурного офиса, который разрабатывал бы архитектуры безопасности проектов в интересах Вертикалей или префектур. В случае отсутствия такового — архитектуры разрабатываются самими Вертикалями. В свою очередь Вертикали/префектуры выступают аудиторами безопасности проектов

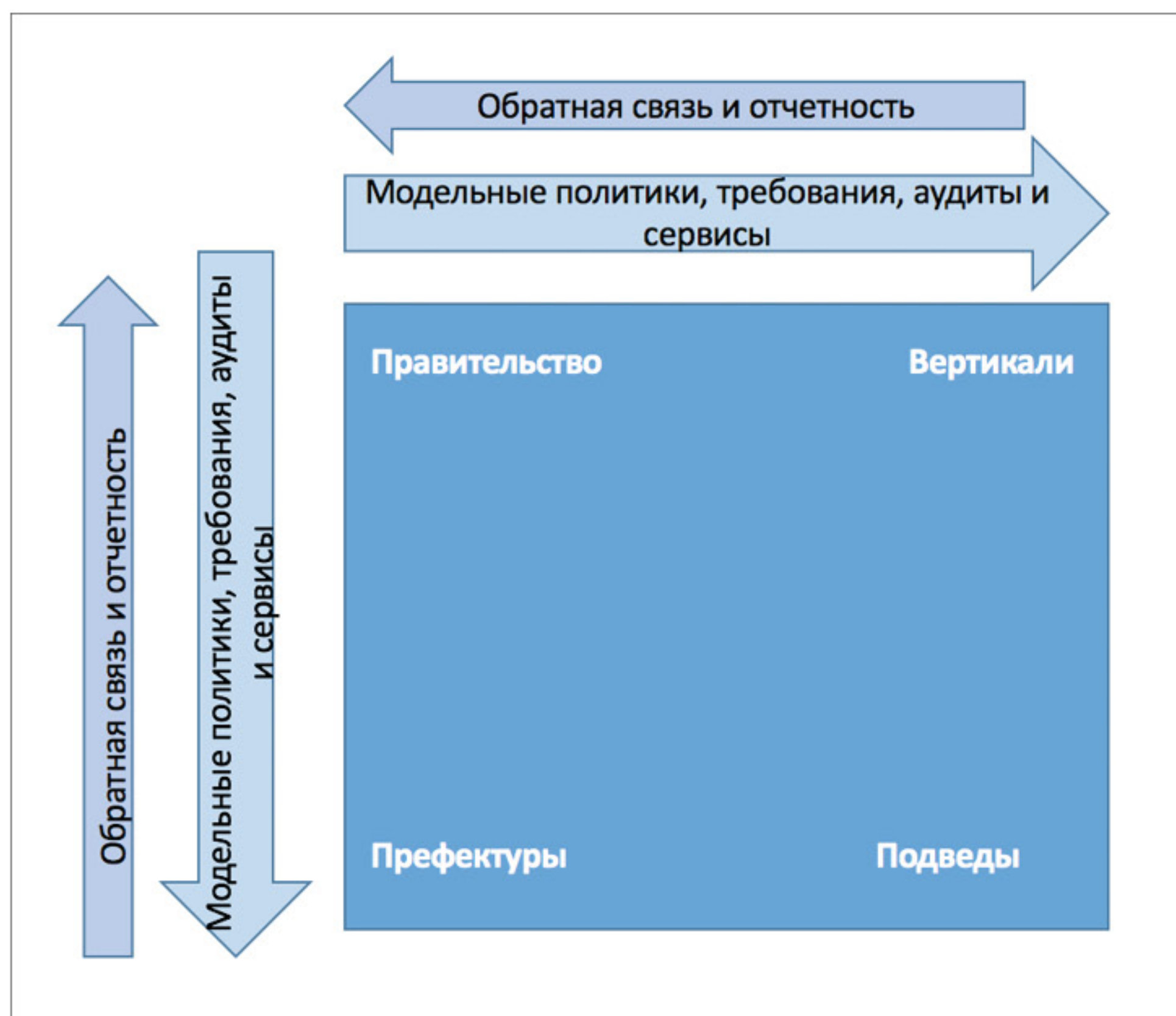


Рисунок 2. Схема взаимодействия контуров системы кибербезопасности Москвы

для своих подведов. Степень централизации может различаться, ключевой момент — разделение деятельности по организации самого конвейера и управлению конвейером, текущего аудита проектов и разработки архитектур безопасности.

Отдельный момент. В случае разногласий между аудиторами и архитекторами (представителями Вертикалей, префектур или подведов) вопрос эскалируется, и риски принимаются на уровне руководителя Вертикали или префектуры, а протокол принятия рисков надлежащим образом хранится. В случае выявления ошибочности принятого решения в будущем, возможно будет извлечь уроки, перестроить конвейер либо повысить/понижить уровень необходимого согласования.

Бюджетирование и планирование могут быть реализованы по ставшей классикой в крупных корпорациях «ножничному» принципу. С одной стороны, происходит планирование «сверху вниз» — централизованная кибербезопасность планирует закупку централизованных мер безопасности (например, комплексов защиты

конечных точек — выросли из антивирусов), а также готовит руководство по бюджетированию кибербезопасности для локальных служб информационной безопасности в префектурах, Вертикалях и подведах. С другой, каждый подвед готовит свои предложения по локальным потребностям, они согласовываются с его Вертикалью или префектурой, позже попадают в интегрированный бюджет по кибербезопасности.

Как одному из самых крупных и разношерстных мегаполисов мира, Москве для устойчивого развития необходима гибкая и всеохватывающая система кибербезопасности. Надеюсь, данный материал поможет привлечь внимание к проблемам систем кибербезопасности не только Москвы, но и других регионов, а также крупных российских корпораций, разнообразие видов и география деятельности которых требует сочетания гибкости, экономности и согласования интересов многих заинтересованных сторон.

КАК ПОВЫСИТЬ?

ПРАКТИЧЕСКИЕ СОВЕТЫ ПО ПОВЫШЕНИЮ ОСВЕДОМЛЁННОСТИ ПЕРСОНАЛА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Будет преувеличением утверждать, что ответ на вопрос «зачем?» применительно к повышению осведомлённости персонала в области информационной безопасности уже не вызывает затруднений у ИТ / ИБ-руководителей. Но, так или иначе, под воздействием регуляторов, коллег или самой жизни (вспоминая про персонал после очередного инцидента), большинство уже пришло к пониманию необходимости (а многие — и к пониманию полезности) повышения осведомлённости персонала.

Эта статья не преследует цель в очередной раз обосновать нужность повышения осведомлённости — немного полистав различного рода и веса нормативные документы (желательно не только «наши»), каждый внимательный их читатель неизменно обнаружит, что повышение осведомлённости есть обязательный компонент корпоративной системы обеспечения информационной безопасности.

Мы попытаемся начать отвечать на вопрос «как?». Иными словами, в статье предлагается ряд практически значимых советов относительно того, как сделать повышение осведомлённости эффективным и «живым» процессом обеспечения и поддержания информационной безопасности в организации. Некоторые из этих советов могут показаться не новыми и даже очевидными, но, поверьте, именно о них чаще всего и забывают.

НАЛИЧИЕ ПОДДЕРЖКИ ВЫСШЕГО РУКОВОДСТВА

Это не ново: для многих значимых в масштабах организации инициатив поддержка высшего руководства — необходимый фактор успеха. То же справедливо и для реализации программы

повышения осведомлённости персонала, причём двояко.

Программа повышения осведомлённости должна быть формально санкционирована высшим руководством организации: это придаёт инициативе административный статус, повышает вероятность должного ресурсообеспечения, включая (правда, не всегда) финансирование, а ответственному за реализацию программы даёт весьма часто полезный административный ресурс.

С другой стороны, поддержка руководства должна выражаться в участии самого высшего руководства в программе повышения осведомлённости в роли слушателей. Если высшее руководство личным примером демонстрирует поддержку программы — это ли не лучший мотиватор для подчинённых!

ДОЛЖНОЕ ДОКУМЕНТАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Чтобы руководство санкционировало программу повышения осведомлённости, а иной требовательный государственный орган не имел вопросов, вполне уместно сформулировать и изложить в соответствующих документах организационный, методологический и методический аспекты повышения осведомлённости в организации. Например, речь может идти о следующих документах:

- ◆ политика повышения осведомлённости персонала;
- ◆ программа повышения осведомлённости персонала;
- ◆ методика оценки уровня осведомлённости персонала;
- ◆ методика оценки эффективности программы повышения осведомлённости персонала.

Разработкой подобных документов часто не считают нужным заниматься,

либо не видя от них пользы, либо опасаясь хлопотности их согласования и ввода в действие. Тем не менее, такие документы закладывают системную основу корпоративной программы повышения осведомлённости, задают её рамки, основные метрики, зоны ответственности и процессы планирования, реализации и совершенствования. Наличие и реальная работа по таким документам свидетельствует о высоком уровне зрелости культуры обеспечения информационной безопасности в организации. Пока в России об этом задумываются, пожалуй, лишь организации финансового сектора да российские представительства западных компаний.

ПРАВИЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПРАВИЛЬНОЙ АУДИТОРИИ

Повышение осведомлённости диспетчеров АСУ ТП с помощью компьютерных экранных заставок может привести к самым неожиданным последствиям, но все они будут негативными. Если учебный курс почти полностью состоит из цитат нормативных актов и организационно-распорядительных документов, пестрит аббревиатурами (в т.ч. англоязычными) и ИТ / ИБ-сленгом, а понятный для не-ИТ / ИБ-специалиста язык в нём «днём с огнём», то, конечно, эффект от такого повышения осведомлённости будет минимальным. Но делать иначе часто не хотят, а ещё чаще — не могут.

Поэтому, основываясь на опыте выполненных UBS проектов по повышению осведомлённости, хотелось бы акцентировать внимание на следующем.

Информационно-обучающие материалы в рамках программы повышения осведомлённости, очевидно, должны быть адаптированы для целевой аудитории. То есть должны учитывать

специфику аудитории (отраслевую и функциональную принадлежность, организационный уровень, текущий уровень осведомлённости и т.д.) и соответствовать целям обучения.

Например, перечень и «вес» тем ИБ-инструктажа для сотрудников казначейства должны отличаться от таковых для менеджеров по продажам, а для высшего руководства базовую версию уместно сократить до ёмкого, но практичного конспекта максимум на 15–20 минут.

В начале реализации программы постарайтесь явно показать, какую личную выгоду извлечёт каждый слушатель из повышения осведомлённости — любой делает что-либо с существенно большей мотивацией при наличии личной заинтересованности.

Например, в курсе по безопасному использованию мобильных устройств нелишне сделать пару слайдов с конкретными рекомендациями по использованию личных мобильных устройств, а в ходе очного тренинга по сетевой безопасности можно обстоятельно ответить на вопросы участников по конфигурированию домашних беспроводных сетей.

Не пытайтесь достичь программой повышения осведомлённости сверхцелей. Очевидно, не надо стараться сделать из каждого сотрудника специалиста по информационной безопасности — это всё равно не удастся, да и совершенно не нужно.

Если вам удастся убедить сотрудников 1) прочитать, 2) понять и 3) выполнять (с ростом номера растёт и сложность задачи!) хотя бы 3–5 базовых правил ИБ, «закрывающих» 80–90% инцидентов в организации, — это уже серьёзный результат, который значительно повысит общий уровень обеспечения информационной безопасности.

ПОГОЛОВНОСТЬ

Возможно, режущая слух, но вполне точная характеристика: если вы хотите добиться реального повышения осведомлённости персонала, программой должен быть охвачен весь персонал, как-либо взаимодействующий с любыми устройствами обработки корпоративных данных. Включая сотрудников



удалённых филиалов и высшее руководство.

И особенно высшее руководство! Во-первых, как говорилось выше, участие руководства в каком-нибудь тренинге по безопасному использованию электронной почты бок о бок с «простыми» сотрудниками свидетельствует о важности этого «отвлечения от созидательного труда». Во-вторых, с точки зрения обеспечения информационной безопасности высшее руководство — такие же пользователи, зачастую ничуть не более осведомлённые (и вполне могущие стать, скажем, жертвой целевого фишинга с труднопредсказуемыми последствиями).

НЕПРЕРЫВНОСТЬ (ПЕРИОДИЧНОСТЬ)

Если ИБ-инструктаж проводится формально и раз в год, а в коридорах висит один и тот же потрёпанный и пожелтевший постер — не стоит ожидать, что персонал будет сам собой помнить о какой-то там информационной безопасности.

Чтобы сотрудники действительно помнили и выполняли правила обеспечения ИБ, совершенно необходимо «заниматься» повышением осведомлённости непрерывно или периодически. Объём повторных мероприятий, степень охвата ими персонала и периодичность их проведения выбираются исходя из потребностей, масштаба и возможностей организации. Кто-то

рекомендует 90-дневные циклы, кто-то советует ежемесячно делать рассылку и/или «прогонять» по одному учебному модулю — конкретный рецепт зависит от подробностей. Главное — не рассматривать повышение осведомлённости как разовое мероприятие, имеющее незатихающий и долговременный эффект. Разумеется, если вас интересует результат.

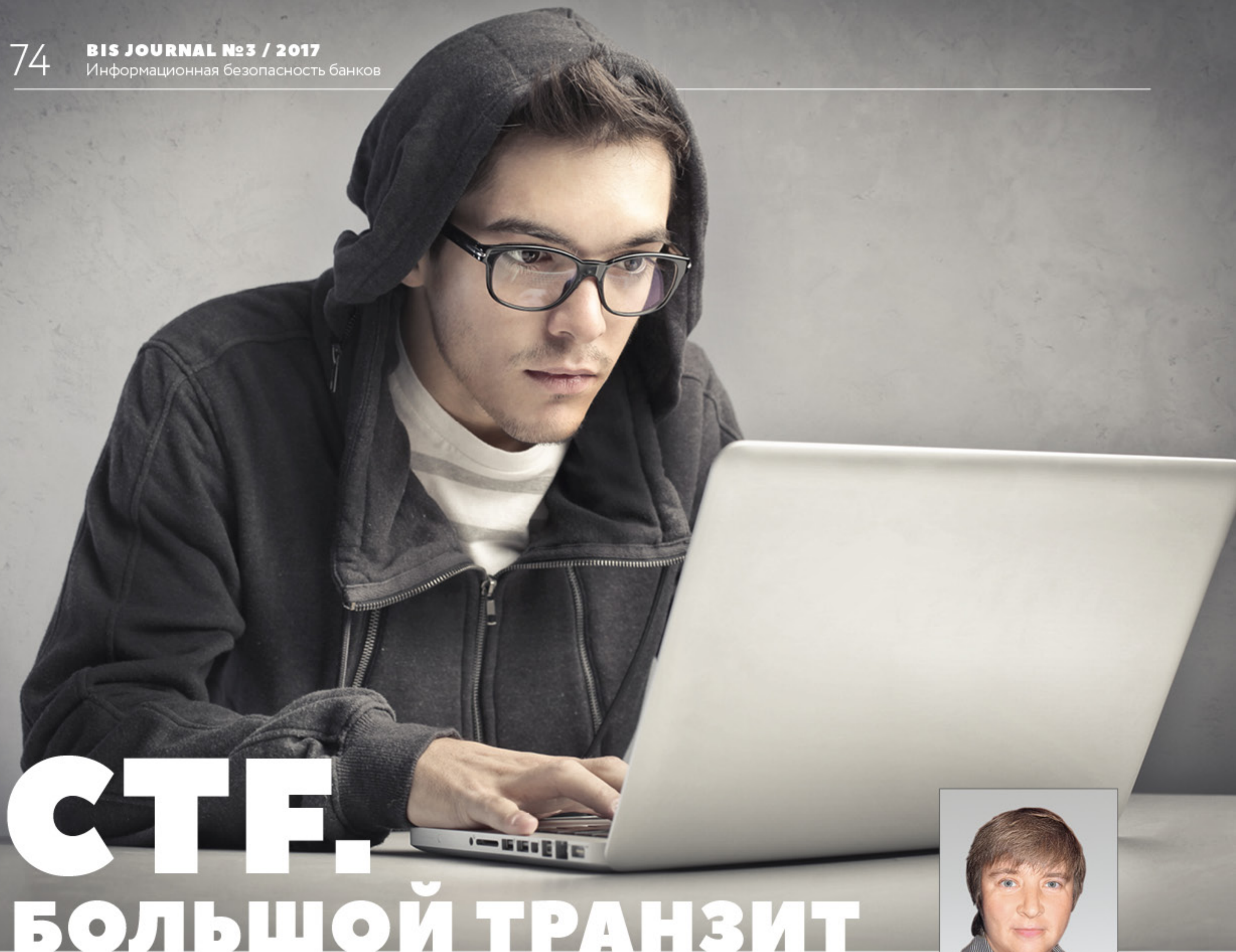
ЗАКЛЮЧЕНИЕ

За рамками этой краткой статьи остались столь важные на практике вопросы как:

- ♦ обоснование целесообразности повышения осведомлённости персонала перед бизнес-руководством организации (спонсорами);
- ♦ методика определения текущего уровня осведомлённости персонала;
- ♦ возможности реализации мероприятий по повышению осведомлённости своими силами, без привлечения сторонних консультантов;
- ♦ измерение эффективности (в т.ч. экономической) программы повышения осведомлённости.

* * *

Автор статьи и специалисты UBS постараются осветить эти и другие вопросы по теме повышения осведомлённости персонала в области информационной безопасности в последующих материалах.



СТЕ. БОЛЬШОЙ ТРАНЗИТ

ЧЕРЕЗ ХАКЕРСТВО В ИБ. МАССОВАЯ
ИГРА ПОМОГАЕТ РЕШАТЬ ПРОБЛЕМЫ
ПРОСВЕЩЕНИЯ И КАДРОВ



Марина БРОДСКАЯ
обозреватель
BIS Journal

Как привлечь большую массу молодежи в информационную безопасность? Ведь мало кто из подростков на вопрос «Кем ты хочешь стать?» ответит: «Хакером». И даже не потому, что такой ответ может показаться молодому человеку не приличным, а просто, скорее всего, он об этой сфере деятельности мало что знает. Давно известно, что самый эффективный и в то же время универсальный способ обучения, помогающий расширить кругозор и сделать некий выбор, — игра. Этот способ эффективен не только при обучении малышей, но и для профессиональной ориентации взрослых. Причем, в массовом порядке.

ПРАВИЛА ИГРЫ

Весна 2017 г. ознаменовалась не только аномальными холодами и масштабной атакой вируса WannaCry на пользователей в 150 странах мира, но и многочисленными соревнованиями по защите информации среди студентов и старшеклассников. Заключительные этапы некоторых соревнований прошли в крупных региональных университетах, а среди участников были не только команды отечественных учебных заведений, но и гости из разных стран мира.

Большинство соревнований прошли в одном из самых популярных на сегодня форматов — Capture the flag. Это командные соревнования, целью которых является оценка умения участников за-

щищать компьютерные системы и проводить аудит их безопасности. Команда должна поддерживать сервисы своего сервера в рабочем состоянии, предотвращать попытки вторжения («удерживать свой флаг») и проводить аудит серверов других команд, чтобы «захватить чужой флаг».

В ходе соревнований участники команд должны показать общую эрудицию в области информационной безопасности и администрирования сетей, знания в области методов компьютерных преступлений, умение решать криптографические задачи, искать и устранять различные уязвимости систем, знания в области программирования и умения анализировать и синтезировать чужие

разработки ПО, показать навыки стеганографии. Компетентное жюри оценивает команды за умение «защитить свои флаги» и «захватить чужие флаги».

МЫСЛИТЬ КАК ХАКЕР

Во многих российских университетах к участию в соревнованиях в формате CTF приглашают студентов, не обучающихся по специальностям в сфере защиты информации. К подобной практике уже давно прибегают в университетах США. Например, профессор Университета Карнеги-Меллон (Пенсильвания, США) Дэвид Брумли в своей статье, посвященной обучению основам ИБ, отмечает, что многих студентов сначала привлекала сама игра в «Захват флага». Уже потом они узнали, что в процессе подготовки к соревнованиям освоили этические навыки взлома и научились мыслить как хакер. Ведь никто из тех, кто стоит перед вы-

бором профессии, не скажет, что мечтает быть киберпреступником.

По данным университетского сайта, посвященного CTF, в этом году соревнованиями заинтересовались более 17 тыс. студентов, которые получили практические навыки взлома компьютерных систем. А с 2013 г., когда университет начал проводить такие соревнования, через CTF прошли более 57 тыс. человек. И многие из них до этого не знали, что цель соревнований — построение надежной информационной защиты компьютерных систем. Простое знакомство со сферой ИБ позволило многим студентам открыть в себе новые способности и продолжить учиться по направлению кибербезопасности.

В РОССИИ

В России первые соревнования CTF прошли в 2014 г. и сегодня только набирают обороты: RuCTF, RuCTFE,

M*CTF, VolgaCTF, SibirCTF, NSKCTF, KrasCTF... С каждым годом все больше регионов включаются во всероссийские соревнования, растет и число участников «игры».

В середине мая в Москве в рамках Школы кибербезопасности Московского политехнического университета прошли II всероссийские соревнования в области защиты информации RCC 2017, одним из организаторов которых стал VolgaCTF. В них приняли участие студенты Самарского университета, Южного федерального университета, МГУ, Московского Политеха, МИФИ, Новосибирского государственного университета, Научной роты Министерства обороны России, Высшей школы экономики и Крымского федерального университета.

А в Южном IT-парке прошёл финальный тур IV Открытой всероссийской олимпиады по информационной безо-

КАЛЕНДАРЬ ЛЕТНИХ СОРЕВНОВАНИЙ В ФОРМАТЕ CTF

1–10 июня 2017, г. Ханты-Мансийск. II Открытые соревнования в области информационной безопасности среди команд школьников старших классов и учащихся профессиональных образовательных организаций UgraCTFSch 2017. Соревнования впервые прошли в 2016 г. в рамках VIII Международного IT-форума с участием стран БРИКС и ШОС. Основной целью игры стало повышение уровня теоретических знаний у школьников и совершенствование их практических навыков. В финал прошли 30 старшеклассников, которые продемонстрировали навыки по защите информационной системы от внешних воздействий и решению логических задач в этой сфере.

21–20 июня 2017, г. Махачкала. III Региональные межвузовские соревнования в области информационной безопасности в Махачкале DagCTF 2017. Впервые школьники и студенты Северного Кавказа приняли участие во всероссийском этапе межвузовских соревнований в области ИБ в 2015 г., соревнования прошли на базе Дагестанского государственного университета народного хозяйства. В 2016 г. в соревнованиях участвовали команды трех местных университетов и гостевая команда, все призовые места достались хозяевам.

26–27 июня 2017, г. Барнаул. III региональные соревнования по информационной безопасности AltayCTF-2017. Очные CTF-соревнования проходят с 2015 г. как для школьников, так и для студентов. Формат AltayCTF-2017 — task-based. К участию ждут студенческие команды из Алтайского края, Сибири и других близлежащих регионов. Организаторами соревнований «AltayCTF-2017» выступают Ассоциация руководителей служб информационной безопасности (АРСИБ), Алтайский государственный технический университет им. И. И. Ползунова, CTF-команда АлтГТУ SharLike.

5–13 августа 2017, г. Дубна, Московская область. Летняя школа «Развитие CTF движения в России». Впервые занятия в школе «Развитие CTF в России» прошли в 2013 г. по инициативе Межрегиональной общественной организации «Ассоциация руководителей служб информационной безопасности» (АРСИБ) и ОЭЗ ТВТ «Дубна» при поддержке оргкомитета RuCTF. Участники Летней школы делятся на несколько команд. Цель каждой команды — набрать наибольшее количество баллов по итогам всех дней школы. Баллы начисляются за выполнение различных конкурсов и заданий. Конкурсы рассчитаны на самых разных по уровню участников. Вне зависимости от уровня подготовки каждая команда курируется одним из организаторов, который на определенных условиях готов помочь участникам в прохождении того или иного конкурса. Помимо конкурсной части, в программу Летней школы входят практические лекции и мастер-классы.

пасности UFO CTF SCHOOL 2017. Ему предшествовал отборочный онлайн-тур, определивший 20 лучших школьников и 20 лучших студентов из Севастополя, Тюмени, Новосибирска, Сочи, Краснодара, Хабаровска, Пятигорска, Омска, Санкт-Петербурга, Москвы, Томска, Владикавказа, Бердска и Красноярска. Финальный этап проходил в традиционном формате task-based CTF, большая часть заданий которого была на эксплуатацию уязвимостей бинарных файлов и реверс-инжиниринг. Особый интерес представляло задание, в котором требовалось изучить обфусцированный код скрипта, эмулирующего работу управляющего центра ботнет сети через посты в сервисе Twitter.

Первый UFO CTF SCHOOL состоялся в 2014 г. в Таганроге на базе кафедры «Безопасности информационных технологий» ИКТИБ ИТА ЮФУ, а с 2016 года финал олимпиады принимает Южный IT-Парк. За эти годы число участников выросло с 300 человек до 3 тысяч.

О ПОЛЬЗЕ ВЗЛОМА ПАРОЛЕЙ

Есть три вещи, которые стоит сделать, чтобы восполнить критическую нехватку специалистов в области ИБ, отмечает профессор Дэвид Брумли в своей статье. Кадровый дефицит в сфере кибербезопасности актуален как для США, так и для России.

Во-первых, стоит поощрять опыты учеников школ по взлому и подбору паролей, но только в соответствии с этическими нормами конфиденциальности и обмена информацией в интернете. Сегодня образование в области ИБ также важно, как и математика и литература. И важно вовремя объяснить, чем отличается хакер — специалист по ИБ, который хочет сделать систему более безопасной, от того, кто эксплуатирует

ПО ОЦЕНКАМ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ, К 2022 ГОДУ В МИРЕ БУДЕТ ПОРЯДКА 1,8 МЛН ВАКАНСИЙ СПЕЦИАЛИСТОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

киберпространство в своих целях. Последние являются преступниками.

Во-вторых, необходимо разработать эффективные программы образования в области кибербезопасности на национальном уровне. Как показывает опыт университетов, многие из них имеют десятки курсов в области ИБ, однако это капля в море. Курсы ИБ стоит внедрять в частную жизнь, преподавать в начальной школе, вводить в программу средней школы, чтобы учителя могли использовать материалы по ИБ в классе.

В-третьих, стоит признать ценность работы хакеров. Они находят уязвимости для того, чтобы сделать систему более безопасной. Хакеры умеют мыслить нестандартно, они любопытны, любознательны и любят экспериментировать. Те, кто занимается развитием своих творческих навыков, становятся мастерами своего дела, художниками, которыми можно восторгаться, если они не переступают черту.

Мыслить нестандартно учат студентов Мэрилендского университета в Колледж-Парке. Им предлагают взломать компьютерную систему учебного заведения, в другом месте за такое деяние могут отправить в тюрьму и надолго. А выпускники университета, освоившие все тонкости взлома и защиты компьютерной сети организации, еще до окончания учебы получают приглашения на высокооплачиваемую работу в крупнейшие технологические компании мира.

ПРОФОРИЕНТАЦИЯ КАК ОСНОВА ОТБОРА

По оценкам международных организаций, к 2022 году в мире будет порядка 1,8 млн вакансий специалистов в области кибербезопасности. Многие аналитики считают, что основная проблема будущей нехватки кадров заключается в отсутствии базового образования по ИБ в средних школах, колледжах и университетах, плохо обстоит дело с профориентацией молодых специалистов и желанием компаний вкладывать средства в обучение и повышение квалификации уже работающих сотрудников.

Еще один аспект профессиональной ориентации рассматривают эксперты компаний IDC и T.E.N, которые в 2015 г. провели опрос кадрового персонала по поводу вакансий в области ИБ. Вакансии в области кибербезопасности для старшего персонала могут быть свободными 12–15 месяцев, поиск кандидата на позицию специалиста по безопасности начального уровня занимает до 3 месяцев. Чаще всего соискатели не понимают, что за работу они ищут. Кто-то полагает, что в сфере ИБ требуются знания только из области IT-технологий, кто-то считает эту работу нудной, потому что предстоит сидеть весь день перед монитором. Кто-то не понимает разницу между безопасностью инфраструктуры, системами безопасности, безопасностью приложений или управления программами. Чтобы преодолеть эту проблему, стоит вести просветительскую работу и чаще рассказывать, чем занимаются специалисты по ИБ.

По мнению исследователей, также стоит пересмотреть подход к требованиям специалиста по ИБ и расширить круг квалифицированных сотрудников, которые могут сделать хороший старт по карьерной лестнице. Ведь знания не технических аспектов проблемы

ВАЖНО ВОВРЕМЯ ОБЪЯСНИТЬ, ЧЕМ ОТЛИЧАЕТСЯ ХАКЕР — СПЕЦИАЛИСТ ПО ИБ, КОТОРЫЙ ХОЧЕТ СДЕЛАТЬ СИСТЕМУ БОЛЕЕ БЕЗОПАСНОЙ, ОТ ТОГО, КТО ЭКСПЛУАТИРУЕТ КИБЕРПРОСТРАНСТВО В СВОИХ ЦЕЛЯХ



Пять уровней карьеры в области ИБ (источник: www.issa.org/?page=CSCL)

безопасности, например, юридических норм, не менее важно, чем умение вовремя предотвратить проникновение в сеть компании.

ОПЫТА НЕТ? ПРИХОДИТЕ!

По опыту Дэна Джера, CISO венчурного фонда In-Q-Tel, созданного при участии ЦРУ США, отличными специалистами в области ИБ становятся разработчики ролевых компьютерных игр, поскольку они имеют нестандартное мышление и талант для работы в кибербезопасности. Однако часто хэдхантеры отсеивают таких кандидатов на вакансию специалиста по ИБ как не имеющих опыта работы в сфере безопасности и тем более не имеющих дипломов и сертификатов. Тем самым они упускают шанс принять на начальную позицию перспективного сотрудника. Для того, чтобы решить проблему кадрового голода в области ИБ, кадровикам стоит убрать многочисленные фильтры. Тем более, что порой бывает глупо требовать от кандидата многолетнего опыта работы с каким-то программным обеспечением, если оно появилось на рынке лишь недавно.

В помощь кадровикам и начинающим безопасникам Международная ор-

ганизация социального труда (ISSA International) выпустила брошюру Cyber Security Career Lifecycle, которая описывает пять уровней карьеры в области ИБ. Любой человек, говорится в ней, не имеющий опыта работы в ИБ, при желании может освоить базовые методы и принципы кибербезопасности, прослушав необходимый курс обучения, и занять первый «Pre-Professional» уровень. В дальнейшем, с получением дополнительных опыта и образования, через 10+ лет специалист по ИБ может занять место в совете директоров компании или возглавить собственную организацию по киберзащите.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИЛИ БЕЗОПАСНОСТЬ ИНФОРМАЦИИ?

В апреле текущего года министр образования и науки РФ Ольга Васильева в рамках парламентских слушаний рассказала сенаторам о направлениях деятельности образовательных учреждений по обеспечению информационной безопасности детей. Она отметила, что навыки ИБ и поведения в сети интернет нужно прививать с детства. Для начальной школы

эти вопросы должны быть оформлены в федеральные образовательные стандарты, старшим ученикам необходимо преподавать курс на занятиях по информатике, праву, обществознанию и ОБЖ. Стоит обращать внимание школьников на правила безопасного обращения в информационном пространстве в рамках дополнительного образования во внеурочной деятельности. Данное направление должны преподавать специалисты и, конечно же, родители дома.

Однако, как и прежде, глава профильного ведомства сделала упор на разработку интернет-ресурсов для детей и безопасность информации для учащихся, а не на обучение школьников навыкам ИБ, как их понимают во всем мире.

* * *

Старая пословица гласит: «Наши дети — наше будущее». Учитывая сегодняшний уровень киберугроз, стоит принять хакерство как необходимый для детей навык, чтобы обеспечить достойный уровень национальной информационной безопасности в будущем.

ШИФРЫ ТРЕХ ВОЙН

О МАСТЕРЕ ВЗЛОМА КОДОВ
Б. А. АРОНСКОМ

(Окончание. Начало в № 2/2017 г.)

НА ПРЕПОДАВАТЕЛЬСКОЙ РАБОТЕ

После войны по существовавшему тогда положению о выслуге лет Б.А. Аронский был награжден вторым орденом Красного Знамени. Впоследствии он преподавал криптографию на курсах в Спецшколе и в Высшей школе криптографов ГУСС¹, которая была образована в 1949 году. С первых дней основания кафедры криптографии Борис Алексеевич был назначен на должность старшего преподавателя и внес большой вклад в дело становления криптографического образования в нашей стране.

Вот что вспоминал об этом Л.А. Кузьмин: «После войны Борис Алексеевич передавал свой опыт молодежи в стенах Высшей школы криптографов (теперь это Институт криптографии, связи и информатики Академии ФСБ России²), слушателем которой в 1951 году стал и я. Занятия Б.А. Аронского состояли в раскрытии целой тетради составленных им „перехваченных кодированных телеграмм послов некоего государства в европейских столицах“ (на русском языке, поскольку он был уверен, что другие языки нам пока неподвластны). Он подталкивал

¹ ГУСС — Главное управление специальной службы, образовано в 1949 году. Подробнее об этой организации можно прочитать в статье [Кузьмин, 1998–2].

² С 1991 года в Москве проводятся Олимпиады для школьников по математике и криптографии, в настоящее время их проведение организуют Академия криптографии Российской Федерации и Институт криптографии, связи и информатики Академии ФСБ России. Более подробную информацию об Олимпиадах можно получить из книги [Зубов, 2013] и на сайте [v-olymp].



Полковник Б.А. Аронский

нас к „легким местам“ этой переписки, мы постепенно надписывали карандашами над кодовыми знаками их смысловые эквиваленты и всё более уверенно находили всё новые и новые их продолжения. Скажу прямо — это было захватывающим занятием, по сравнению с которым разгадывание кроссвордов стоит несколькими „этажами“ ниже. Курс лекций заканчивался экзаменом, состоявшим в раскрытии „новой перехваченной“ кодо-телеграммы (у каждого своей). Так Борис Алексеевич наглядно проиллюстрировал технологию своего легендарного успеха времен начала войны.

Фактически же его задача в военные годы была значительно труднее, поскольку первичный кодовый текст в то время уже перешифровывался еще каким-либо шифром. Принципиальные возможности „снятия“ такой перешифровки составляли содержание его последующих лекций. Мне довелось после окончания Школы, в 1953–56 годах, работать с Борисом Алексеевичем в одной комнате и узнать из первых рук многие подробности его успехов военных лет, так что в достоверности вышесказанного у меня сомнений нет» [Кузьмин, 1998–1, с. 84]. Б.А. Аронский лично и в соавторстве с коллегами написал ряд учебных книг по криптографии, длительное время использовавшихся при подготовке советских криптографов.

В СПЕЦСЛУЖБЕ ВМФ

Как опытный специалист Б.А. Аронский часто направлялся на наиболее важные и трудные участки дешифровальной работы.



Дмитрий ЛАРИН
кандидат
технических наук



Геннадий ЕМЕЛЬЯНОВ
член-корреспондент
Академии криптографии РФ



Награжденные орденами и медалями сотрудники ГУСС. Б.А. Аронский в третьем ряду в центре

В 1954 году он был направлен в Специальную службу военно-морского флота, где и закончил военную службу в звании полковника в 1958 году.

Обаятельный и талантливый человек, неутомимый труженик, тонкий знаток поэзии и живописи, полиглот, любитель музыки и шахмат, — таким Борис Алексеевич запомнился коллегам, работавшим с ним. Б.А. Аронский скончался 15 февраля 1976 года и похоронен на Даниловском кладбище в Москве [Кузьмин, 1998–1], [Энциклопедия, 2004, с. 433].

ДЕШИФРОВАННЫЕ ТЕЛЕГРАММЫ

В заключение статьи приведем тексты ряда дешифрованных советскими криптографами немецких телеграмм.

ИЗ ДЕШИФРОВАННОЙ ПЕРЕПИСКИ ПОДРАЗДЕЛЕНИЙ 17-Й НЕМЕЦКОЙ АРМИИ

9 октября 1943 г.

К положению на Таманском полуострове. Отвод остатков войск из предмостного укрепления будет осуществляться под видом отхода на новые рубежи с целью обмануть противника, однако эти позиции заниматься не будут. Для того чтобы заставить противника терять время на атаку ложных рубежей, отходящие части совершат марш с линии обороны непосредственно к переправочным рубежам. Как линия обороны, так и ложный промежуточный рубеж защищены проволочным заграждением, концы которого заминированы с таким расчётом, что каждое прикосновение к проволоке вызывает взрыв мины. Перед последним оборонительным

рубежом и на всей его глубине будут установлены новые шестиствольные деревянные минные аппараты, которые в момент стрельбы самовзрываются. Прекращение боевых действий будет осуществлено по всему фронту одновременно; войска будут направлены к местам переправы, где будут подготовлены все переправочные средства, которыми располагает понтонный полк полковника Генке, с таким расчетом, чтобы все войска были переправлены одним рейсом. Для противодействия авиации противника ожидается прибытие 100 истребителей и 50 бомбардировщиков. В с. Коломка, что в 6 км северо-восточнее г. Керчи, установлена тяжёлая артиллерия, которая будет прикрывать отход арьергардов.

ЦА ФСБ России [Органы, 1995, том 4, книга 2].

ДЕШИФРОВКА ТЕЛЕГРАММЫ МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ ГЕРМАНИИ ГЕРМАНСКОМУ ПОСОЛЬСТВУ В БАНГКОКЕ

14 июля 1941 г.

Из Берлина в Бангкок германскому посольству. Циркулярная.

Для нас имеет большое значение текущая информация о положении в Москве, а если представляется возможным, и по всему Советскому Союзу. Наряду с военной информацией особенно интересными являются сообщения о положении в правительстве и партии, о настроении населения и отношении его к правительству, а также о состоянии снабжения.

Прошу использовать все возможности для получения подобных сведений и в случае успеха телеграфировать.

Вермахт. ЦА ФСБ России [Органы, 1995, том 2, книга 1].



Б.А. Аронский (слева) во время службы в ВМФ

**ДЕШИФРОВКА ТЕЛЕГРАММЫ № 1052
МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ ГЕРМАНИИ
ГЕРМАНСКОМУ ПОСОЛЬСТВУ В ЛИССАБОНЕ**

11 декабря 1941 г.

Из Берлина в Лиссабон германскому посольству. Весьма секретно. Циркулярная телеграмма. Военному атташе для информации. Восточный театр военных действий.

Наши операции 1941 г. в значительной степени ослаблены быстрым наступлением снежной зимы и холодного периода. Отдельные, ещё не законченные операции будут продолжены.

После больших побед в сентябре и октябре наши войска при сознательном напряжении всех сил достигли, преодолевая превосходящего как в живой, так и в материальной силе противника, цели, поставленной перед началом кампании.

У неприятеля отняты наиболее важные для вооруженных сил экономические и военные центры. Поставленная перед войсками задача — разгромить массу красных войск в глубине страны — в результате боёв этого года в значительной мере выполнена. Военная мощь противника сильно ослаблена превзошедшими все ожидания потерями в живой и материальной силе. Между тем цель — окончательно уничтожить военную мощь русских — стоит ещё на повестке дня.

Задачей германских войск зимой 1941/42 гг. будет охрана оккупированных областей путем создания фронта обороны с максимальной экономией сил, с тем, чтобы под его защитой усилить и освежить восточные войска для выполнения поставленной перед ними на весну 1942 г. задачи, а также произвести новое разделение оккупированных областей и их экономическое использование. Необходимое для этого планомерное отступление отдельных головных частей, продвинувшихся в результате наступления далеко вперед, уже частично проведено, например, у Ростова, частично начато восточнее Тулы, северо-западнее Москвы и у Тихвина.

Вражеская пропаганда попытается представить это отступление, которое при данных метеорологических условиях сопряжено с определенными потерями в материальной части (взрыв замерзших орудий и автомашин), как победу Крас-

ной Армии. Вы должны с сознанием своей силы энергично, но вежливо воспротивиться этому.

В особых случаях следует указать на то, что г. Москва, как таковая, большого значения для германского командования не имеет, что давление на Москву должно было лишь вынудить противника бросить в бой свои последние резервы. Эта цель достигнута. В упорных боях противнику нанесен большой урон. В результате германских атак Москва очищена, во-первых, как столица страны, от властей, во-вторых, от всей сравнительно важной военной промышленности. Результатом этого является нарушение работы вражеских административных и военных учреждений. У Ленинграда мы полностью достигли своей цели — отрезать Ленинград, употребив на это небольшое количество войск. Промышленные предприятия города продолжают планомерно уничтожаться огнём нашей артиллерии. Свирепствуют голод и заразные болезни.

Верховное командование армии, отдел атташе Крамарц, ЦА ФСБ России [Органы, 1995, том 2, книга 2].

ИЗ БЕРЛИНА В ТОКИО

19 января 1943 года

Германскому посольству

... в течение следующей недели в Германии будет производиться большая кампания с целью дальнейшей тотализации войны. Среди других мер предусмотрено введение трудовой повинности для мужчин в возрасте от 16 до 65 лет и для женщин — от 17 до 50 лет; закрываются промышленные и торговые предприятия, не имеющие военного значения, как например, склады, цветочные магазины; сокращаются всевозможные промысловые предприятия, учреждения и инстанции; распускаются организации, союзы и т.д., не имеющие значения для победы... [Органы, 1995, том 4, книга 1].

ИЗ АНКАРЫ № 247

13 июля 1941 года

... Задачи на разведку по Америке и Англии: состояние авиационной промышленности, расширение программы строительства, данные отдельных фирм. Продукцию давать в фактических цифрах, а не в процентах. Количество всего поставляемого военного имущества в Англию, важные новые изобретения, пеленгаторные приборы и детали американских поставок в Мидлест... [Органы, 1995, том 2, книга 2].

**СООБЩЕНИЕ НКВД-НКГБ СССР В ГКО
С ИЗЛОЖЕНИЕМ СОДЕРЖАНИЯ ТЕЛЕГРАММ,
ПЕРЕХВАЧЕННЫХ НА НЕМЕЦКИХ ЛИНИЯХ СВЯЗИ**

Не ранее 14 апреля 1944 года

Дешифровально-разведывательной службой НКВД-НКГБ СССР с осени 1941 года нерегулярно, а с весны 1942 года систематически фиксировался шифрованный радиообмен на немецких линиях связи София — Будапешт, София — Вена и др.

Пеленгацией радиопередатчика было установлено, что он находится в предместье г. Софии в Болгарии.

По смыслу перехваченной и дешифрованной переписки организационного характера было установлено, что она исходит от германского военно-воздушного атташата в Болгарии, сотрудники которого подписывали телеграммы кличкой «Клатт» (условное обозначение одного из подразделений военной разведки Абвер, занимавшееся сбором разведывательной информации об СССР, странах Восточной Европы, Турции и Ближнего Востока. «Бюро» было создано по личному распоряжению В. Канариса. Первоначально дислоцировалось в Софии — авт.), позднее — «Виго». Много телеграмм прошло также без подписи.

Содержание телеграмм касалось главным образом передвижения войск Красной Армии.

Было предпринято специальное изучение этих материалов с целью установления, во-первых, их соответствия действительности и, во-вторых, каналов, по которым эти сведения могли проникать в Софию.

Проверкой значительной части телеграмм этой категории через Генштаб Красной Армии установлено, что подавляющее большинство приведенных в телеграммах данных о частях Красной Армии и их передвижениях вовсе не соответствует действительности и является вымыслом.

Некоторые телеграммы являются повторением дезинформации, передаваемой с утверждения Разведывательного Управления Генштаба Красной Армии нашими радиостанциями, участвующими в радиоигре с немцами.

Некоторая, очень небольшая часть радиogramм общего характера о передвижениях войск без указания номеров частей и точных направлений при проверке оказалась похожей на правду.

Следует считать, что эти правдоподобные данные могли быть установлены немцами путем авиаразведки, перехвата радиотелеграфных и радиотелефонных линий низовой армейской связи и допросом военнопленных.

В настоящее время обмен шифрпереписки по указанным линиям продолжается, хотя по сравнению с прошлым временем значительно сократился.



Немецкий солдат за настройкой ранцевой УКВ-радиостанции пехоты



Немецкие связисты у КВ приемника Kw.E.a («Антон»)

Соответствие содержания перехваченных телеграмм действительности проверяется каждый раз Главным Управлением Контрразведки НКО «Смерш».

Конкретно в отношении радиотелеграмм, помещенных в сборнике 5-го Управления НКГБ СССР за 14 апреля 1944 года за № 5/1/2532, проверкой через Генштаб Красной Армии — тов. Антонова установлено:

1. Текст телеграммы:

12.04.1944 года. Радиogramма № 41. Из Софии в Будапешт. «Войска 2-го Балтийского фронта получили приказ на подготовку и проведение наступления в направлении Рига, а также на Остров и Псков».

Результаты проверки:

Войска 2-го Прибалтийского фронта действительно получали приказ о наступлении, но не 12 апреля, а 1 апреля. Глубина наступления до Риги не планировалась. Задача ставилась начать наступление 5–6 апреля, фактически оно начато 7 апреля.

Таким образом, радиogramма № 41 была послана через 5 дней после начала наступления.

2. Текст телеграммы:

12.04.1944 года. Радиogramма № 40. Из Софии в Будапешт. «Согласно донесениям за 12 марта из Калинина на участок фронта Невель-Великие Луки вылетели: 191-я дивизия ночных бомбардировщиков, 64-я отдельная истребительная бригада, 28 транспортных и 8 санитарных самолётов».

Результаты проверки:

Ни 191-й дивизии ночных бомбардировщиков, ни 64-й отдельной истребительной бригады в составе ВВС Красной Армии нет. 12 марта перебазирование нашей авиации из Калинина куда бы то ни было не производилось.

3. Текст телеграммы:

12.04.1944 года. Радиogramма № 35. Из Софии в Будапешт. «Части 271-й дивизии ночных бомбардировщиков, расположенные в Речице, получили приказ на подготовку к вылету на участок фронта Бобруйск, совместно с одной эскадрильей ночных истребителей, 27 штурмовиками и 20 дальними разведчиками».

Результаты проверки:

В составе ВВС Белорусского фронта имеется 271-я авиадивизия ночных бомбардировщиков, но она дислоцирована не в Речице и приказа на подготовку к перелёту не получала.

4. Текст телеграммы:

12.04.1944 года. Радиogramма № 42. Из Софии в Будапешт. «Из Кременец (северо-восточнее Львова) в Заложец отправляются: одна моторизованная бригада, 18-я противотанковая бригада, один моторизованный зенитный полк, две пехотных бригады, один полк минёров и два штурмовых саперных батальона».

Результаты проверки:

18-й противотанковой бригады в составе войск 1-го Украинского фронта нет. Из частей, расположенных в г. Кременец, ни одна в указываемый период никуда не перемещалась. Возможно, что было отмечено прохождение через Кременец танковых и мотострелковых частей Рыбалко, что по сроку совпадает.

Перехват указанных телеграмм НКГБ СССР и их проверка через Главное Управление Контрразведки НКО «Смерш» продолжается.

Народный комиссар внутренних дел СССР Берия

Народный комиссар государственной безопасности СССР комиссар госбезопасности 1-го ранга Меркулов. ЦА ФСБ России [Органы, 1995, том 5, книга 1].

Иногда из радиоперехвата вражеских сообщений выявлялись недостатки в организации ведения боевых действий советских войск. Например:

СООБЩЕНИЕ ГУКР «СМЕРШ» НКО СССР

**№ 193/А В ГКО И ГЕНШТАБ РККА ОБ
ОБНАРУЖЕНИИ ПРОТИВНИКОМ ПЕРЕГРУППИРОВКИ
НАШИХ ВОЙСК НА УЧАСТКЕ 39-Й АРМИИ
ВСЛЕДСТВИЕ НАРУШЕНИЯ ПРАВИЛ МАСКИРОВКИ**

7 августа 1943 г.

По сообщению УКР «Смерш» Калининского фронта, противник с воздуха обнаружил начавшуюся 25 июля сего года перегруппировку наших войск на участке 39-й армии.

Произошло это вследствие того, что передвижение войск происходило с нарушением маскировки. Во время движения, особенно в ночное время, раскладывались костры, автомашины двигались со светом, техника сосредотачивалась в большом количестве на открытой местности.

Обнаружив перегруппировку наших войск, авиация противника начиная с 27 июля сего года групповыми и эшелонированными налётами стала бомбить сосредоточение войск и техники на железнодорожной ст. Ломоносове и переднем крае, в то время как до этого налеты авиации противника на участке 39-й армии носили одиночный характер.

Кроме того, перехваты радиogramм противника за последние дни также дают основание полагать, что немцы обнаружили перегруппировку наших войск на участке 39-й армии.

26 июля сего года отдел «Смерш» 39-й армии о фактах демаскировки и беспорядках при перегруппировке войск доложил Военному совету армии, который принял необходимые меры к восстановлению порядка.

Начальник ГУКР «Смерш» НКО СССР Абакумов. ЦА ФСБ России [Органы, 1995, том 4, книга 2].

ЛИТЕРАТУРА

1. [Абросов, 2003] Абросов С.В. В небе Испании 1936–1939. М., 2003.
2. [Анин, 1996] Анин Б.А., Петрович А.И. Радиоспионаж. М., «Международные отношения», 1996.
3. [Болтунов, 2011] Болтунов М.Е. «Золотое ухо» военной разведки. М.: Вече 2011. //
4. [Бутырский, 2012] Бутырский Л.С., Ларин Д.А., Шанкин Г.П. Криптографический фронт Великой Отечественной. Монография. М.: Гелиос АРВ, 2012. 2 изд. исправл. и дополн. М. 2013.
5. [Гольев, 2008] Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008.
6. [Емельянов, 2016] Емельянов Г.В., Ларин Д.А. Рождение советской криптографии // Информационная безопасность банков, № 2 (21) 2016, с. 61–65, № 3 (22), 2016 с. 74–79.
7. [Зубов, 2013] Зубов А.Ю., Зязин А.В., Никонов Н.В., Рамоданов С.М., Фролов А.А. Олимпиады по криптографии и математике. М.: МЦНМО, 2013.
8. [Клепов, 2009] Клепов А. Информационное оружие Сталина // www.proza.ru/2009/06/17/949
9. [Кузьмин, 1998–1] Кузьмин Л.А. Не забывать своих героев // Защита информации. Конфидент № 1, 1998, с. 83–85.
10. [Кузьмин, 1998–2] Кузьмин Л.А. ГУСС — этап в развитии советской криптографии // Защита информации. Конфидент. № 4, 1998, с. 89–94.
11. [Ларин, 2008] Ларин Д.А., Шанкин Г.П. Криптографическая деятельность во время гражданской войны в Испании. // Защита информации. INSIDE. № 1, 2008, с. 62–64.
12. [Органы, 1995] Органы государственной безопасности СССР в Великой Отечественной войне 1941–1945. Сборник документов. М.: «Русь» 1995. Издание подготовлено в Академии ФСБ России. <http://mosohin.ru>
13. [Соболева, 2002] Соболева Т.А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.
14. [Энциклопедия, 2004] Энциклопедия секретных служб России. М.: Астрель, 2004.
15. [agentura] <http://www.agentura.ru>
16. [kosino] kosino-uhomski.vaonews.ru/2p=6155
17. [v-olymp] v-olymp.ru
18. [vif2ne] <http://vif2ne.ru>

ГЛАВНОЕ СОБЫТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ



infosecurity

RUSSIA

InfoSecurity Russia

БЕЗОПАСНОСТЬ. ИННОВАЦИИ. СООБЩЕСТВО

5817 профессиональных посетителей

3985 участников деловой программы

более 15 000 предварительно назначенных встреч

более 500 продуктов и решений, представленных в экспозиции

213 мероприятия на стендах экспонентов и в конференц-залах

196 спикеров из числа ведущих мировых и российских экспертов, выступающих в четырех параллельных конференционных потоках.

19–21
сентября
2017



Прием заявок на участие открыт:
www.infosecurityrussia.ru
Выставка обеспечивает максимальную
полезность визита для заказчика
и наивысший в России ROI
для экспонента

Groteck
Business Media



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

СТО ЛЕТ НАЗАД

ТРИУМФ И ТРАГЕДИЯ РАДИОРАЗВЕДКИ БАЛТИЙСКОГО ФЛОТА

(Окончание. Начало в № 2/2017 г.)

ПРОВЕРКА БОЕМ

8 июля 1915 г. на радиостанцию особого назначения (РОН) были переведены сотрудники МИД надворный советник Ю. Павлович и коллежский регистратор Б. Орлов. Эти назначения, существенно усилив дешифровальное бюро, оказались весьма своевременными: спустя всего несколько дней, в ходе начавшейся операции германского флота в Рижском заливе, РОН пришлось выдержать настоящий боевой экзамен.

«Благодаря работе дешифровального бюро разведке Балтийского флота удалось заблаговременно вскрыть подготовку к этой операции, определить ее сроки, а затем, по сути, контролировать весь ее ход, обеспечивая командо-

вание ценнейшей информацией о действиях противника. Специалисты РОН практически в реальном времени производили разбор шифрованного радиобмена германских кораблей. Содержание отдельных германских радиogramм оказывалось известно русскому командованию даже раньше, чем их получали фактические адресаты. По оценкам современников, РОН успешно выдержала эту „проверку боем“ и в полной мере оправдала возлагавшиеся на нее надежды» [7].

Не менее успешно действовала РОН и все последующие месяцы войны. В основе таких достижений лежало своевременное вскрытие новых шифров, вводимых в действие противником [8].

УСУГУБИЛИ...

Следует признать, что действия командования германским флотом по защите своей системы шифрования способствовали успехам русских дешифровальщиков. Компрометация шифрсистемы, связанная с потерей кодовых книг, усугублялась явно не достаточной периодичностью смены ключа (шифра простой замены). Однако «эта система шифрования просуществовала практически в неизменном виде вплоть до 1916 года» [1].

Здесь важно указать, что «командование Балтийского флота всячески стремилось сохранить в тайне работу РОН и ее дешифровального бюро. Все, связанное с шифрперехватом, легендировалось под агентурный источник» [6].

Когда же германское командование узнало, что «Сигнальные книги» «Мадгебурга» находятся в руках русских? Можно достоверно говорить о том, что уже в августе 1915 года оно располагало данной информацией. Источником сведений стал русский морской лётчик, попавший в плен 8 августа 1915 года. Согласно немецким публикациям, эта информация сразу была доведена до сведения немецкого командования [5].

«Реакция на такое сообщение была вялой и непонятной. Предпринятые немецкими специалистами шаги по защите своей радиосвязи были совершенно не убедительными... Важно подчеркнуть, что к этому времени дешифровальщики Балтийского флота уже успели приобрести большой опыт в обработке германского шифрперехвата, установили рабочие контакты и наладили плодотворное сотрудничество с дешифровальными службами МГШ,



Остров Оденсхольм, за морским проливом виден мыс Шпитгамн — место дислокации РОН

МИД, а также со своими английскими коллегами из «Комнаты 40». Это позволило им сравнительно легко парировать предпринятые германским командованием первоочередные шаги по защите своей шифрованной связи. Даже введение в действие в 1916 году нового сигнального кода не стало в сложившихся условиях большой проблемой для русских дешифровальщиков. Система германского шифрования не претерпела серьезных изменений, а при разработке нового сигнального кода были использованы, по сути, те же принципы и подходы, что и в «Сигнальной книге» 1913 года. Данное обстоятельство позволило подключенным к работе специалистам «чёрного кабинета» МИД относительно быстро воссоздать новый сигнальный код, используя представленные в их распоряжение материалы германского шифр-перехвата» [5].

НАГРАДЫ ОСОБОГО НАЗНАЧЕНИЯ

Особенно существенную помощь дешифровальному бюро РОН оказал один из ведущих криптографов МИД статский советник Э. К. Феттерлейн, заслуги которого перед радиоразведкой Балтийского флота были отмечены двумя орденами. Он прибыл на РОН 5 мая 1916 года и уже через три недели шифр был определен. Затем еще через три недели Э. К. Феттерлейн восстановил общий план кодовой книги и все ее 13 разделов. Благодаря самоотверженной работе и таланту этого специалиста, был разгадан смысл почти 15 тыс. буквенных сочетаний, которыми противник пользовался для описания и выполнения своих боевых задач. Все разделы книги были восстановлены до такой степени, что дешифровальщики успешно использовали её на практике как оригинальную. В дальнейшем содержание кодовой книги уточнялось на новом материале радиоперехвата [9].

Деятельность РОН весьма высоко оценивалась командованием флота. Свидетельством тому — неоднократные представления личного состава РОН к боевым наградам. Только за 1915 г. состоялось несколько награждений. Так, уже 29 апреля мичман В. И. Марков был награжден орденом

Св. Станислава 3 степени с мечами и бантом «за отличие, выразившееся в разборе неприятельского шифра». А 6 декабря орденами различного достоинства были награждены сразу несколько представителей РОН: В. П. Пржиленцкий, Д. П. Измалков, О. О. Проффен, Ю. Павлович и Б. Орлов. Здесь вместе указаны и военные моряки и сотрудники МИД, что лишний раз свидетельствует о неформальном единстве российских криптографов вне зависимости от их ведомственной принадлежности.

ЗАСЛУГИ НЕПЕНИНА

В 1916 году радиоразведку Балтийского флота обеспечивали уже 10 станций радиоперехвата и 10 радиопеленгаторных станций, расположенных на побережье. Радиограммы, перехваченные другими береговыми станциями, также поступали для дешифрования на РОН.

«Использование Российским флотом сил и средств радиоразведки на Балтийском море оказалось чрезвычайно эффективным в немалой степени благодаря начальнику Службы связи БФ А. И. Непенину, назначенному в 1916 г. на должность командующего Балтийским флотом. Высокий уровень использования результатов разведывательной деятельности на флоте подтверждается свидетельствами современников. «Зарубежные авторы отмечают, что Непенин до предела отточил способности исходя из сведений радиоразведки и дешифрования создавать полную картину перемещения вражеских кораблей, а по ней вскрывать намерения врага» [9].

СОЮЗНИКИ

«Помимо обеспечения отечественного флота балтийская радиоразведка добывала и ценные сведения для союзников. Например, русское морское командование неоднократно предупреждало англичан о готовившихся налетах немецкой авиации. В 1916 г. отечественная радиоразведка получила восторженный отзыв со стороны английского адмирала Р. Филлимора, лично ознакомившегося с ее работой. Надо отметить, что и британцы добросовестно делились с русским морским командованием своими открытиями и достижениями в области радиоразведки, а также



А. И. Непенин — организатор радиоразведки БФ

некоторыми ценными документами, попадавшими им в руки с захваченных немецких подводных лодок и иным путем» [9].

БАЛТИЙСКИЙ КОД

Добавим, что разведывательное отделение штаба флота контролировало соблюдение дисциплины радиосвязи и обеспечение стойкости шифров и кодов, используемых в каналах радиосвязи. Для этого использовался специальный дежурный по радио корабль. «Отступления от правил радиосвязи немедленно пресекались. Выход кораблей в эфир максимально сокращался. Кораблям выдавали шифровальные документы, действующие только на время одного похода. В целях проверки доступности противника к русским шифрам периодически практиковалась передача радиограмм, которые в случае их прочтения должны были вызывать определенные действия противника. Ни одна из таких проверок не имела последствий, что позволяло делать вывод о стойкости «Балтийского кода», составленного в 1915 г. И. И. Ренгартенем» [9].

НА ЧЕРНОМ МОРЕ

Необходимо отметить, что боевой опыт РОН был использован при организации аналогичного центра на Черном море в Севастополе. Создание центра было ускорено находкой на Черноморском флоте турецкой «Сигнальной книги». 21 марта 1915 года подорвался на Одесском минном заграждении и за-

тонул на мелководье турецкий крейсер «Меджидие». В конце мая крейсер был поднят и поставлен в док в Одессе, 30 мая 1915 года при целенаправленном поиске в командном помещении нашли «Сигнальную книгу», находившуюся в воде в течение 70 дней [10].

Специалистами МГШ практически сразу был раскрыт один из применявшихся в турецком флоте шифров, чему весьма способствовали грубые нарушения правил шифрпереписки. Все захваченные документы детально изучались в штабе командующего ЧФ. Выявлено «наличие германских радиотелеграфистов на турецких судах и широкое использование в радиопереговорах действующих в германском флоте документов по связи». Поэтому к анализу радиоперехвата привлекли специалистов из Службы связи Балтийского флота, направив их в Севастополь [10].

ВЫГОДА АНГЛИЧАН

Благодаря дешифровке немецких радиogramм на Балтике, а затем и турецких на Чёрном море русский флот был точно осведомлён о составе и действиях неприятельских сил.

Такое развитие получила «магдебургская» история в России. В союзных державах продолжение «магдебургской» истории оказалось не менее впечатляющим.

У немецкого флота было заведено каждый день по радио сообщать командованию точное положение каждого судна и представлять регулярные отчеты о передвижении в море. Таким образом, у «Комнаты 40» появилась возможность по дешифрованному радиоперехвату создать точную картину действий германского Флота Открытого Моря и, исходя из маршрутов кораблей, понять, где находятся минные поля и безопасные пути.

«Комната 40» извлекла огромную выгоду из широкого радиообмена между немецкими судами, а также из привычки немцев передавать сообщения всегда на полной мощности. Немецким флотом до 1917 года не было предпринято никаких попыток ограничить использование радиосвязи, а позже это было сделано только из опасений пеленгации, но не потому, что командование тревожила возможность дешифрования.

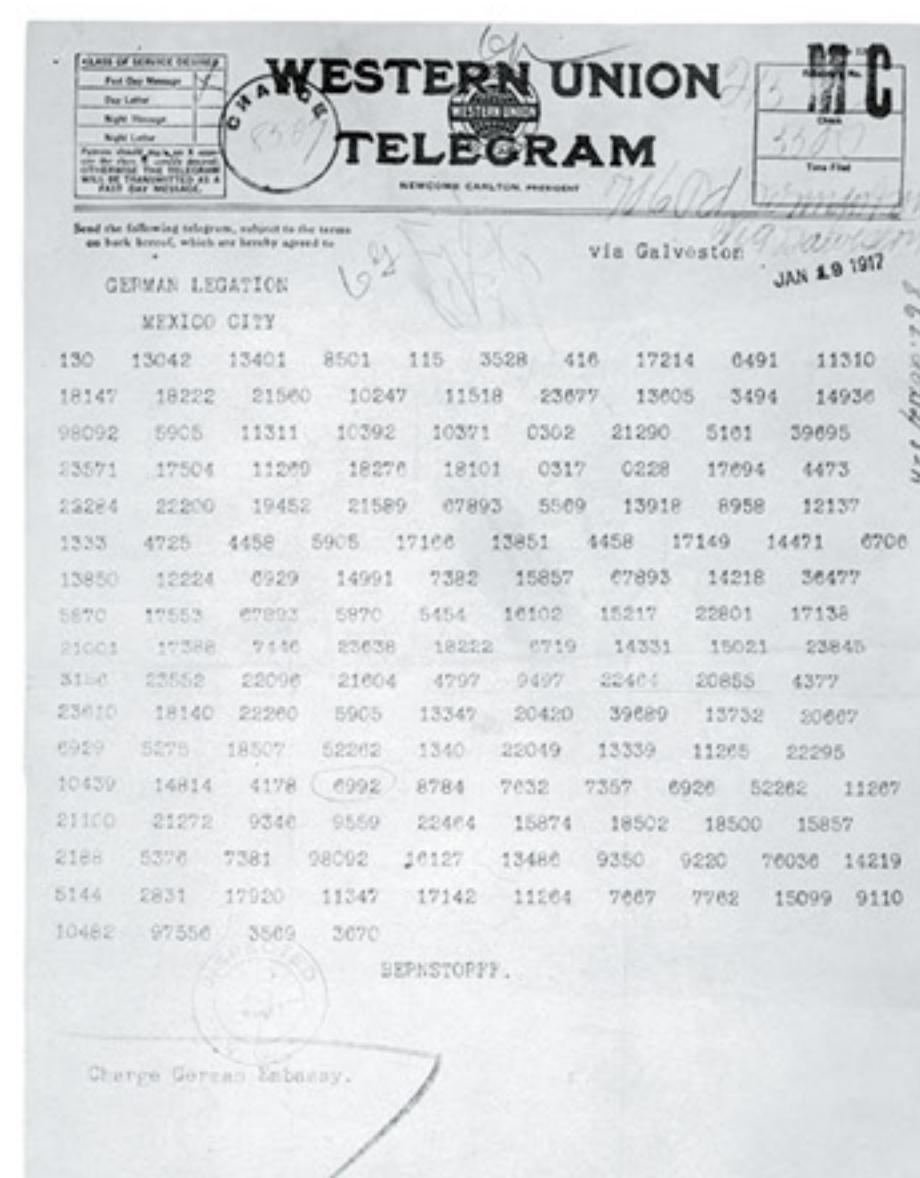
ТЕЛЕГРАММА ЦИММЕРМАНА

Всё же наиболее существенным вкладом «Комнаты 40» в военные усилия Великобритании стала дешифровка телеграммы А. Циммермана. На её основе британская разведка провела известную операцию, с помощью которой удалось втянуть США в Первую мировую войну. 16 января 1917 г. министр иностранных дел Германии А. Циммерман направил немецкому послу в Мехико телеграмму через Вашингтон, в которой сообщалось о грядущей неограниченной подводной войне и среди инструкций содержалась фраза о том, что если Мексика решит «вернуть себе утраченные владения в Техасе, Нью-Мексико и Аризоне», Германией это будет встречено с пониманием.

Телеграмма была передана в Вашингтон по телеграфу как дипломатическое сообщение через два нейтральных государства: Швецию и Соединённые Штаты. Ведь у Германии не было прямого телеграфного доступа к Американскому континенту, так как англичане перерубили трансатлантические кабели немцев и уничтожили их передающие станции в нейтральных странах. Но президент США В. Вильсон разрешил Германии использовать американский дипломатический канал связи. А. Циммерман надеялся, что англичане не смогут использовать перехваченное сообщение, не признав, что проверяют дипломатическую почту Соединённых Штатов. Телеграмма была перехвачена сразу после отправки и вскоре дешифрована.

По мнению У. Черчилля, в «Комнате 40» смогли дешифровывать телеграмму, благодаря захваченным кодовым книгам, в частности, на «Магдебурге». Но перед Британией стояло две проблемы: нужно было объяснить американцам, как была получена телеграмма, не раскрыв при этом, что британская разведка контролирует дипломатическую почту нейтральных стран; и предстояло публично объяснить появление расшифрованного текста таким образом, чтобы Германия не заподозрила, что её шифр был взломан.

Обе проблемы были благополучно решены и 20 февраля 1917 года дешифрованная телеграмма была доведена до сведения американского посла



Телеграмма Циммермана

в Лондоне, о чём тот доложил президенту США. Телеграмму опубликовали 1 марта, не разглашая информации об источнике. Её подлинность неожиданно подтвердил сам А. Циммерман. 2 апреля 1917 г. В. Вильсон поставил перед Конгрессом вопрос об объявлении войны Германии. 6 апреля Конгресс дал согласие и Соединённые Штаты вступили в Первую мировую войну на стороне Антанты.

УДАЧИ НЕМЦЕВ

Морских криптоаналитиков Германии, случалось, удача тоже баловала кодовыми книгами противника. Дважды в руки немецких дешифровальщиков попадали военно-морские коды Великобритании, но воспользоваться ими должным образом не удалось: англичане быстро узнавали о компрометации и заменяли коды.

Во время Первой мировой войны немцы смогли снимать и дешифровывать информацию с подводного кабеля связи США — Англия, используя при этом подводные лодки и решив технически сложные проблемы.

ПОБЕДА АНТАНТЫ

В целом следует признать, что на криптографическом фронте морской войны 1914–1918 годов Антанта безусловно одержала победу. В этом достижении велик вклад радиоразведчиков и криптографов Балтийского флота и МИД России, сумевших создать и раз-

вить общий с союзниками успех, начавшийся с «магдебургской» истории. Деятельность РОН и отлаженного механизма эффективной реализации её результатов стала яркой и впечатляющей демонстрацией возможностей и места криптографии в военном противостоянии.

РЕВОЛЮЦИЯ ИЗМЕНИЛА ХОД СОБЫТИЙ

Но российским морякам и криптографам, как мы знаем, не довелось разделить с союзниками радость окончательной победы. Революция сурово изменила ход событий, приближавших долгожданный победный итог. 4 (17) марта 1917 года был смещён «революционными матросами» и убит на базе флота в Гельсингфорсе командующий БФ адмирал А. И. Непенин. Всего в первые дни «бескровной» Февральской революции Балтийский флот потерял до 100 офицеров. После заключения Брестского мира с Германией и предоставления независимости Латвии, Эстонии и Финляндии радиоразведывательная служба Балтийского флота прекратила своё существование как система. В январе 1920 года не стало И. И. Ренгартена. Ещё раньше погибли или вынужденно эмигрировали многие его сослуживцы, спасая свои семьи и не желая участвовать в братоубийстве.

Уже во время Гражданской войны руководители Советского государства были вынуждены налаживать разорённое криптографическое хозяйство. Исследователь истории российской радиоразведки В. Г. Кикнадзе обоснованно предложил считать временной промежуток 1918–1940 годов периодом восстановления и развития отечественной радиоразведки [9]. Вероятно, подобный взгляд справедлив и для других направлений криптографической деятельности. Как мы теперь знаем, отечественной криптографической службе предстояло пройти долгий и сложный период восстановления и развития, прежде чем в условиях свершившихся революционных перемен в государстве и новой эпохи криптографии шифровальных машин советские криптографы смогли заявить о себе так же достойно, как это удалось их предшественникам в годы Первой мировой войны.

КУРГАН ПАМЯТИ

Закончим очерк строками, написанными известным литератором Николаем Андреевичем Черкашиным («Адмиралы мятежных флотов», М., 2003) по давним впечатлениям от посещения мыса Шпитгамн. Точнее, мыса Пыласапеа, так по-эстонски переменили шведское название.

«Где-то вдаль темнели утёсы Оденсхольма (ныне Осмусаар) — того са-

мого острова, у подножия которого и сейчас ещё ржавеют останки крейсера „Магдебург“. Посреди просторной поляны между лесом и морем был насыпан холм, а на холме всюду пахла небо антенна-качалка радиолокационной станции дальнего воздушного обнаружения. Шпитгамн — эта эфирная гавань, заложенная Непениным, — существовал, жил, действовал!.. Правда, задачи у него были несколько иными, но ведь на том же самом антенном поле, где тралили эфир мачты секретного центра радиоразведки русского флота, выставил свои ажурные параболы и радиолокационный дозор ПВО страны.

— Здесь поразительное по своим радиофизическим свойствам место, — сказал командир радиолокационной роты капитан Богданов, который и слыхом не слыхивал об адмирале Непенине и, тем не менее, отдал должное его выбору.

Итак, посреди старого антенного поля был насыпан новый подантенный холм. Поросший травой, он походил на те курганы, которые насыпали древние над могилами вождей или в память больших событий. Пусть же и эта шпитгамнская радиогорка станет курганом памяти адмирала А. И. Непенина (а также И. И. Ренгартена и их соратников — радиоразведчиков и криптографов Балтики — Б. С.)».

ЛИТЕРАТУРА

1. Партала М. А. Рифы и мифы острова Оденсхольм // Защита информации. Инсайд. 2007. № 1.
2. Соболева Т. А. История шифровального дела в России. М., 2002. С. 281–282.
3. Кан Д. Война кодов и шифров. М., 2004.
4. Ежов М. Ю. Один из мифов о крейсере «Магдебург» // Вопросы истории. 2007. № 2.
5. Партала М. А. «Магдебургская» история — «работа над ошибками» // Защита информации. Инсайд. 2014. № 2.
6. Партала М. А., Симонов Д. Н. Радиоразведка русского императорского флота на Балтийском море: история создания // Защита информации. Инсайд. 2005. № 1.
7. Партала М. А. Радиостанция особого назначения на мысе Шпитгамн (1915–1917) и её место в истории радиоразведки Балтийского флота // Санкт-Петербург и страны Северной Европы: Материалы седьмой международной научной конференции — СПб.: РХГА, 2006.
8. Партала М. А. Радиоразведка Балтийского флота в Первую мировую войну (к истории создания) // Санкт-Петербург и страны Северной Европы: Материалы шестой международной научной конференции — СПб.: РХГА, 2005.
9. 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.
10. Партала М. А. «Сигнальная книга» с турецкого крейсера «Меджидие» // Защита информации. Инсайд. 2007. № 5.

ОБЕЗЛИЧИВАНИЕ: КОЛИЧЕСТВО УБИВАЕТ КАЧЕСТВО...

ЭССЕ НА ТЕМУ ФЗ-54
И ОБЕЗЛИЧИВАНИЯ
ФИСКАЛЬНЫХ ДАННЫХ

*Помните, не всегда то,
что вы хотите,
действительно вам нужно.
Далай Лама*

Новая редакция ФЗ-54 открыла широчайшие возможности не только для фискального контроля в режиме on-line, но и для аналитических исследований движения товаров и услуг. Это просто кладезь для маркетинговых структур! То, что раньше делалось путем опросов и полулегального сбора информации, теперь можно делать на вполне легальной основе. Правда не всем и не всегда.

Здесь, как всегда, встает проблема баланса интересов. Что русскому здорово, то немцу — смерть, гласит русская поговорка. Многие из того, что можно «вытянуть» из обработки фискальных данных, может составлять коммерческую тайну, которую совсем не хочется отдавать конкуренту, но с другой стороны, эта информация может позволить правильно распределить товарные потоки. Преимущества в анализе такой информации законом отданы операторам фискальных данных. И на них лежит особая ответственность по сохранению коммерческих секретов и по удовлетворению потребностей в важной информации. Можно ли эту дилемму решить? Можно! Закон предполагает, что фискальные данные можно обрабатывать в аналитических целях, но в обезличенном виде (чтобы соблюсти баланс интересов). Одна проблема, в федеральном законе, определяющем по-

рядок применения ККТ, введено понятие «обезличивание фискальных данных»¹. Однако, четкого определения процесса их обезличивания — нет. Вот и давайте попробуем разобраться в этой коллизии.

ОПРЕДЕЛЕНИЕ ОБЕЗЛИЧИВАНИЯ ФИСКАЛЬНЫХ ДАННЫХ

Понятие «обезличенный» имеет свое общепризнанное содержание: обезличенный — не закрепленный за определенным владельцем, такой, который может принадлежать любому, имеющему на это право. Это понятие закрепляется словарями русского языка. Так, согласно Толкового словаря Т. Ф. Ефремовой, обезличивать — делать безличным; лишать своеобразие, самостоятельности либо ставить в условия, при которых никто не несет личной ответственности за дело². В словаре Даля указано: обезличивать — устранить или скрыть всякую личность, лицо, не называть людей, говорить в общих словах³.

Следовательно, обезличенные данные — это информация, не относящаяся прямо или косвенно к конкретному субъекту.

Процесс обезличивания фискальных данных не имеет законодательного регулирования. Вместе с тем, согласно части 1 ст. 6 ГК РФ, в случаях, когда отношения прямо не урегулированы законодательством, к таким отношениям, если это не противоречит их существу, применяется гражданское законодательство, регулирующее сходные отношения (аналогия зако-

на). Вопрос об аналогии возникает при пробелах, то есть для разрешения ситуаций, когда отношение требует гражданско-правового регулирования в условиях отсутствия нормы законодательства. В этом случае образовавшийся в процессе правового регулирования пробел может быть устранен нормой гражданского законодательства, регулирующей сходное отношение. Аналогия закона — признанный законом регулятор гражданских отношений, при этом процесс правового регулирования здесь обеспечивает именно норма законодательства, а потому и регулирование является нормативным.

В данном случае целесообразно рассмотреть возможность применения установленных законом норм права, регулирующих отношения при обезличивании персональных данных (аналогия закона). Так, федеральным законом установлено, что: «обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных»⁴. Данная дефиниция полностью соответствует общепринятому понятию, конкретизируя его применительно к персональным данным.

Аналогичное определение содержится и в методических рекомендациях Роскомнадзора, изданных в развитие требований федерального законодательства: «обезличенные данные — это данные, хранимые в информационных



Сергей ВИХОРЕВ
директор
по информационной
безопасности Филиала
ООО «ПЕТЕР-СЕРВИС
Спецтехнологии»

системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации»⁵.

Трансформируя это понятие, закрепленное законодательно, к рассматриваемой сфере деятельности оператора фискальных данных, можно сформулировать следующие определения:

Обезличивание фискальных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить их принадлежность конкретному субъекту налогообложения (налогоплательщику).

Обезличенные данные — это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту налогообложения (налогоплательщику) невозможно определить без дополнительной информации.

Необходимо отметить, что процедура обезличивания — это специфическая форма обработки фискальных данных в результате которой данные теряют свою принадлежность к фискальным данным, что приводит к снижению требований по защите данных, полученных в результате обезличивания.

Отметим, что налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике⁶. Если после проведения процедуры обезличивания фискальных данных становится невозможным отнести эти данные к конкретному налогоплательщику, то они, по нашему мнению, уже не являются налоговой тайной и не подлежат регулированию нормами НК РФ.

ИДЕНТИФИКАЦИОННАЯ СОСТАВЛЯЮЩАЯ ФИСКАЛЬНЫХ ДАННЫХ

Как следует из полученного определения, для обезличивания фискальных данных необходимо изъять из них те данные, которые позволяют однозначно привязать их к субъекту налогообложения (налогоплательщику) — идентификационные данные.



Согласно закону, фискальные данные — сведения о расчетах, в том числе сведения об организации или индивидуальном предпринимателе, осуществляющих расчеты, о контрольно-кассовой технике, применяемой при осуществлении расчетов, и иные сведения, сформированные контрольно-кассовой техникой или оператором фискальных данных. Такие данные представляются по установленным форматам в виде кассового чека, бланка строгой отчетности и (или) иного документа, предусмотренного законодательством⁷.

Законом предусмотрено, что кассовый чек и бланк строгой отчетности содержат следующие данные⁸:

- ◆ наименование документа;
- ◆ порядковый номер за смену;
- ◆ дата, время и место (адрес) осуществления расчета;
- ◆ наименование организации-пользователя или фамилия, имя, отчество ИП;
- ◆ идентификационный номер налогоплательщика пользователя;
- ◆ применяемая при расчете система налогообложения;
- ◆ признак расчета (приход, возврат прихода, расход, возврат расхода);

◆ наименование товаров, работ, услуг, платежа, выплаты, их количество, цена за единицу с учетом скидок и наценок, стоимость с учетом скидок и наценок, с указанием ставки налога на добавленную стоимость;

◆ сумма расчета с отдельным указанием ставок и сумм налога на добавленную стоимость по этим ставкам;

◆ форма расчета (наличные денежные средства и (или) электронные средства платежа), а также сумма оплаты наличными денежными средствами и (или) электронными средствами платежа;

◆ должность и фамилия лица, осуществившего расчет с покупателем (клиентом);

◆ регистрационный номер контрольно-кассовой техники;

◆ заводской номер экземпляра модели фискального накопителя;

◆ фискальный признак документа;

◆ адрес сайта уполномоченного органа в сети Интернет, на котором может быть осуществлена проверка факта записи этого расчета и подлинности фискального признака;

◆ абонентский номер либо адрес электронной почты покупателя (клиента) в случае передачи ему кассово-

КАТЕГОРИЯ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ ВЕСЬМА БЛИЗКА КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ТАК КАК ИМЕННО ЭТА КАТЕГОРИЯ СВЕДЕНИЙ ПОЗВОЛЯЕТ ОДНОЗНАЧНО ОПРЕДЕЛИТЬ СУБЪЕКТА ИЛИ ОТНОСИТСЯ К ОПРЕДЕЛЯЕМОМУ СУБЪЕКТУ

го чека или бланка строгой отчетности в электронной форме;

- ♦ адрес электронной почты отправителя кассового чека или бланка строгой отчетности в электронной форме в случае передачи покупателю (клиенту) кассового чека или бланка строгой отчетности в электронной форме;

- ♦ порядковый номер фискального документа;

- ♦ номер смены;

- ♦ фискальный признак сообщения.

Категория идентификационных данных весьма близка категории персональных данных, так как именно эта категория сведений позволяет однозначно определить субъекта или относится к определяемому субъекту. При этом, оценку состава фискальных данных необходимо проводить расширительно, учитывая возможность идентификации не только субъекта персональных данных, но и юридического лица — субъекта налогообложения. Анализ показывает, что каким-либо образом определить (идентифицировать) субъекта налогообложения (налогоплательщика) возможно используя следующие сведения, содержащиеся в фискальном документе:

- ♦ место (адрес) осуществления расчета;

- ♦ наименование организации-пользователя или фамилия, имя, отчество ИП;

- ♦ идентификационный номер налогоплательщика пользователя;

- ♦ должность и фамилия лица, осуществившего расчет с покупателем (клиентом);

- ♦ абонентский номер либо адрес электронной почты покупателя (клиента);

- ♦ адрес электронной почты отправителя кассового чека (бланка строгой отчетности).

Использование иной информации, содержащейся в фискальном документе, не позволяет определить принадлежность к конкретному субъекту налогообложения. Таким образом, указанные выше сведения, содержащиеся в фискальном документе, могут быть отнесены к идентификационным фискальным данным.

Следовательно, для обезличивания данных достаточно исключить идентификационные фискальные данные из общей базы фискальных данных.

ФОРМЫ И МЕТОДЫ ОБЕЗЛИЧИВАНИЯ ФИСКАЛЬНЫХ ДАННЫХ

В данном случае возможно использовать методический аппарат обезличивания, изложенный в действующих рекомендациях Роскомнадзора⁹. Согласно этому документу, возможны две основные формы обезличивания:

- ♦ обезличивание абсолютное, когда невозможно провести восстановление исходной информации (деобезличивание) и фискальные данные, как таковые, теряются;

- ♦ обезличивание обратимое, когда возможно, при определенных условиях, провести восстановление исходной информации (деобезличивание) и возможно восстановление фискальных данных.

При обратимом обезличивании необходимо обеспечить требуемый уровень анонимности полученных данных — невозможности однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации, в том числе с использованием дополнительных данных о субъектах налогообложения (налого-

плательщиках), полученных из других источников.

Наиболее перспективными и удобными для практического применения методами обезличивания фискальных данных могут быть:

- ♦ метод введения идентификаторов (замена части сведений (значений фискальных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

- ♦ метод изменения состава или семантики (изменение состава или семантики фискальных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

- ♦ метод декомпозиции (разбиение множества (массива) фискальных данных на несколько подмножеств (частей) с последующим отдельным хранением подмножеств).

Проведя анализ рекомендаций Роскомнадзора в части массива данных, передаваемых налогоплательщиком оператору фискальных данных, одним из методов обезличивания может быть метод изменения состава или семантики, в рамках которого часть особо чувствительных реквизитов удаляется, а для ряда других применяется обобщение, обеспечивающее невозможность однозначной идентификации налогоплательщика при сохранении возможности статистической обработки. Предложения по применению метода обезличивания представлены в табл. 1.

ОБЕЗЛИЧИВАНИЕ ФИСКАЛЬНЫХ ДАННЫХ У ОПЕРАТОРА ФИСКАЛЬНЫХ ДАННЫХ

Обработкой фискальных данных согласно закону признается любое действие (любая операция) или совокупность действий (операций), совершаемых оператором фискальных данных с применением технических средств оператора фискальных данных при формировании и (или) использовании базы фискальных данных, включая получение, проверку достоверности, сбор, запись, систематизацию, накопление, хранение в некорректируемом виде, извлечение, использование, передачу

Реквизит	Результат при обезличивании
Наименование документа	Сохраняется неизменным
Порядковый номер за смену	Сохраняется неизменным
Дата, время осуществления расчета	Сохраняется неизменным
Место (адрес) осуществления расчета	Из иерархии адресной информации исключаются сведения о номерах домов, строений, земельных участков, после чего полученный результат проверяется на наличие уникальных записей. При обнаружении уникальных значений адресные атрибуты заменяются объектами территориального деления более высокого порядка. Например, в случае уникальности значения «г. Москва, проектируемый проезд № 5678» значение заменяется на «г. Москва, район Очаково-Матвеевское»
Наименование организации-пользователя или фамилия, имя, отчество ИП	Исключается
Идентификационный номер налогоплательщика пользователя	Исключается
Применяемая при расчете система налогообложения	Исключается
Признак расчета (приход, возврат прихода, расход, возврат расхода)	Сохраняется неизменным
Наименование товаров, работ, услуг, платежа, выплаты, их количество, цена за единицу с учетом скидок и наценок, стоимость с учетом скидок и наценок, с указанием ставки налога на добавленную стоимость	Сохраняется неизменным
Сумма расчета с отдельным указанием ставок и сумм налога на добавленную стоимость по этим ставкам	Сохраняется неизменным
Форма расчета (наличные денежные средства и (или) электронные средства платежа), а также сумма оплаты наличными денежными средствами и (или) электронными средствами платежа	Сохраняется неизменным
Должность и фамилия лица, осуществившего расчет с покупателем (клиентом)	Исключается
Регистрационный номер контрольно-кассовой техники	Исключается
Заводской номер экземпляра модели фискального накопителя	Исключается
Фискальный признак документа	Исключается
Адрес сайта уполномоченного органа в сети Интернет, на котором может быть осуществлена проверка факта Записи этого расчета и подлинности фискального признака	Сохраняется неизменным
Абонентский номер покупателя (клиента) в случае передачи ему кассового чека или бланка строгой отчетности в электронной форме	Маскируется путем замены 4 и более цифр на символы *, например, 9261****36 или 7*****0536
Либо адрес электронной почты покупателя (клиента) в случае передачи ему кассового чека или бланка строгой отчетности в электронной форме	Исключается или маскируется
Адрес электронной почты отправителя кассового чека или бланка строгой отчетности в электронной форме в случае передачи покупателю (клиенту) кассового чека или бланка строгой отчетности в электронной форме	Сохраняется неизменным
Порядковый номер фискального документа	Сохраняется неизменным
Номер смены	Сохраняется неизменным
Фискальный признак сообщения	Исключается

Таблица 1. Предложения по применению метода обезличивания

в адрес налоговых органов в виде фискальных документов, предоставление налоговым органам таких данных и доступа к ним¹⁰.

Вместе с тем, закон также предоставляет оператору фискальных данных право осуществлять обработку фискальных данных в статистических или иных исследовательских целях при ус-

ловии обязательного обезличивания таких фискальных данных¹¹.

Таким образом, в деятельности оператора фискальных данных можно выделить два самостоятельных бизнес-процесса обработки фискальных данных:

(I) при формировании и (или) использовании базы фискальных данных;

(II) в статистических или иных исследовательских целях.

В случае (I) закон требует от оператора фискальных данных осуществлять обработку фискальных данных в режиме реального времени, а также обеспечивать запись в некорректируемом виде фискальных данных, в том числе в виде фискальных доку-

ментов, а также их хранение в течение пяти лет с даты их записи¹². В данном случае обработка фискальных данных, в том числе и ее хранение в базах данных, осуществляется без обезличивания, что необходимо для решения задач, определенных законом перед оператором фискальных данных. Законом напрямую запрещается уничтожение, удаление, блокирование, модификация (корректировка), обезличивание фискальных данных, записанных в базе фискальных данных¹³. Сторонами правоотношений в этом случае выступают владелец ККТ, оператор фискальных данных и налоговые органы.

В случае (II) оператор фискальных данных самостоятельно принимает решение о необходимости проведения статистических и иных исследований и формирования на их основе вторичной информации. При этом, согласно требованиям закона, вторичная информация может быть получена только с использованием обезличенных фискальных данных. Такая вторичная информация может использоваться оператором фискальных данных для предоставления различных сервисов любым заинтересованным субъектам,

так как не является фискальными данными. Сторонами правоотношений в данном случае являются оператор фискальных данных и любое заинтересованное в получении вторичной информации лицо.

Таким образом, анализ дефиниций Федерального закон № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа» показывает, что процесс обезличивания фискальных данных не затрагивает действия (операции) оператора фискальных данных с применением технических средств при формировании и (или) использовании базы фискальных данных, включая получение, проверку достоверности, сбор, запись, систематизацию, накопление, хранение в некорректируемом виде, извлечение, использование, передачу в адрес налоговых органов в виде фискальных документов, предоставление налоговым органам таких данных и доступа к ним, и распространяется только на действия (операции) оператора фискальных данных с применением технических средств при формировании

вторичной информации на основе статистической обработки или иных исследований.

Необходимо также отметить, что организация или индивидуальный предприниматель, применяющие контрольно-кассовую технику при осуществлении расчетов (пользователь¹⁴), как лицо, самостоятельно создавшее информацию (фискальные данные), является обладателем этой информации¹⁵ и, в силу закона, имеет право разрешать или ограничивать доступ к такой информации, определять порядок и условия такого доступа, использовать информацию, в том числе распространять ее, по своему усмотрению, передавать информацию другим лицам по договору или на ином установленном законом основании, осуществлять иные действия с информацией или разрешать осуществление таких действий¹⁶.

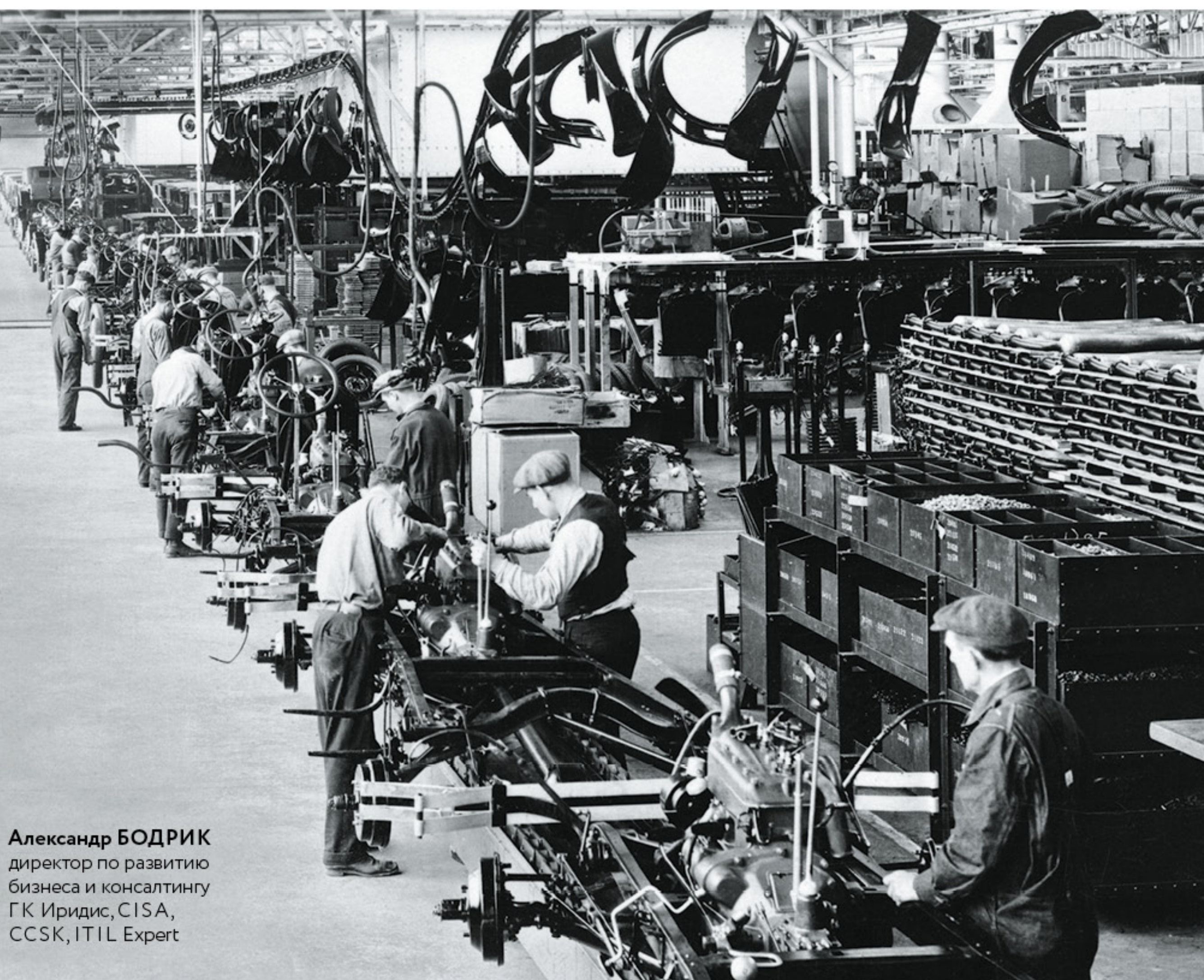
Из этого следует, что владелец ККТ (пользователь) вправе дать распоряжение оператору фискальных данных передать фискальные данные или часть этих данных, в том числе и в неизменном виде, сформированные с применением принадлежащей ему ККТ, любому третьему лицу на условиях, установленных им.

ЛИТЕРАТУРА

1. Федеральный закон № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа», часть 9 ст. 4.1
2. Толковый словарь Ефремовой. Т.Ф. Ефремова. 2000
3. Толковый словарь живого великорусского языка: в 4 т. / авт.— сост. В.И. Даль, 2-е изд., СПб.: Типография М.О. Вольфа, 1880–1882
4. Федеральный закон № 152 «О персональных данных», ст. 3, п. 9
5. Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (Утв. Руководителем Роскомнадзора А.А. Жаровым 13.12.2013 г.)
6. НК РФ, ст. 102
7. Федеральный закон № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа», ст. 1.1
8. Федеральный закон № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа», часть 1 ст. 4.7
9. Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».
10. Федеральный закон № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа», ст. 1.1
11. Федеральный закон № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа», часть 9 ст. 4.1
12. Федеральный закон № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа», часть 2 ст. 4.5
13. Федеральный закон № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа», часть 9 ст. 4.1
14. Федеральный закон № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа», ст. 1.1
15. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ст. 2 п. 5
16. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», часть 3 ст. 6



Александр БОДРИК
директор по развитию
бизнеса и консалтингу
ГК Иридис, CISA,
CCSK, ITIL Expert



КОНВЕЙЕР КИБЕРБЕЗОПАСНОСТИ ДЛЯ 200 ИТ-ПРОЕКТОВ В ГОД

ЗАМЕТКИ БЕЗОПАСНИКА

ИТ, ИБ и бизнес обычно разделяют не так много тезисов, но один мы вспоминаем практически всегда: кибербезопасность должна быть экономически эффективной! И дальше: максимальная эффективность возможна лишь при «встроенной» кибербезопасности, когда риски и контроли кибербезопасности анализируются, адаптируются и реализуются как часть архитектуры еще до перевода разрабатываемых или внедряемых систем в production — до загрузки бизнес-данных и начала предоставления сервисов пользователям системы.

Однако встраивание кибербезопасности в ИТ-проекты потребует встраивания конвейера контроля и разработки архитектуры безопасности ИТ-проектов, иначе или ИТ-проекты затормозят (в отдельных крупных организациях очередь ИТ-проектов на контроль достигает полугода) и бизнес недополучит прибыль, или безопасность из проектов выбросят, чтобы не мешала трансформировать бизнес.

Несколько лет назад, работая в центре компетенции ИБ нефтегазовой корпорации, я построил конвейер контроля кибербезопасности для ИТ-проектов, и добился приличных даже по се-

годняшним меркам результатов: SLA отклика на запрос на проверку — 8 рабочих часов, SLA проверки — 3 дня, SLA отклика на запрос по осмечиванию архитектурного участия — 4 часа и отсутствие претензий по всем проектам с архитектурным участием. При этом на поток в 200 проектов приходилось всего 2 человека на функцию контроля, а функция разработки архитектуры была распределена по проектам и не создавала нагрузки на бюджет блока безопасности компании.

После этого я стал обращать внимание, как строят подобные конвейеры коллеги в других компаниях, информа-

ция накапливалась, ко мне стали обращаться за консультациями, и я решил формализовать этот опыт, изложив его в кратком виде.

КОНТЕКСТ

Существенным компонентом успеха любого проекта всегда будет среда, в которой он реализуется. В моем конкретном случае компания была крупной, с развитыми бизнес-процессами, а значит существовал ряд значимых предпосылок:

1. Контрольные точки. По всему циклу реализации ИТ-проектов уже было 2 контрольные точки — без согласования CISO было невозможно утвердить архитектурный план системы, а также сдать систему в промышленную эксплуатацию. Помогало то, что в моем ведении находился сервис контроля ИТ-изменений, а значит, без согласованной документации не открывались сетевые порты. Обойти контрольные точки кибербезопасности было тяжело — потребовались бы де-факто усилия уровня Исполнительного директора — члена правления (одного из акционеров).

2. Владение активами и P&L-ответственность. В компании была внедрена концепция владения ИТ-активами бизнес-подразделениями, и те уже привыкли что именно они отвечают за состояние своих активов, в том числе и за принятие и финансирование решений по обеспечению их кибербезопасности.

3. Централизованные интерфейсы в ИТ. Компания реализовывала

большую часть проектов централизованно, имела коммуникационные инструменты для донесения позиции кибербезопасности на все уровни проектной деятельности — спонсоры, ИТ-директора бизнес-направлений (Upstream, Downstream, Finance, Services), руководители проектов — все, кто выступал представителем внутренних клиентов и бюджетировал участие безопасности на стадии создания архитектуры.

4. Компетентность персонала. Создающая конвейер группа службы кибербезопасности была опытной (8+ лет), она хорошо понимала корпоративные процессы, предметную область ИБ и, в частности, лучшие практики по созданию масштабируемых процессов ИБ.

НАШИ ДЕЙСТВИЯ НА СТАРТОВОМ ЭТАПЕ

Мы начали с создания основы — списка требований безопасности к ИТ-проектам. Такой чек-лист стал де-факто стандартом качества операционного контроля, позволил нормировать трудозатраты на контроль и обещать руководителям проектов и бизнес-заказчикам средние сроки рассмотрения документов.

Естественно, мы не ограничились чек-листом. Проверка также включала в себя анализ рисков, который выполнялся тем тщательнее, чем понятнее были драйверы риска кибербезопасности. Например, доступность из сети Интернет и автоматизация критично-

го процесса (движение углеводородов, «цифровое месторождение», закупки и МТО, финансовые процессы и т.п.).

По итогам проверки архитектурного плана каждый проект получал требования к безопасности и должен был их реализовать. Для критичных систем требования могли включать тест на проникновение либо аудит фрод-рисков. Для решения этих задач привлекалась внешняя экспертная компания, но иногда делали и сами. Для входящих в контур формирования финансовой отчетности т.н. материальных систем к проверке привлекались специалисты Департамента внутреннего контроля — чтобы удостовериться в правильном формировании матрицы доступа, корректной идентификации и управлении риском конфликта полномочий (SoD — Segregation of Duties).

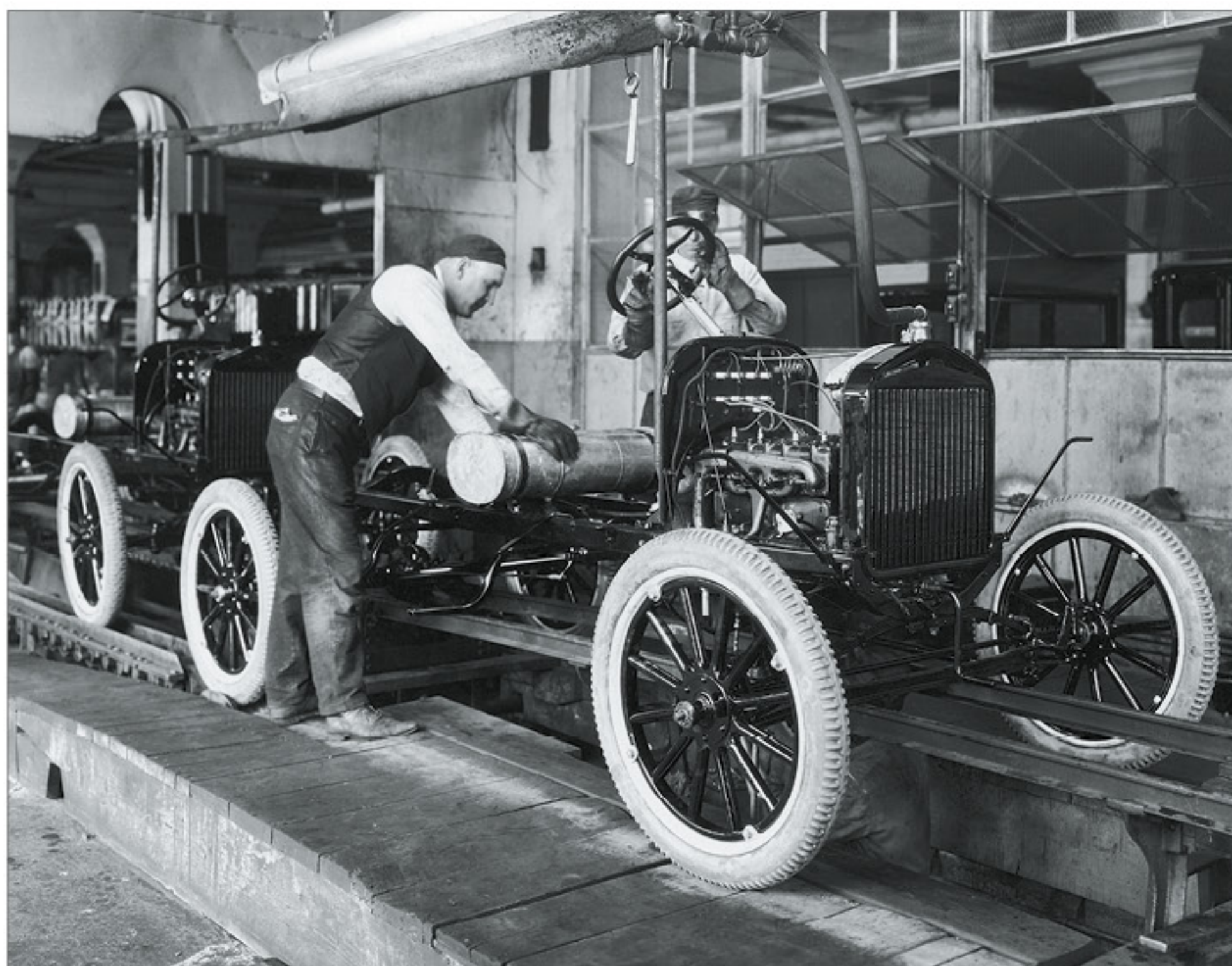
На каждом из последующих этапов реализации проекта производился контроль проектирования и реализации требований, в том числе проверка проведения тестов на проникновение для бизнес-критичных, а также доступных из интернета, веб-приложений.

Возвращаясь к стартовому этапу — после разработки чек-листа и внедрения в технический проект дополнительной контрольной точки был создан специальный почтовый ящик (вида sec-projects@oilcompany.com), проведены обучение сотрудников проектного офиса новому процессу и последующая рассылка необходимых материалов руководителям проектов.

ПОДДЕРЖИВАЮЩИЕ ИНСТРУМЕНТЫ (АРТЕФАКТЫ)

Для облегчения работы и контроля качества для специалистов сервиса контроля, руководителей проектов и проектных групп был создан набор из 7 инструментов (артефактов):

1. Таблица требований безопасности.
2. Контрольный лист безопасности проекта (создавался для каждого проекта).
3. Опросник для определения критичности системы по параметрам конфиденциальности, целостности и доступности.
4. Шаблоны документов — архитектурного плана, технического проекта и заявки на поддержку.
5. Контрольные практики в документах — матрица ролей, RPO / RPO, матрица взятия на поддержку компонентов системы и др.
6. Концепция контроля — каким видам контроля подвергаются системы в зависимости от интегральной степени их критичности (документарный контроль, дополнительный аудит и т.п.).
7. База знаний сервиса контроля (централизованное хранение проверенной и проверяемой проектной документации).



БЕЗОПАСНОСТЬ НЕ СТАНОВИЛАСЬ ТОРМОЗОМ ДЛЯ БИЗНЕСА, НО ПРОВЕРЯЛА РИСКИ НАДЛЕЖАЩИМ ОБРАЗОМ, МОЛ, ИДЕНТИФИЦИРОВАНЫ, УЧТЕНЫ И КОНТРОЛИРУЮТСЯ

ПЕРВЫЕ РЕЗУЛЬТАТЫ

Руководители проектов приняли перемены благосклонно. Сняв нагрузку по контролю проектов с CISO, мы сразу сократили сроки анализа на порядок (с недель-дней до дней-часов), а также разработали стандарт архитектурного участия кибербезопасности в проектах.

По прошествии месяца руководители проектов стали все чаще обращаться за оценками стоимости архитектурного участия безопасности в проекте, хотя часть неплохо спроектировала и реализовала требования силами подрядчиков или внутренних служб (проекты тиражей).

В случае невозможности реализации был вариант — подписать протокол принятия риска, но желающих подписывать такие протоколы среди бизнес-заказчиков не находилось. За первые полгода был один случай подписания дорожной карты по развитию ИБ одной из корпоративных платформ (СЭД),

так как платформа просто не интегрировалась в AD (выступавшей в виде SSO, интеграция с которой была в списке требований безопасности). Такие практики создавали канал для «выпуска пара»: безопасность не становилась тормозом для бизнеса, но проверяла риски надлежащим образом, мол, идентифицированы, учтены и контролируются.

РАЗВИТИЕ МЕТОДОЛОГИИ

Параллельно с быстрым запуском сервиса контроля (на все про все ушло две недели) был запущен проект по комплексному редизайну сервиса контроля и контрольной функции ИБ в отношении ИТ-проектов в целом. В рамках проекта мы проделали много работы, в том числе:

1. Пересмотрели шаблоны документов — архитектурного плана, технического проекта и заявки на обслуживание.
2. Разделили проекты на типы (внедрение, тираж и модернизация) и виды

(консалтинг, АСУ ТП, бизнес-приложения и инфраструктура).

3. Проанализировали лучшие мировые практики (ISO 27k, PCI DSS, PA DSS, NIST 800–53, Australian Information Security Manual, СТО БР ИББС) и практики схожих по масштабу деятельности глобальных нефтегазовых компаний (2 200+ контролей).

4. Сформировали матрицу контролей безопасности в зависимости от вида и типа проектов.

5. Разработали презентацию для обучения заинтересованных сторон.

Оглядываясь назад, я понимаю, что 2 200+ контролей могут показаться избыточными (тем более, что добрая половина из них повторяла друг друга), но такова была культура организации. Подход *best enough* («и так сойдет») не приветствовался, организация ставила себе задачу вырасти в мирового лидера нефтегазового комплекса и применяла самые современные и совершенные практики и системы.

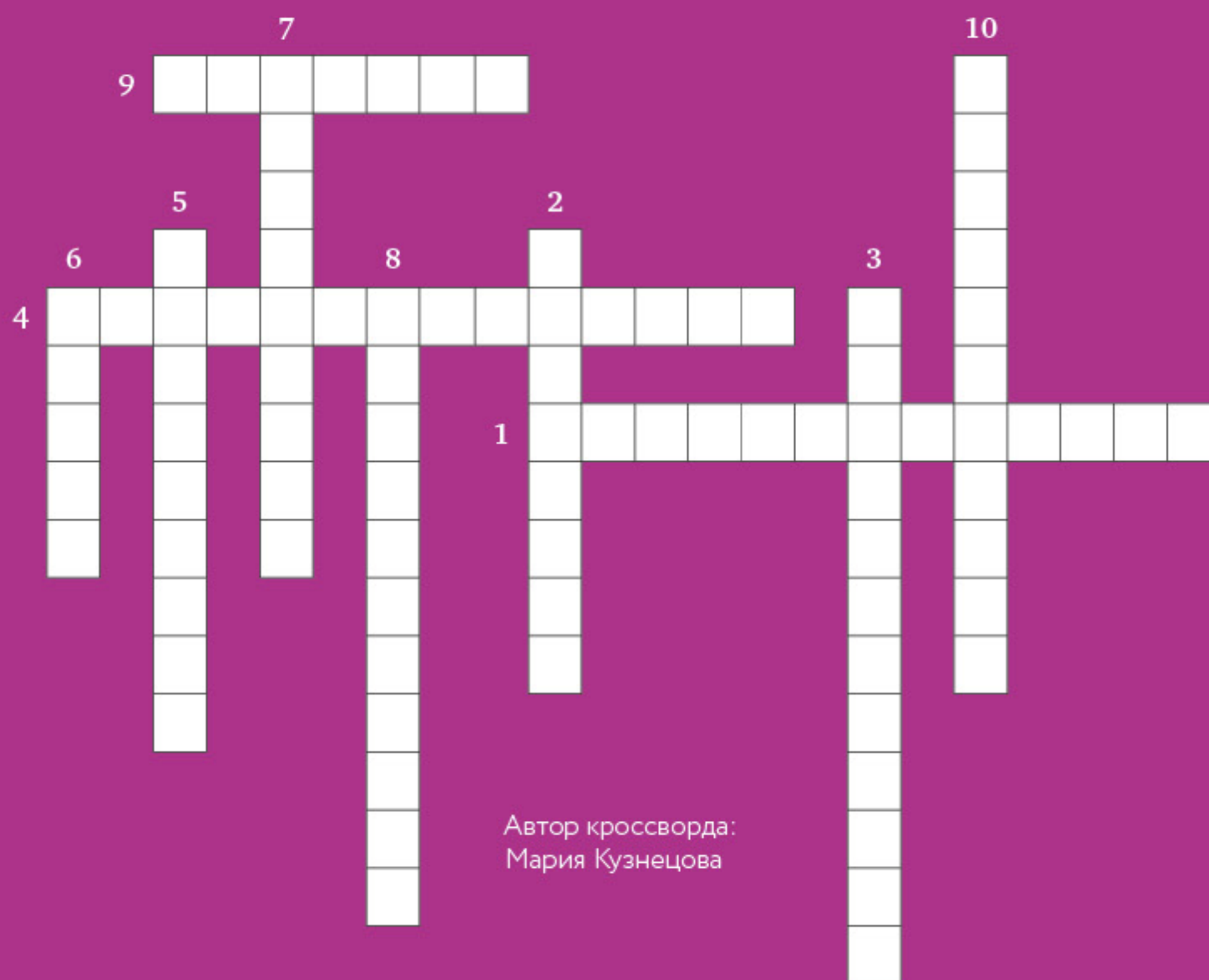
НЕОЖИДАННЫЕ РЕЗУЛЬТАТЫ

Качество внедрённых процессов и артефактов получило признание обеих ключевых сторон процесса. Во-первых, практически все непосредственные участники получили или повышение (двое стали начальниками подразделений в центральном аппарате, один — директором по развитию бизнеса ИТ-компании), или существенный рост заработной платы (экспертный путь развития).

А, во-вторых, попавшие под контроль руководители проектов («мыши») не единожды рекомендовали руководителя сервиса контроля («кошку») на работу в другие организации, в том числе и в те, где сами работали.

Вероятно, значительная часть проблем и недопонимания в коммуникациях между ИБ, ИТ и бизнесом в том, что ИТ и бизнес просто не понимают, что для них делает безопасность. Деятельность по кибербезопасности для них непрозрачна и непрогнозируема. Может быть, это главный урок, который я вынес из этого проекта.

КРОССВОРД



Автор кроссворда:
Мария Кузнецова

ПО ГОРИЗОНТАЛИ:

1. Свойство шифрующего преобразования усложнять взаимосвязи между элементами данных, что затрудняет восстановление функциональных и статистических связей между открытым текстом, ключом и шифртекстом.
4. Обеспечение гарантий идентичности предъявленной сущности.
9. Вид сетевой атаки, при которой одна программа (или пользователь) выдает себя за другую с целью получения определенных преимуществ.

ПО ВЕРТИКАЛИ:

2. Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерную систему.
3. Процесс аналитического раскрытия противником и/или нарушителем сообщения, открытого без предварительного полного знания всех элементов криптографической системы.
5. Неправомерный доступ или проникновение любого рода (физическое или информационное) в компьютеры, информационные системы и сети непосредственно или опосредованно через корреспондирующие сети или системы.
6. Попытка злоумышленника вызвать отклонения от нормального протекания информационного процесса.
7. Свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.
8. Защита систем передачи и хранения информации от навязывания ложных данных.
10. Распространение влияния одного знака открытого текста на много знаков шифртекста, а также распространение влияния одного элемента ключа на много знаков шифртекста.

ПРО ХАКЕРА

Из криминальной хроники: «Вчера был убит известный спамер. В списках подозреваемых 300 млн адресов».

Объявление: «Серьезная организация возьмет на высокооплачиваемую должность опытного хакера. Резюме просим размещать на главной странице сайта www.microsoft.com».

Хакер на приеме у врача:

— Доктор, помогите, у меня дома такое! Диски по комнате летают, сами в компьютер лезут и Windows устанавливают!

— У-у, батенька, да у вас полтерГейтс!

Две бабки увлеченно тараторят между собой. «Какой трафик!», — воскликнул хакер.

Навстречу хакеру двое громил с ножами:

— Гони деньги.

«Провайдеры!», — испугался хакер.

Переквалифицировался хакер в священника и приходит на проповедь с большого похмелья:

— И да поможет тебе F1, и сохранит тебя F2! Во имя Controla, Alta и святого Dela, да будет так, ENTER!

Из сообщения информагентства: «Группа российских хакеров взломала защиту на главном сервере господина Бога и поставила себе бесконечные деньги и вечную жизнь».

— Мама! Ну сколько раз тебе говорить, я не нахер, я — ХАКЕР!

Поделились Алексей Лукацкий и Евгений Родыгин



РКИ-Форум Россия

15 лет

г. Санкт-Петербург
12–14 сентября 2017 года

www.pki-forum.ru



Встречаемся в Питере!



Кибербезопасность крупных организаций и предприятий

Комплексная платформа для защиты
крупных IT-инфраструктур и промышленных сред

- Контроль и защита рабочих мест
- Защита виртуальных сред
- Защита центров обработки данных
- Экспертные сервисы в области кибербезопасности
- Защита от целевых и DDoS-атак
- Кибербезопасность критических инфраструктур
- Защита мобильного и онлайн-банкинга

kaspersky.ru/enterprise

© АО «Лаборатория Касперского», 2017. Зарегистрированные товарные знаки
и знаки обслуживания являются собственностью их правообладателей.