

10>

Андрей КУРИЛО
(Финансовый университет при
Правительстве РФ)
**Главное мероприятие
отрасли. Вершины ждут!**



16>

Руслан ВЕСТЕРОВСКИЙ
(Банк России)
**Требуется новый
профстандарт ИБ**

26>

Игорь НОВИКОВ
(ПАО Сбербанк)
**Цифровая экономика:
от стратегии к тактике**



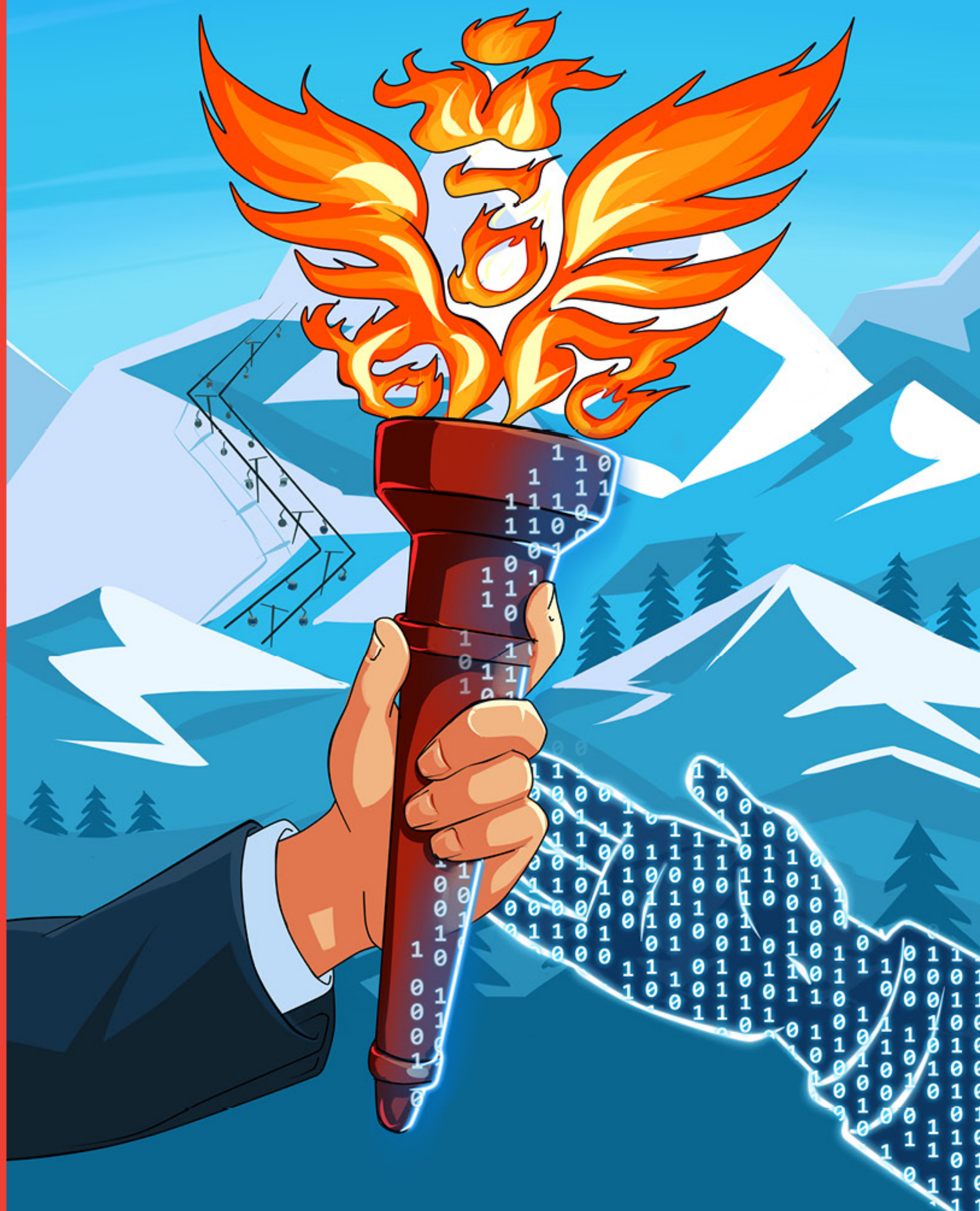
30>

Петр ЕФИМОВ
(Информзащита)
**«Цифровая экономика» —
документ эволюционный**

46>

Карл СУММАНЕН
(Банк ВТБ)
**От реестра населения
к реестру субъектов**

УРАЛЬСКОМУ ФОРУМУ — ДЕСЯТЬ ЛЕТ!





Ежегодные мероприятия в области информационной безопасности:

- **X Уральский форум** (12–16 февраля 2018 года, республика Башкортостан)
Ключевое мероприятие Банка России по информационной безопасности финансовой сферы.
ural.ib-bank.ru
- **SOC-Форум Казахстан** (апрель 2018 года, Астана)
Ежегодная конференция по практике противодействия кибератакам и построения центров мониторинга ИБ. Проводится при поддержке ГТС Министерства информации и коммуникаций Республики Казахстан.
soc-forum.ib-bank.ru
- **XXIII Конференция «Комплексная защита информации»** (22–24 мая 2018 года, г. Суздаль)
Конференция Союзного государства России и Беларуси, проводится при поддержке Совета безопасности Российской Федерации.
www.kzi.su
- **VII Симпозиум CTCrypt 2018** (27–30 мая 2018 года, г. Суздаль)
Симпозиум «Современные тенденции в криптографии».
Организаторы: ТК 26, Академия криптографии РФ и МИАН им. В.А.Стеклова.
www.ctcrypt.ru
- **DLTReg 2018** (31 мая 2018 года, г. Суздаль)
Международная конференция по регулированию распределённых реестров.
Организаторы: Ассоциация ФинТех и ТК 26.
www.dltreg.ru
- **Летняя сессия Уральского форума** (7 июня 2018 года, г. Москва)
Однодневная конференция по информационной безопасности финансовой сферы.
ib-bank.ru
- **IV Международная конференция «Актуальные вопросы развития наличного денежного обращения»** (19–20 июня 2018 года, г. Ярославль)
Международная конференция по безопасности оборота наличных денег и ценностей.
Проводится при поддержке Банка России.
inkas.ib-bank.ru
- **XVI PKI-Форум Россия** (25–27 сентября 2018 года, г. Санкт-Петербург)
Международная научно-практическая конференция, посвященная проблематике инфраструктуры открытых ключей, электронной подписи и электронного документооборота.
Проводится по инициативе Минкомсвязи России.
www.pki-forum.ru
- **SOC-Форум** (ноябрь 2018 года, г. Москва)
Ежегодная конференция по практике противодействия кибератакам и построения центров мониторинга ИБ. Проводится при поддержке ФСБ России, ФСТЭК России, Банка России.
soc-forum.ib-bank.ru



Артем ЗУБКОВ
генеральный директор
Медиа Группы «Авангард»



Игорь НЕКРАСОВ
главный редактор
BIS Journal



Андрей МИНАКОВ
директор по развитию
BIS Journal

Мы, безусловно, волнуемся. Подготовка к десятому — юбилейному — Уральскому форуму занимает все наши мысли и время. Готовимся к грандиозному. И этот номер BIS Journal не исключение. Он получился своеобразным началом, въездным порталом главного события нашей отрасли.

Начать с того, что зампред Банка России Роман Вестеровский анонсирует в нем свое выступление на форуме, посвященное качеству подготовки специалистов по информационной безопасности в кредитно-финансовой сфере. Проблема злее некуда — запутанная и неоднозначная. Зампред рассматривает ее как триединую задачу, а редакция — в помощь — в традиционном обзоре скрупулезно исследует один из ее аспектов — профстандарты в сфере ИБ.

Заместитель начальника ГУБиЗИ Артем Сычев привносит в этот номер детективный оттенок — рассказывает о том, что в ФинЦЕРТе появилось подразделение (особого назначения!), которое занимается криминалистикой инцидентов в финансовой сфере. Инструмент этот для банковских безопасников новый, и обсудить его на форуме будет весьма полезно.

Особая интрига с цифровой экономикой. Известно, что недавно Правительство утвердило план мероприятий по направлению «Информационная безопасность», но также общеизвестно, что не все тут окончательно и бесповоротно. Мы со своей стороны собрали сумму интересных мнений, но это для затравки, главный разговор, конечно, должен состояться на форуме. Отметим, что дискуссию, посвященную цифровой экономике, будут вести президент ГК InfoWatch Наталья Касперская и зампред Банка России Дмитрий Скобелкин.

Еще одна масштабная тема для обсуждения — единый идентификатор. Если раньше разговор о нем скользил всего лишь на уровне национального самолюбия (мол, в Индии с населением 1,2 млрд человек такой идентификатор давно введен, а у нас?!), то теперь две мощные статьи от Банка ВТБ, как два прожектора, вырвали сей предмет из незаслуженной тени. И сразу многое стало понятно. Но не все.

Если вспомнили о национальной гордости, то есть в этом номере для нее и бальзам. Отечественные разработчики в области голосовой биометрии победили в сложнейшем международном конкурсе, то есть официально признаны лучшими в мире (статья «Продукт победы»). И как это у них получилось?

В общем, открытых тем, вопросов, проблем и т.д. в этом номере много. Собирали специально, чтобы с чувством, с толком, с расстановкой обсудить на форуме.

Читайте, составляйте свое мнение.

И до встречи на Урале!

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Емельянов Г.В. — член-корреспондент Академии криптографии РФ, действительный государственный советник РФ 3 класса
Сычев А.М. — заместитель начальника Главного управления безопасности и защиты информации Банка России, кандидат технических наук, доцент
Шпилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Былевский П.Г. — шеф-редактор, кандидат философских наук
Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А.Ю. — начальник управления информационной безопасности АО КБ «Златкомбанк»
Вихорев С.В. — заместитель руководителя направления информационной безопасности НТЦ «Вулкан»
Дзержинский Ф.Я. — главный эксперт — координатор системной экспертизы блока «информационные технологии» ПАО «Промсвязьбанк», CSDP
Зубков А.Н. — генеральный директор ООО «Медиа Группа „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Курило А.П. — заместитель генерального директора компании «РНТ», кандидат технических наук
Левинов Д.О. — председатель Совета НП «Партнерство специалистов по информационной безопасности»
Мельников С.Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», кандидат физико-математических наук
Некрасов И.В. — главный редактор журнала
Окулесский В.А. — руководитель департамента ООО «ЦИБИТ», кандидат технических наук
Пазизин С.В. — начальник Управления по обеспечению информационной безопасности ОАО Банк ВТБ, кандидат физико-математических наук
Шумский Л.С. — руководитель направления ИБ АО «Альфа-Банк»
Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Одувалов М.В. — эксперт BIS Journal
Филипчук А.А. — технический директор ГК ЦРТ
Калашникова Е.В. — Банк ВТБ (ПАО)

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**
Шеф-редактор: **Былевский П.Г.**
Директор по развитию: **Минаков А.В.**
Арт-директор: **Мельников Н.С.**
Обозреватели, корреспонденты: **Бендин С.В.**, **Северный В.П.**, **Хвастунова О.Н.**, **Бродская М.А.**, к.т.н.
Иллюстрация на 1-й обложке: **Ларичкина О.А.**
Фото в номере: фотобанк DepositPhotos, 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 15.01.2018. Тираж 7000 экз.
Заказ № 11/4. Цена договорная.
Отпечатан в «Типографии на Угрешской»
115088 РФ, Москва, ул. Угрешская, д.2, стр.2.
Тел.+7 495 720-62-28

© BIS Journal, 2018



НОВОСТИ

5 В мире, криминал, в России, технологии

10 ЛЕТ УРАЛЬСКОМУ ФОРУМУ

10 Юбилей

Андрей КУРИЛО (Финансовый университет при
Правительстве РФ)
Вершины ждут!



РЕГУЛЯТОРЫ

16 Кадры

Руслан ВЕСТЕРОВСКИЙ (Банк России)
Триединая задача

20 Криминалистика

Артем СЫЧЕВ (Банк России)
Фиксировать, расследовать, предупреждать

22 Стандарты

Александр ВЕЛИГУРА (Ассоциация российских
банков)
ГОСТ Р 57580.1-2017. Первый национальный
и другие



ТЕМА НОМЕРА

25 Цифровая экономика

Наталья КАСПЕРСКАЯ (ГК InfoWatch)
В поисках синергии

26 Цифровая экономика

Игорь НОВИКОВ (ПАО Сбербанк)
Цифровая экономика: от стратегии к тактике

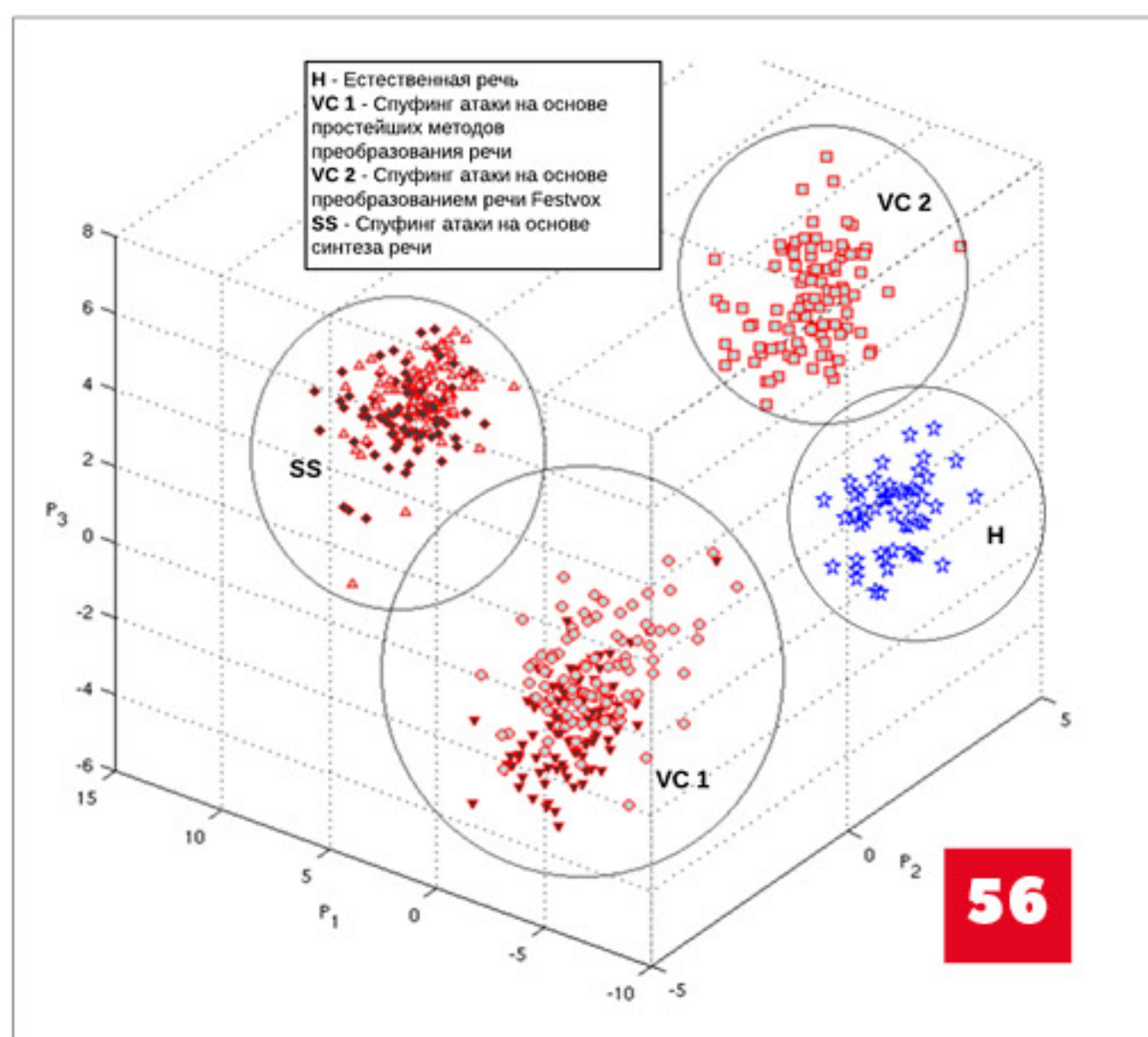
30 Цифровая экономика

Петр ЕФИМОВ (Информзащита)
Риски – это обыденность

36 Цифровая экономика

Тимур АИТОВ (ТПП РФ)
Умный банк в большом городе





БАНКИ

- 40** **Единый идентификатор**
Екатерина КАЛАШНИКОВА (Банк ВТБ)
К единому идентификатору
- 46** **Единый идентификатор**
Карл СУММАНЕН (Банк ВТБ)
После первого шага
- 50** **Госкорпорации**
Алексей ОЛЬШАНИКОВ (АО «Гринатом»)
Как обустроить функцию

УГРОЗЫ И РЕШЕНИЯ

- 54** **Инцидент**
Александр БОДРИК, Виктор ФЕДОТОВ
(ANGARA Professional Assistance), Лев ПАЛЕЙ
(эксперт ИБ)
Уроки простоты
- 56** **Биометрия**
Вадим ЩЕМЕЛИНИН (ООО «ЦРТ»),
Галина ЛАВРЕНТЬЕВА (ООО «ЦРТ-инновации»)
Продукт победы
- 60** **Аудит**
Антон СВИНЦИЦКИЙ (АО «ДиалогНаука»)
Стимул в действии
- 62** **УТМ-системы**
Андрей ДАВИДОВИЧ (ГК «Смарт-Софт»)
В сторону центра
- 64** **Системы контроля**
Дмитрий МИХЕЕВ (АйТи БАСТИОН)
Кто бреет бороду?
- 66** **SOC**
Павел ГОЛОВИСТИКОВ (АМТ-ГРУП)
Vulnerability management
- 68** **Anti-APT**
Александр РУСЕЦКИЙ (Инфосистемы Джет)
Anti-APT: муки выбора
- 70** **Облачные технологии**
Андрей АКИНИН (Web Control)
Shadow IT. Всем выйти из тени!
- 72** **Законодательство**
Владимир ИВАНОВ (Актив)
Банк на диване
- 74** **Судебная практика**
Евгений ЦАРЕВ (RTM Group)
Многоликая экспертиза

ИНФРАСТРУКТУРА

- 76 Аналитика**
Ольга ЗИНЕНКО (Positive Technologies)
Мишень для терпеливых
- 78 Аналитика**
Лев ПАЛЕЙ (эксперт ИБ)
Аналитика особого назначения
- 81 Compliance**
Олег ИВАНОВ, Василий ОКУЛЕСКИЙ
(ООО «ЦИБИТ»)
Как успеть за регулятором?
- 84 Стандарты**
Сергей КУЗНЕЦОВ (Gemalto)
Три регламента
- 86 Деловые мероприятия**
Анна ВОРОБЬЕВА (BIS Journal)
SOC-Форум 2017
- 90 Деловые мероприятия**
Николай КОЛЬСКИЙ (BIS Journal)
RAIF 2017
- 93 Деловые мероприятия**
Корней РЕУТ (BIS Journal)
ZeroNights 2017
- 96 Деловые мероприятия**
Марк НОВОДАЧНЫЙ (BIS Journal)
TERADATA Форум 2017
- 98 Деловые мероприятия**
Корней РЕУТ (BIS Journal)
AntiFraud Russia 2017

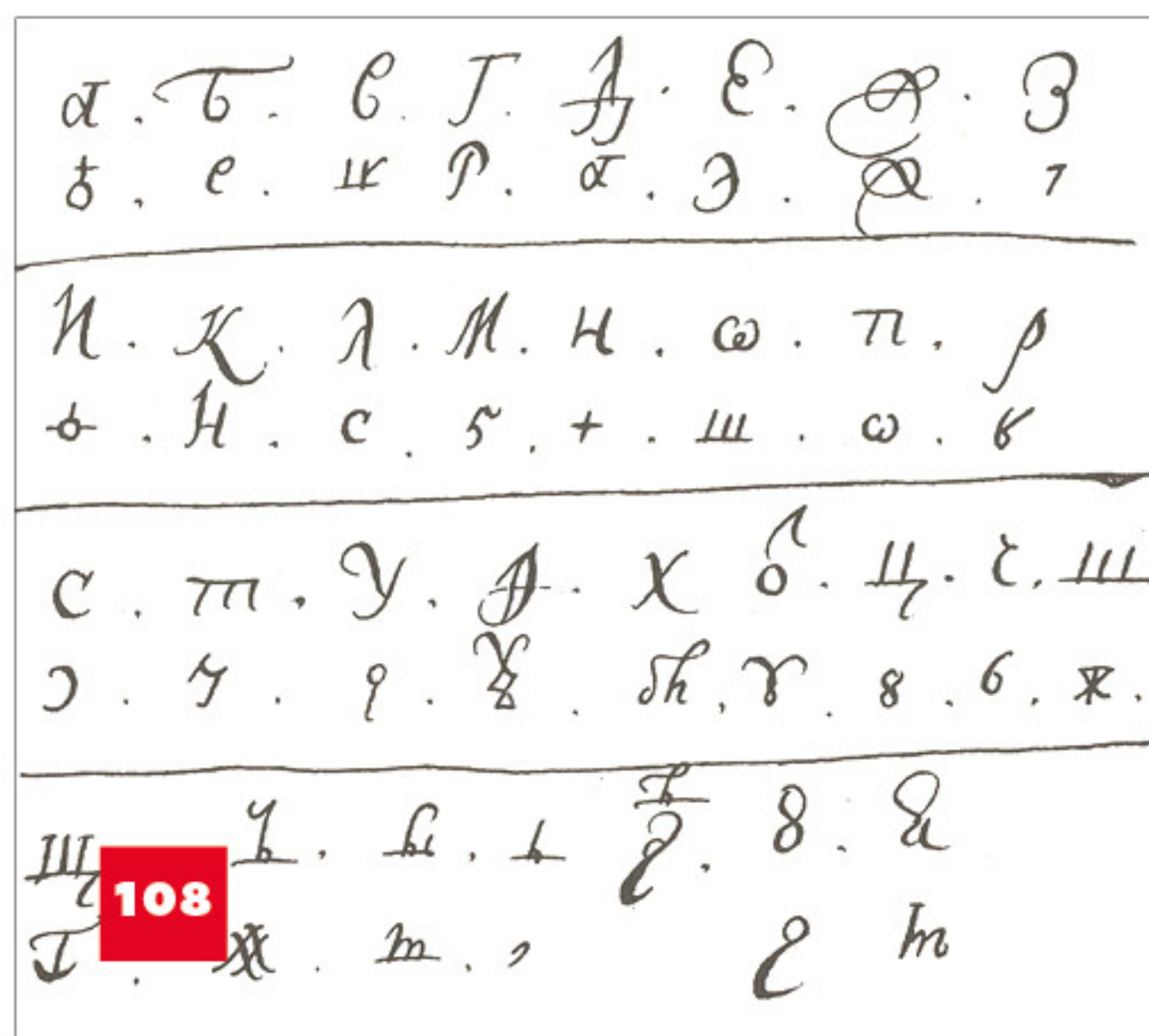


ОБРАЗОВАНИЕ И КАРЬЕРА

- 100 Персонал**
Игорь ДОЛОТИН (UBS)
Как повысить?
- 102 Обзор**
Марина БРОДСКАЯ (BIS Journal)
Новые профстандарты

СУБЪЕКТЫ

- 108 Корифеи**
Дмитрий ЛАРИН (историк криптографии)
Петр I и криптография
- 112 Корифеи**
Борис СТОЛПАКОВ (историк криптографии)
Сто лет назад
- 116 Мысли вслух**
Александр БОДРИК (ANGARA Professional Assistance)
Кибербезопасность по Адизесу
- 118 Прогноз**
Алексей ПЛЕШКОВ (эксперт ИБ)
Знал бы, где упадешь...



ОФФТОПИК

- 120 Блогеры усмеваются**
Кроссворд, юмор

В ИНДИИ ВЗЛОМАН ГЛАВНЫЙ БАНК БИОМЕТРИЧЕСКИХ ДАННЫХ

В Индии взломали самый крупный в мире банк данных UIDAI, где хранятся биометрические данные миллиарда жителей страны. Журналисты The Tribune в рамках расследования сделали это через посредника всего за 10 минут, цена вопроса не превысила и 13 долларов.

Репортеры связались по WhatsApp с анонимным дилером и, заплатив ему сущие копейки, получили все необходимые логины и пароли для входа в базу Агентства Индии по уникальной идентификации. Еще 5 долларов журналисты потратили на программное обеспечение для изготовления ID-карт пользователей UIDAI.

В Индии каждому гражданину страны при рождении присваивается 12-значный номер, Aadhaar, к которому привязываются все личные данные. Aadhaar позволяет узнать не



только фамилию, имя, адрес, телефон, банковские реквизиты человека, но и его отпечатки пальцев, сканы радужной оболочки глаза. Такой 12-значный номер используется для идентификации человека при проведении банковских операций, получении различного рода субсидий и компенсаций, оплате штрафов, получении медицинской помощи и прочих услуг.

В настоящее время несколько сервисных центров Индии подозреваются в приобретении незаконного доступа к Aadhaar.

ХАКЕР УГОДИЛ В ТЮРЬМУ, ВЫЗВОЛЯ ДРУГА

Житель Мичигана взломал компьютерную сеть местной тюрьмы, чтобы раньше срока освободить своего товарища. Однако план провалился, и он сам оказался за решеткой.

27-летний Конрадс Войтс с помощью фишинговых рассылок, телефонных звонков, а также подставного сайта, название которого похоже на название сайта окружной тюрь-

мы, пытался заставить сотрудников учреждения загрузить на свои компьютеры вредоносное ПО. С помощью вируса мужчина рассчитывал проникнуть в ИТ-систему тюрьмы, чтобы внести изменения в базу данных и ускорить освобождение друга.

После успешной установки малвари хакер получил полный доступ к тюремной сети, в том числе к системе XJail, содержащей данные о заключенных. Также ему стала доступна закрытая информация, включая внутренние дисциплинарные записи и личные дела сотрудников тюрьмы. Кроме того, по данным ФБР, к Войтсу попали персональные дела более чем 1600 сотрудников учреждения, включая логины, пароли и адреса электронной почты.

Войтс все-таки разыскал в базе данных своего друга и поменял записи. Однако сотрудники тюрьмы заметили изменения и сообщили об этом в ФБР. Агенты вышли на след горе-хакера и задержали его.



UBER СКРЫЛ КИБЕР-ОГРАБЛЕНИЕ

Компания Uber была вынуждена объявить о том, что в 2016 году хакеры украли с ее серверов данные 50 миллионов клиентов и 7 миллионов водителей. Одновременно было объявлено об увольнении главы службы безопасности компании Джо Салливана, который занимался этим инцидентом.

В нарушение установленного законом порядка Uber в 2016 году не сообщила о взломе ни властям, ни своим водителям, номера удостоверений которых были похищены. Вместо этого Uber заплатила хакерам 100 тысяч долларов, чтобы те удалили информацию и не сообщали о взломе.

После саморазоблачения Uber расследование начал прокурор Нью-Йорка. Одновременно несколько клиентов подали против Uber совместный иск о неадекватном обращении с их данными.

БИТКОИН-БАНКОМАТ ПОЯВИЛСЯ НА КИПРЕ

Терминал для покупки криптовалюты расположен в баре Pitta&More города Лимасола и, по словам его владельцев, пользуется популярностью у туристов.

Банкомат открыли на пике «биткоиновой лихорадки», когда курс электронной валюты перевалил через отметку в \$11 000 за единицу. Чтобы приобрести биткоины, пользователю достаточно ввести QR-код электронного кошелька, после чего произойдет связь с одной из бирж криптовалют, которая перелагает более выгодный на этот момент курс.

Стремительный рост курса биткоина начался после объявления CME Group, являющейся мировым биржевым лидером, привязать криптовалюту к фьючерсам. К этому проекту позже присоединилась биржа Nasdaq, что значительно увеличило ажиотаж и содействовало увеличению курса.

13 ЛЕТ ШПИОНИЛ ЗА ЛЮДЬМИ

На протяжении 13 лет американский киберпреступник шпионил за тысячами пользователей, используя шпионскую программу, установленную на зараженные компьютеры.

Некий Филлип Дурачински, житель Огайо, обвиняется по 16 пунктам, один из которых — разработка вредоносной программы Fruitfly, позволяющей шпионить за пользователем зараженного компьютера (снимать скриншоты, перехватывать нажатия клавиш, записывать аудио и видео с камеры и микрофона).

Как утверждает обвинение, хакер похищал персональные данные жертв, включая банковские, налоговые и медицинские данные, фотографии. Более того, подслушивал и подглядывал за пользователями. В одном из эпизодов Дурачински скачал гигабайты порнографических картинок с компьютера одного из жителей, включая порнографию с детьми. Теперь гражданину Америки грозит многолетний тюремный срок.

ДЕНЬГИ ВЫВЕЛИ ЧЕРЕЗ SWIFT

Незадолго до Нового года мошенники впервые вывели деньги из российского банка через систему SWIFT.

Факт успешной атаки подтвердил Банк России. Название банка и сумма ущерба не называется, однако отмечается, что атака была совершена через международную систему передачи финансовой информации SWIFT. До этого деньги из российских банков мошенническим путем через SWIFT не выводились. Уточняется также, что банк атаковали 15 декабря, и то, что ранее проверка Банка России показала в атакованном банке проблемы с ИБ.

По данным компании по предотвращению и расследованию киберпреступлений Group-IB, к атаке причастна группировка Cobalt. Атака проведена через вирус, которой группировка рассылала в начале декабря.

МОШЕННИКИ АТАКУЮТ ОТ ИМЕНИ БАНКА РОССИИ

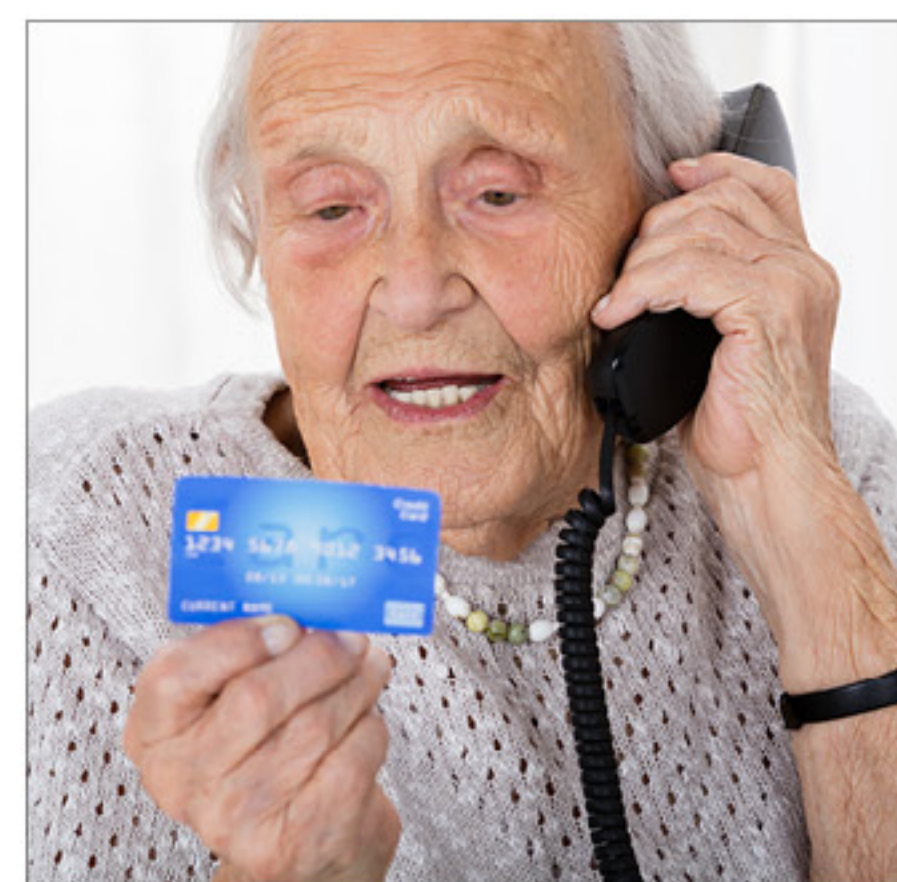
Банк России обеспокоен активизацией мошенников, которые от имени сотрудников БР выманивают у физлиц денежные средства, данные банковских карт, паспорта и т.д.

Целевая аудитория аферистов — граждане, ставшие жертвами финансовых пирамид, псевдопсихологов и экстрасенсов, продавцов приборов и биодобавок. Аферисты звонят доверчивым людям, представляются сотрудниками Банка России и обещают выплатить компенсацию за потерянные когда-то деньги. Но чтобы получить ее, нужно заплатить комиссионный сбор, подоходный налог, госпошлину или что-то другое.

Другой способ обмана — ложные СМС-сообщения о блокировке банковской карты и предложение перезвонить по указанному номеру. Позвонив, человек попадает к мошенникам. Еще одна схема — уведомления о выплатах и компенсациях в письменном виде. По почте на бланке с якобы

реквизитами Банка России гражданину поступает уведомление о том, что судом принято решение о выплате компенсации за приобретение каких-либо товаров в мошеннических организациях.

Никакого отношения к таким оповещениям и уведомлениям Банк России не имеет. ЦБ не работает напрямую с физическими лицами, не блокирует их карты и не выплачивает гражданам никаких компенсаций.



ХАКЕРЫ ПРОТИВ АВТОПЕРЕВОЗЧИКОВ

Московские полицейские разоблачили банду Интернет-мошенников, которые нанесли ущерб российским автоперевозчикам на сумму в 40 млн рублей.

Злоумышленники взламывали аккаунты компаний, занимающихся автоперевозками, и перехватывали заказы от различных фирм. Затем отправлялись на склад и по поддельным документам вывозили партию товара. Естественно, до пункта назначения товар не доезжал.

Хакеры работали с 2016 года — в Москве, Московской, Брянской, Владимирской и Челябинской областях, а также в Кабардино-Балкарии и Башкортостане. Некоторое время назад лидер и девять активных участников банды были задержаны сотрудниками правоохранительных органов.

В отношении задержанных возбуждено дело по статьям 201 (органи-

зация преступного сообщества или участие в нем), 158 (кража, совершенная организованной группой в особо крупном размере) и 159 УК РФ (мошенничество).



ЦИФРОВАЯ ЭКОНОМИКА: УТВЕРЖДЕН ДОРОЖНЫЕ КАРТЫ

На заседании Правительственной комиссии по использованию информтехнологий утвержден план мероприятий Программы «Цифровая экономика Российской Федерации» по четырем направлениям: «Нормативное регулирование», «Формирование исследовательских компетенций и технологических заделов», «Информационная инфраструктура» и «Информационная безопасность».

Для актуализации каждого из направлений Минэкономразвития, Минфину и Росстату поручено подготовить до 15 марта «предложения, направленные на совершенствование системы государственной статистики в части повышения оперативности получения отчетных данных и полноты собираемой информации».

Кроме того, Минкомсвязи и Минэкономразвития, совместно с АНО «Цифровая экономика» и Аналитическим центром при Правительстве РФ, поручено представить до 15 февраля



предложения по включению в программу «новых направлений, предусматривающих цифровую трансформацию отдельных отраслей экономики и социальной сферы».

Отметим, что утвержденные дорожные карты будут реализовываться с 2018 по 2020 годы. Для этого предусмотрено выделить из государственной казны 22 333 млн руб. Вложения из внебюджетных источников составят примерно 11 710 млн руб.

СБЕРБАНК ОТКРЫЛ САМЫЙ БОЛЬШОЙ ЦОД

Сбербанк открыл один из крупнейших в Европе и самый большой в России центр по обработке данных «Сколково». В церемонии запуска ЦОД приняли участие глава Сбербанка Герман Греф, вице-премьер Аркадий Дворкович, министр связи и массовых коммуникаций Николай Никифоров, президент «Сколково» Виктор Вексельберг и др.

«На создание четырех очередей ЦОД потрачено 14 млрд рублей, строительство пятой очереди заканчивается, ее мы планируем использовать под нужды нашей экосистемы», — сообщил Герман Греф.

Вице-премьер Аркадий Дворкович акцентировал, что в новом ЦОД используется множество отечественных технологий, некоторые системы создавались специально для него.

Президент фонда «Сколково» Виктор Вексельберг рассказал, что мощ-



ность ЦОД составит 29,9 МВт. По его словам, ЦОД уже прошел экспертизу Руководства по энергоэффективному и экологическому проектированию в США и получил серебряный сертификат соответствия экологическим стандартам.

«Запуск такого объекта в Сколково очень важен для эффективности экономики в целом. От этого выигрывает не только Сбербанк, но и вся Россия», — прокомментировал министр Николай Никифоров.

БАНКИ НЕДОВОЛЬНЫ

Половина российских банков недовольна своими средствами защиты от киберугроз. Таков итог исследования Qrator Labs среди банков и платежных систем, входящих в ТОП-200 по размеру активов.

Так, 32% банков заявили об увеличении бюджета на кибербезопасность в 2016 г., при этом 39% сообщили, что бюджет не изменился, а 13% бюджет сократили.

53% назвали недостаточный уровень защиты как причину для замены решений обеспечения ИБ. Более 25% видят необходимость в замене средств защиты при переходе на новые инфраструктурные решения, например, облачные технологии. 13% заменяют импортные решения на российские аналоги.

Чаще всего банки сталкивались с фишингом (30%) и DDoS-атаками (26%). При этом 55% кредитных организаций ни разу не сталкивались с DDoS-атакой в 2016 году, 29% сталкивались 1–2 раза, 8% — 3–5 раз, 8% — 5 и более раз.

РОССИЯ НА 10-М МЕСТЕ

В рейтинге 2017 года Международного союза электросвязи (МСЭ) по индексу кибербезопасности Россия заняла 10 место, на один пункт опередив Японию и Норвегию.

Россия также опередила целый ряд мировых лидеров. Великобритания заняла 12 место, Южная Корея — 13-е, Финляндия — 16-е, Германия — 24-е, Италия — 31-е. Всего в исследовании приняли участие 193 страны.

Напомним, Минкомсвязь России последовательно призывает все государства к широкому сотрудничеству в области ИБ и защиты ИКТ-инфраструктуры. Так, вопросы ИБ, а также управления критической инфраструктурой интернета регулярно обсуждаются на встречах «Большой двадцатки», на площадке ООН, на встречах министров телекоммуникаций и информационных технологий стран БРИКС.

ГЛОБАЛЬНЫЙ ЦЕНТР ПО КИБЕРБЕЗОПАСНОСТИ

Сбербанк принял участие в обсуждении и формировании принципов Глобального центра по кибербезопасности, созданного под эгидой Всемирного экономического форума 25 января в Давосе.

Глобальный центр по кибербезопасности является ключевой вехой развития «Cybercrime project» — обширной инициативы ВЭФ по кибербезопасности. Представители Сбербанка надеются, что Центр возьмёт на себя роль уникальной платформы по взаимодействию государственного и частного секторов, развитие которой будет происходить по трём ключевым направлениям: установление взаимовыгодного сотрудничества, формирование необходимых условий для постоянного обмена информацией и создание надёжного исследовательского центра независимой оценки кибербезопасности на международной арене.



БАНК РОССИИ ГОТОВИТСЯ К ЧМ-2018

Банк России разослал целевые рекомендации по кибербезопасности в кредитные организации, работающие в городах проведения матчей чемпионата мира по футболу. Рекомендации касаются защиты от компьютерных атак объектов банковской инфраструктуры, банкоматов и POS-терминалов.

В частности, Банк России рекомендует установить на банкоматы антискинминговое оборудование, своевременно обновлять ПО, установленное в устройствах самообслуживания, настроить системы мониторинга на оповещение ответственных

лиц в случае длительного отсутствия отклика от банкомата, вскрытия или другой нештатной ситуации.

Регулятор также рекомендует напоминать гостям чемпионата о правилах пользования банкоматами и платежными терминалами. Рекомендуется обращать внимание на наличие посторонних устройств на банкомате, не пользоваться некорректно работающим банкоматом и не прибегать при возникновении сложностей к помощи посторонних людей. Если в работе банкомата возникли сбои, следует обратиться в банк, которому он принадлежит.

PHDays
Positive Hack Days
DIGITAL BET
15 – 16 МАЯ, 2018



БИЛЕТЫ
УЖЕ В ПРОДАЖЕ

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



WTC
MOSCOW

facebook.com/PHDays
twitter.com/phdays_ru

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

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

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

#PHDays

phdays.com

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

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

POSITIVE TECHNOLOGIES

WI-FI ALLIANCE АНОНСИРОВАЛА ПРОТОКОЛ WPA3

Некоммерческая организация Wi-Fi Alliance, объединяющая Apple, Microsoft, Qualcomm, анонсировала разработку протокола следующего поколения — WPA3.

В отличие от своих предшественников новая версия защищает пользователей открытых беспроводных сетей с помощью индивидуального шифрования данных. Благодаря этому другие клиенты сети и случайные пользователи не смогут получить доступ к трафику между вами и роуте-

ром. Кроме того, протокол задействует 192-битное шифрование, которое совмещается с комплектом CN SA (Commercial National Security Algorithm). Это существенно повышает защиту государственных и промышленных сетей.

Также протокол адаптирован для работы с небольшими мобильными устройствами, упрощая настройку сетевой безопасности на устройствах с маленьким экраном или без такового. Оборудование, оснащенное новым протоколом, появится на рынке уже в текущем году.

При этом протокол WPA2 никто не оставляет без присмотра. Организация и дальше продолжит работу над ним. Обновления, которые должны появиться в ближайшем будущем, снизят вероятность появления уязвимостей и обеспечат надежную защиту сетей с централизованной аутентификацией.



ВРЕДНОС КРАДЕТ БИТКОИНЫ

Троян под названием Evrial способен отслеживать появление в буфере обмена адресов электронных кошельков или URL-предложения обмена Steam, а затем заменять их на адрес или ссылку, принадлежащие хакерам.

Также он умеет похищать файлы cookie, учетные данные, сохраненные на устройстве пароли и делать скриншоты открытых окон пользователя. В данный момент вирус активно продается на отечественных даркнет-ресурсах, приобрести его можно всего за 1500 рублей. Судя по всему, вирус имеет российские корни, так как среди браузеров, из которых злоред умеет похищать данные, числится и Яндекс.Браузер.



iFin
media

АРБ
Ассоциация
Российских
Банков

iFin-2018

XVIII МЕЖДУНАРОДНЫЙ ФОРУМ

20-21 февраля 2018, г. Москва,
"Рэдиссон Славянская"

Электронные финансовые
услуги и технологии

Спонсоры

BIFIT

BSS

ICAM

→ Технологии

- Интернет-банкинг
- Мобильный банкинг и платежи
- Системы самообслуживания
- Технологии по приему платежей
- Электронные расчеты
- Платежные системы
- ИТ-инфраструктура
- Интеграция, облака, аутсорсинг
- Информационная безопасность
- Небанковские сервисы

→ Бизнес

- Анализ развития рынков
- Экономическая эффективность
- Решение бизнес-задач с помощью электронных каналов
- Создание и развитие банковских услуг
- Привлечение и удержание клиентов
- Активизация продаж
- Современные средства продвижения финансовых услуг

Оргкомитет iFin-2018

<http://forumifin.ru>
тел. (495) 229-85-02

ВЕРШИНЫ ЖДУТ!

Уральскому форуму — 10 лет



**Андрей КУРИЛО**

основатель Уральского форума,
доцент Финансового университета
при Правительстве РФ

Не берусь судить, много или мало 10 лет для публичного мероприятия, живущего по своим медиа-законам. С одной стороны, не так уж и много, есть конференции, которые существуют и в два раза больше и, конечно же, вызывают этим огромное уважение. Но с другой стороны, десять лет далеко не так уж и мало, если речь идет о сфере банковской информационной безопасности.

Это огромный срок, судя по интенсивности происходящих изменений, смене за это время не только информационных технологий и технологий безопасности, но и парадигм безопасности, возникновения новых сущностей, реакции на них рынка, научных и учебных заведений и самих организаций кредитно-финансовой сферы. Отметим, что за это время существенным образом поменялась и продолжает меняться позиция регулятора (Банка России) в отношении информационной безопасности всей кредитно-финансовой сферы. Серьезное понимание найдено у госрегуляторов, ответственных за безопасность информации, криптографической защиты информации и персональных данных. Возникла новая задача — соответствие ФЗ № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

За прошедшие десять лет практически выросло новое поколение специалистов, на форуме появляется и заявляет о себе все большее число прекрасно подготовленных и образованных моло-



Первая межбанковская конференция по информационной безопасности, позднее ставшая Уральским форумом, прошла в 2009 году



Большое деятельное участие в создании форума принял Председатель Национального банка Республики Башкортостан Рустэм Хабибович Марданов, ныне Председатель Правительства Республики Башкортостан

дых людей, а отцы-основатели плавно перемещаются в статус ветеранов движения и авторитетных экспертов.

Форум стал полигоном для обкатки и проработки многих тем, инициатив, идей. Идея ФинЦЕРТа тоже зародилась на Урале. В этом смысле, история форума практически отражает всю историю

развития проблематики информационной безопасности в России.

Гибко и быстро меняется программа форума, становясь все более насыщенной. Великолепно выступают докладчики, проводятся мастер-классы, локальные мероприятия. За это время сформировался устойчивый контин-

гент гостей форума, заинтересованных в постоянном участии в нем и в общении с коллегами.

Колоссальная насыщенность программы потребовала интенсивной работы участников в течение четырех дней, что само по себе дает эффект повышения квалификации большого ко-



Артём СЫЧЕВ
председатель
программного комитета
Уральского форума,
заместитель начальника
Главного управления
безопасности и защиты
информации Банка
России

МЕСТО СИЛЫ

Для меня Уральский форум — это место нашей профессиональной силы. Нельзя сказать, что, работая в своих городах, отражая атаки злоумышленников, выстраивая контуры защиты, мы не ощущаем единства и энергии нашего общего дела. Но рутина, согласитесь, имеет свойство пожирать эту энергию, не восполняя. И в тысяче маленьких текущих проблем вдруг начинает растворяться высокая миссия, которой мы служим, локальные вопросы становятся важнее общей большой цели.

Каждый год, вырываясь сюда — на зимнее озеро посреди седых гор, — я наблюдаю и сам с радостью участвую в уникальном процессе сборки нашей профессии. Уральский форум взламывает внутреннюю скорлупу угнетенного большим городом профессионала и извлекает на свет его мощную личность, полную энергии, дерзости и таланта. Объединившись, эти личности в течение пяти дней составляют освобожденный коллективный разум профессии. И часто идеи, рожденные этим разумом, определяют вектор развития нашей отрасли на годы вперед.

Тем более, что Уральский форум давно вышел за рамки исключительно банковской тематики. Я бы назвал его тимбилдингом для всей отрасли информационной безопасности — в нем зримо и масштабно работают все наши профессиональные связи: и вертикальные, и горизонтальные.

Казалось бы, все просто, но механика форума, как и любого творческого акта, не поддается анализу. Она складывалась из года в год в мучительном поиске, и все тут имеет значение. И зима, и горы, и лазертаг, и «Наши» и «Тоже наши», и неумная энергия Артема Зубкова, и, конечно, сложная, разветвленная программа выступлений и дискуссий, которая продумывается и готовится не один месяц.

Я рад, что у нас есть такое сакральное место, которое, как в сказке, открывается только раз в году — далеко на Урале.

С юбилеем!

личества людей. В результате на форуме царит некий особый творческий дух, что крайне эффективно и ценно.

В разное время форум посещали руководители республики Башкортостан, Центрального банка РФ, ФСБ России, ФСТЭК России, ФНС, Минкомсвязи, АСВ, ведущих коммерческих банков России, банковских ассоциаций.

Неоднократно в работе форума принимали участие коллеги из Польши, Беларуси, Украины, Казахстана, Азербайджана, Армении.

Возник целый отраслевой портал ib-bank.ru, посвященный вопросам банковской информационной безопасности, есть интересный журнал, в котором выступают компетентные авторы, телевидение. Форум и тематика живут своей жизнью, в ногу со временем.

Именно поэтому Уральский банковский форум занимает в многочисленном ряду мероприятий по информационной безопасности особенное место, являясь украшением всей сферы информационной безопасности России.

В чем слагаемые успеха форума?

Их несколько.

Во-первых, была четко сформулирована цель: создать отраслевое мероприятие, с максимальной представительностью практикующих специалистов по информационной безопасности банковского сектора.

Во-вторых, была поставлена цель собрать вместе специалистов на несколько дней, с минимальным отрывом от

мероприятия. В Москве или Санкт-Петербурге это сделать невозможно.

В-третьих, была определена предельная численность участников в 400 человек. Это потребовало поиска подходящего зала для заседаний, мест для комфортного размещения, отдыха и питания участников. Потребовалось решить задачу и выбора места проведения мероприятия и решения логистических задач. Отмечу только, что в стране мало таких мест. Немаловажным оказался факт наличия конкуренции за присутствие на форуме, ведь число мест ограничено.

В-четвертых, нужно было не попасть параллельно с каким-нибудь другим

мероприятием, они бы мешали друг другу, отвлекали людей, усложняли финансирование их участия в работе форума.

И наконец, в-пятых, организаторы хотели предоставить участникам условия для активного отдыха. Все эти требования на условиях компромисса сошлись в одном месте, и это место — предгорье южного Урала, озеро Банное, санаторий Юбилейный. Рядом горнолыжный центр Магнитогорского металлургического комбината, несколько дальше база отдыха Абзаково и еще дальше — город Белорецк. Есть возможность и на горных лыжах покататься, и в футбол поиграть, и в стендо-



Неформальное общение профессионалов. На Уральском форуме оно особенно эмоциональное



Артем ЗУБКОВ
генеральный директор
Медиа Группы
«Авангард»

В НАЧАЛЕ ПУТИ

У Медиа Группы «Авангард» к Уральскому форуму особое — нежное и трепетное — отношение. Одно из направлений нашей деятельности — организация мероприятий в сфере информационной безопасности, и так получилось, что начинали мы десять лет назад именно с организации Первого Уральского форума. Можно сказать, мы вырастили и выпестовали его с пеленок.

Год за годом он рос, формировался, мужал, доставляя нам много радости и, конечно, проблем. Но вместе с ним росли, учились, набирались опыта и мы — каждый следующий форум был для нас новой вершиной, которую мы покоряли вместе. И сегодня, пройдя путь от локальной межбанковской конференции до главного мероприятия отрасли информационной безопасности России, мы, конечно, счастливы.

Счастливы не только тем, что с гордостью готовим к выпускному балу нашего достойного во всех отношениях десятиклассника, но и тем, что мы просто вместе, и снова волнуемся: что же там впереди? А ждет нас ещё более интересная жизнь: новые преодоления, открытия и свершения.

Потому что мы снова молоды и снова в начале пути.



Традиционный ужин на свежем воздухе сопровождается салютом



Официальный вид спорта Уральского форума — хоккей в валенках. На «Банковских битвах» накал страстей нешуточный

вой стрельбе поупражняться, и на снегоходах поездить.

Интересно вспомнить, как зарождалась идея создать такое мероприятие. В целом, история вопроса насчитывает примерно тринадцать-четырнадцать лет. В то время в банковской системе начала активно развиваться тематика стандартизации банковской информационной безопасности, получившая свое логическое завершение только сейчас. Но какое! Создан и работает

технический подкомитет по стандартизации в составе технического комитета ТК 122 Банка России. Выпущен первый ГОСТ Р по вопросам банковской безопасности, готовится и, надеюсь, выйдет ГОСТ Р по оценке соответствия. Создан комплекс Стандартов Банка России. Прорабатываются самые современные вопросы, направленные на повышение качества работы и предоставляемых услуг, снижение издержек заказчиков. В этих успехах есть и вклад форума,

в рамках которого вырастают и выделяются отдельные целевые мероприятия с более узкой и специализированной проблематикой.

Именно тогда огромное и деятельное участие в проработке вопроса и создании форума принял Председатель Национального банка Республики Башкортостан Рустэм Хабибович Марданов, ныне Председатель Правительства Республики Башкортостан. Вместе с ним и его коллегами мы объехали все места,



Александр ВЕЛИГУРА
председатель Комитета по информационной безопасности Ассоциации российских банков

АЗАРТ И ВДОХНОВЕНИЕ

На Уральском форуме я был все девять раз. Это незабываемо, каждый форум удивлял своей новизной, энергией, вдохновением. Каждый год, как только начинается зима, меня туда тянет. И я знаю почему. Потому что на сто процентов уверен: там меня ждут новые открытия.

Конечно, из всех форумов особенно запомнился первый. Ведь до этого ничего подобного не было. Несомненно, форум год от года растет, мужает, укрупняется... Масштабы, размах, мощь первого и последнего — несопоставимы. Программа форума постоянно усложняется, ветвится, углубляется, приезжают все более и более интересные, крупные люди. Но первый — он и есть первый — самый важный, как рождение ребенка, как начало начал.

Чем Уральский форум отличается от других мероприятий в сфере ИБ? Безусловно, масштабом, атмосферой. Приподнятое настроение, напряжение мысли, чистейший горный воздух... Форум уникален. Правда, я не был ни разу на РКІ-Форуме в Санкт-Петербурге. Говорят, что там тоже какая-то потрясающая — ни с чем не сравнимая обстановка. Но, думаю, хоккея в валенках там точно не бывает. А на Уральском форуме бывает!

В этом году ожидаю от форума новых идей. Уральский форум — это место, где словно сами собой рождаются инициативы, проходят обкатку масштабные идеи и решения. Например, идея ФинЦЕРТа Банка России структурировалась и получила одобрение профессионального сообщества именно на Уральском форуме.

Хочу пожелать форуму: так держать! А это значит — постоянно искать новое.



На заседаниях яблоку негде упасть

потенциально пригодные для проведения форума, даже провели предварительно один раз конференцию в самом центре Урала, много раз прикидывали разные варианты, но все сошлось только здесь, в Юбилейном. Хотя в Башкортостане и Челябинской области есть очень много замечательных и удивительно красивых мест. Рекомендую посетить.

Крайне велика в создании форума роль руководства Банка России, сумев-

шего поверить в весьма оригинальную идею, и Главного управления безопасности и защиты информации, как основного двигателя вопроса, организатора поддержки и проведения этого мероприятия, а также Ассоциации Российских банков. Организаторы форума неизменно получали от них самую активную поддержку. И это правильно воспринимает банковская среда.

Были и сложности. Когда в первый раз конференцию проводили в актовом

зале санатория, в нем практически не было отопления и работали тепловые пушки, что серьезно мешало слушать докладчиков, а давно не крашенные стены приходилось закрывать рекламными баннерами. Да по-другому и быть не могло, ведь зал до этого не использовался 10 лет. Чувствуете разницу?

Бывали аномальные, даже для южного Урала, холода. Но были и ужины на открытом воздухе при 42 градусах ниже нуля. И на горнолыжных спусках было невозможно кататься, потому что из-за низких температур выключали подъемники, лыжи теряли свои характеристики и свойства, а открытые части лица обжигал мороз.

Но организаторов и энтузиастов проведения форума ничто не останавливало.

Что пожелать форуму и форумчанам? Успехов в работе, нахождения в тренде, здоровья и творческого долголетия, умения решать новые задачи, эффективности и стабильности.

Уверен, что следующее десятилетие будет не менее интересным и эффективным и потребует от нас обязательного участия в этом замечательном мероприятии.

Вершины ждут!



Лев ШУМСКИЙ
руководитель
направления ИБ
АО «Альфа-Банк»

ЧУВСТВО ПОБЕДЫ

Езжу на Уральский форум каждый год. Теперь вот в десятый раз — отмечать заслуженный юбилей. Мне Уральский форум особенно дорог, потому что именно с ним я связываю свой личный и профессиональный рост. Он для меня — как ежегодная веха, своеобразное подведение итогов. Например, на шестом по счету форуме состоялось мое первое выступление перед широкой профессиональной публикой. Незабываемое ощущение.

Мало того, что я тогда впервые вышел на трибуну с серьезной темой, это выступление принесло мне победу в качестве спикера дня. Такую же победу — как лучшего спикера — подарил мне и седьмой форум. А потом были победы в командных соревнованиях по хоккею в валенках, разных интеллектуальных играх... Это были потрясающие по своему накалу баталии. Естественно, успех в соревновательном смысле этого слова сопутствовал мне не каждый год, но Уральский форум так устроен, что даже если ты и не стал в чем-то первым, ты все равно в выигрыше и ощущаешь себя победителем.

Именно этим Уральский форум отличается от других мероприятий в сфере ИБ. Где еще возможно такое отключение от повседневных задач и в то же время тесное общение с коллегами по цеху на волнующие темы? Там в горах, забыв о рутине, ты ощущаешь свой и личный и профессиональный рост. И именно там, далеко от Москвы, начинаешь отчетливо видеть и понимать, как изменяется, в какую сторону движется наша отрасль.



ТРИЕДИНАЯ ЗАДАЧА

КАК ПОВЫСИТЬ КАЧЕСТВО ПОДГОТОВКИ
СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ



Руслан ВЕСТЕРОВСКИЙ
заместитель председателя
Банка России

ПО ПРОГНОЗАМ, ПРИ СУЩЕСТВУЮЩИХ ОБЪЁМАХ ПОДГОТОВКИ В 2020 ГОДУ ДЕФИЦИТ СПЕЦИАЛИСТОВ ПО ИБ СОСТАВИТ ОКОЛО 20 ТЫСЯЧ ЧЕЛОВЕК

Немаловажно, что при этом в стране завершается формирование национальной системы квалификации, которое включает реализацию следующих задач: обеспечение качества разработки профессиональных стандартов, создание основных и дополнительных программ обучения специалистов профильного рынка, а также реализацию этих программ в вузах и учреждениях дополнительного профессионального образования, организацию системы оценки квалификации.

Пути решения большей части этих задач применительно к направлению «финансы и экономика» нам уже понятны. Мы обсуждали их с профессиональным сообществом — с Ассоциацией участников финансового рынка «Совет по профессиональным квалификациям финансового рынка», с которой Банк России заключил соглашение о сотрудничестве. Тем не менее, в сфере информационной безопасности поиск оптимальных организационных и методических путей подготовки и квалификационной оценки персонала продолжается. Эта тема — одна из ключевых на X Уральском форуме по информационной безопасности финансовой сферы, и мы рассчитываем плотно проработать ее со всеми заинтересованными сторонами.

СТРАННОСТИ ДЕФИЦИТА

По данным Минобрнауки, на обучение в государственные образовательные учреждения по группе специальностей «Информационная безопасность» в 2004 году было принято 4,4 тысячи человек, а в 2015 году — 6,3 тысячи. Рост существенный — 43%. Но недостаточный. По прогнозам, при существующих объёмах подготовки в 2020 году дефицит специалистов по ИБ составит около 20 тысяч человек.

Ощутимы ли предвестники такого дефицита сегодня? Результаты опроса кредитных организаций по теме квалифицированных кадров в сфере информационной безопасности показывают, что «голод» на таких специалистов испытывают около 80% банков. Однако причиной респонденты в половине случаев называют не нехватку специалистов, а их низкую зарплату. А если обратиться к рынку труда и сравнить число вакансий в сфере информбезопасности с числом предлагаемых резюме, то обнаружится разница в два порядка в пользу предложений.

Проблема, очевидно, не в количестве специалистов, а в качестве.

Но что такое качество в этом контексте? Качество подготовки специалистов — это результат объединения как ми-

ИНТЕРЕСЫ ОТРАСЛИ И ГОСУДАРСТВА

Формируя миссию, цели и ценности Банка России, мы определили в числе первоочередных задач постоянное наращивание профессиональных компетенций наших сотрудников. При этом поддержание высокой квалификации работников Центрального банка — это лишь часть задачи. Не менее важно, на мой взгляд, найти пути взаимодействия с образовательными институтами, которые призваны поднять уровень квалификации специалистов, необходимых финансовому рынку России.

нимум трех составляющих: адекватных требований к квалификации, учебных программ и их реализации, эффективной системы оценки квалификации.

ТРЕБУЕТСЯ НОВЫЙ ПРОФСТАНДАРТ

Сегодня требования к квалификации формулируются в виде профессиональных стандартов. В области информационной безопасности разработаны и утверждены семь таких стандартов:

- ♦ Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности;
- ♦ Специалист по технической защите информации;
- ♦ Специалист по защите информации в телекоммуникационных системах и сетях;
- ♦ Специалист по защите информации в автоматизированных системах;
- ♦ Специалист по безопасности компьютерных систем и сетей;
- ♦ Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак;
- ♦ Специалист по противодействию технической разведке.

Это достаточно качественные документы, разработанные ведущими организациями в сфере защиты информации. Но вместе с тем, с нашей точки зрения, для кредитно-финансовой сферы нужен не только технический взгляд на проблемы защиты информации, превалирующий в перечисленных стандартах, но также и взгляд из предметной области — финансовой.

Специалисты по информационной безопасности, работающие в финансовых организациях, сопровождают бизнес — и технологические процессы, напрямую связанные с движением денежных средств, и, безусловно, должны быть серьезно подготовлены в финансово-экономической области. Кроме того, работа специалиста по ИБ в кредитно-финансовой сфере должна основываться на знании действующего законодательства и нормативно-правовых актов, в том числе нормативных актов и требований Банка России.

В таком контексте наши специалисты считают необходимым разработку отдельного, специального профессионального стандарта «Специалист по информационной без-

опасности в кредитно-финансовой сфере». Мы обратились к Ассоциации участников финансового рынка с предложением инициировать его разработку.

Работу над семью вышеперечисленными стандартами организовывал Совет по профессиональным квалификациям в области информационных технологий. Однако мы рассчитываем также на тесное взаимодействие с Советом по профессиональным квалификациям финансового рынка, поскольку полагаем, что в данном пограничном случае центр ответственности должен находиться в поле финансового рынка.

БАЗОВЫЕ ОСНОВАНИЯ

Обеспечение информационной безопасности и противодействие компьютерным атакам на финансовом рынке, в том числе при внедрении и использовании инновационных технологий, являются важными задачами государственного уровня. На сегодняшний день существует два базовых документа в этой сфере — «Доктрина информационной безопасности Российской Федерации» и Программа «Цифровая экономика Российской Федерации».

«Доктрина информационной безопасности Российской Федерации», утвержденная Президентом России в декабре 2016 года, констатирует, что 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. Также Доктрина констатирует рост масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере.

Программа «Цифровая экономика Российской Федерации», утвержденная Правительством России в июле 2017 года, предусматривает обеспечение правовых условий для внедрения и использования инновационных технологий на финансовом рынке, включая совершенствование механизмов предоставления финансовых услуг и обеспечение информационной безопасности.

В соответствии с «Доктриной информационной безопасности» Банк России является органом, входящим в систему обеспечения информационной безопасности Российской Федерации, а финансовые организации определяются в качестве участников системы обеспечения информационной безопасности Российской Федерации.

Принимая во внимание стратегический характер этих документов, а также тематическое разделение экономической и информационной безопасности, Банк России считает, что имеются веские основания для разработки отдельного Стандарта для специалистов по информационной безопасности в кредитно-финансовой сфере.

С НАШЕЙ ТОЧКИ ЗРЕНИЯ, ДЛЯ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ НУЖЕН НЕ ТОЛЬКО ТЕХНИЧЕСКИЙ ВЗГЛЯД НА ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ПРЕВАЛИРУЮЩИЙ В ПЕРЕЧИСЛЕННЫХ СТАНДАРТАХ, НО ТАКЖЕ И ВЗГЛЯД ИЗ ПРЕДМЕТНОЙ ОБЛАСТИ — ФИНАНСОВОЙ

ВТОРАЯ СОСТАВЛЯЮЩАЯ— ОБРАЗОВАНИЕ

Согласно логике внедрения профессиональных стандартов на их основе должны разрабатываться федеральные государственные образовательные стандарты, а также основные и дополнительные профессиональные образовательные программы.

Сегодня разработаны девять ФГОС по ИБ:

- ◆ Информационная безопасность;
- ◆ Компьютерная безопасность;
- ◆ Информационная безопасность автоматизированных систем;
- ◆ Информационная безопасность телекоммуникационных систем;
- ◆ Информационно-аналитические системы безопасности;
- ◆ Безопасность информационных технологий в правоохранительной сфере;
- ◆ Криптография;
- ◆ Противодействие техническим разведкам.

Эти ФГОС утверждались в 2016 году примерно в то же время, что и профессиональные стандарты. Можно предположить, что изначально профессиональные стандарты не были положены в основу образовательных стандартов. Кроме того, известно, что ни в 2016, ни в 2017 году образовательные стандарты не перерабатывались в соответствии с профессиональными. Все это является серьезной недоработкой, поскольку такое соответствие должно быть обеспечено, исходя из целей и непосредственных функций профессиональных стандартов.

ОПЫТ ЕСТЬ

Что можно было бы в такой ситуации сделать образовательным учреждениям, обучающим специалистов по информационной безопасности?

Если обратиться к известному нам опыту Совета по профессиональным квалификациям финансового рынка (СПК ФР), то можно было бы прибегнуть к процедуре профессионально-общественной аккредитации образовательных программ. Не так давно СПК ФР аккредитовал четыре образовательных программы бакалавриата и тринадцать образовательных программ магистратуры для Уральского государственного экономического университета, Финансового университета, Российской академии народного хозяйства и государственной службы, Санкт-Петербургского государственного экономического университета и Санкт-Петербургского государственного университета. Тем самым СПК ФР подтвердил соответствие аккредитованных программ профессиональным стандартам. Насколько нам известно, Совет по профессиональным квалификациям в области информационных технологий такой работы ещё не проводил.

512 ЧАСОВ

Полномочным органом, курирующим вопросы образования в сфере ИБ, является Федеральная служба по техническому

БАНК РОССИИ СЧИТАЕТ, ЧТО ИМЕЮТСЯ ВЕСКИЕ ОСНОВАНИЯ ДЛЯ РАЗРАБОТКИ ОТДЕЛЬНОГО СТАНДАРТА ДЛЯ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ

и экспортному контролю (ФСТЭК). По сложившейся практике, ФСТЭК организует разработку и утверждение базовых программ профессиональной переподготовки, которые служат основой для рабочих программ обучения в образовательных учреждениях дополнительного профессионального образования.

Имея в виду профессиональный стандарт «Специалист по информационной безопасности в кредитно-финансовой сфере» и новый вид профессиональной деятельности «Обеспечение информационной безопасности в кредитно-финансовой сфере», Банк России готовит к рассмотрению ФСТЭК и заинтересованными образовательными учреждениями примерную программу профессиональной переподготовки. Её продолжительность 512 часов.

ТРЕТЬЯ СОСТАВЛЯЮЩАЯ— ОЦЕНКА КВАЛИФИКАЦИИ

Завершающее звено системы обеспечения качества специалистов — это оценка квалификации. В стране создаются центры оценки квалификации, которые проводят независимую оценку на основе оценочных средств, разработанных в соответствии с профессиональными стандартами.

Правовой основой системы оценки квалификации является ФЗ-238 от 3 июля 2016 года «О независимой оценке квалификации», в соответствии с которым с 1 июля 2019 года все параллельно существующие системы оценки квалификации, за исключением системы оценки, предусмотренной законом, должны прекратить своё существование.

Банк России сейчас отвечает за работу системы аттестации специалистов финансового рынка. Она заметно отличается от внедряемой системы независимой оценки квалификации, поэтому новации, касающиеся оценки квалификации, не могут нас не беспокоить. Мы ищем пути гармонизации отношений между этими двумя системами, в том числе в рамках Соглашения о сотрудничестве между Банком России и Ассоциацией участников финансового рынка, о котором говорилось выше.

Решая эту задачу, мы принимаем во внимание и вопросы, связанные с аттестацией специалистов по информационной безопасности в кредитно-финансовой сфере. Задача сложная, но время для её решения пришло.

ФИКСИРОВАТЬ, РАССЛЕДОВАТЬ, ПРЕДУПРЕЖДАТЬ



Артем СЫЧЕВ
заместитель начальника
Главного управления
безопасности и защиты
информации
Банка России

ПОДРАЗДЕЛЕНИЕ ТЕХНИЧЕСКОГО АНАЛИЗА ФИНЦЕРТ БАНКА РОССИИ ЗАНИМАЕТСЯ КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКОЙ ИНЦИДЕНТОВ В ФИНАНСОВОЙ СФЕРЕ

Подразделение технического анализа является структурным подразделением ФинЦЕРТ (Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере) Банка России. Подразделение было создано в декабре 2016 года и прошло период становления, в ходе которого активно подбирались кадры, закупалось специальное оборудование и программное обеспечение, вырабатывались основные подходы и методики, подбирались кадры. Что представляют собой подразделение технического анализа и его деятельность сегодня?

СФЕРА ОТВЕТСТВЕННОСТИ

В настоящее время в подразделении технического анализа работают высококвалифицированные специалисты — аналитики вредоносных программ, реверс-инженеры, компьютерные криминалисты. В ближайшее время будут завершены процедуры закупки необходимого оборудования. Основные направления работы подразделения — анализ вредоносных программ, о которых сообщают в ФинЦЕРТ участники информационного обмена; оказание технической и консультативной помощи кредитным организациям, подвергшимся компьютерным атакам; проведение криминалистических исследований по запросам правоохранительных органов, проводящих проверки или расследующих уголовные дела по фактам компьютерных атак на организации кредитно-финансовой сферы.

Объем работ пока невозможно сравнить с «аналогичными периодами» прошлых лет, так как их не было, но можно уже уверенно утверждать, что скучать нашим сотрудникам не приходится: злоумышленники не дают. В отчетной документации ФинЦЕРТ содержится информация, в основном, о технических аспектах проведенных расследований. Потому, что в задачи подразделения технического анализа не входит рассмотрение в каком-либо виде «юри-

дических аспектов» расследований, это — прерогатива правоохранительных органов, с которыми мы сотрудничаем по реальным уголовным делам. Но при этом мы, разумеется, ориентируемся и на практику правоохранительных органов, изучаем доступные методики проведения исследований, учитываем решения высших судебных органов в касающейся нас части.

Заключения подразделения технического анализа используются в работе правоохранительных органов и в судебных процессах. За небольшой период, что существует подразделение, проведено уже более 20 криминалистических исследований по самым разным материалам и уголовным делам. Специалисты подразделения за этот год увидели и детально изучили все основные схемы атак, которые, применялись. Также ими разобраны вредоносные (и не только) программы и аппаратные средства, используемые для хищений денежных средств, о которых вы неоднократно слышали из новостных сообщений и читали в отчетах организаций, менее стесненных обязательствами конфиденциальности.

ПРОЦЕССУАЛЬНОЕ СОДЕЙСТВИЕ

Порядок привлечения специалистов подразделения технического анализа к процессуальным действиям строго регламентирован Уголовно-процессуальным кодексом Российской Федерации. В случаях, когда сотрудники подразделения участвуют в каких-либо действиях в качестве специалистов, их задачи формулируется ст. 58 УПК РФ.

**В ЗАДАЧИ ПОДРАЗДЕЛЕНИЯ
ТЕХНИЧЕСКОГО АНАЛИЗА НЕ ВХОДИТ
РАССМОТРЕНИЕ В КАКОМ-ЛИБО
ВИДЕ «ЮРИДИЧЕСКИХ АСПЕКТОВ»
РАССЛЕДОВАНИЙ**

А именно: «Содействие в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию». При этом оформление процессуальных документов, а следовательно, и решение юридических процессуальных вопросов, возлагается на следователей или действующих по их поручениям сотрудников оперативных подразделений.

В настоящее время практика работы подразделения технического анализа только формируется. Однако по накопленному на сегодня опыту мы уже можем присоединиться к большинству представителей профессионального, экспертного и юридического сообщества, которые говорят о несовершенстве ряда положений Федерального закона от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». Прежде всего, в части регулирования судебно-экспертной деятельности лиц, не являющихся государственными судебными экспертами. Как известно, предложения об изменении данного закона или о принятии нового закона обсуждаются не один год.

ОБМЕН КРИМИНАЛИСТИЧЕСКОЙ ИНФОРМАЦИЕЙ

Подразделение технического анализа ФинЦЕРТ сотрудничает с аналогичными подразделениями государственных органов — ФСБ России, МВД России и т.п., — а также коммерческих компаний преимущественно в форме информационного взаимодействия.

Мы обмениваемся с государственными судебно-экспертными учреждениями и информацией общего характера — и о методиках проведения криминалистических исследований, и об отдельных, наиболее интересных, резонансных случаях из повседневной практики. Для нас ценен опыт, который накоплен государственными учреждениями. В то же время преимущество ФинЦЕРТ — это обладание информацией о вредоносных программах, используемых при совершении преступлений в отношении организаций кредитно-финансовой сферы и их клиентов.

Что касается коммерческих лабораторий, с которыми взаимодействует ФинЦЕРТ, то большинство из них является подразделениями известных компаний, оказывающих широкий спектр услуг и поставляющих различные продукты в сфере информационной безопасности. С ними ФинЦЕРТ заключает соглашения о сотрудничестве в сфере противодействия компьютерным атакам, обменивается информацией в рабочем порядке.

Надо отметить, что ФинЦЕРТ никоим образом не конкурирует с коммерческими компаниями, поскольку, в отличие от них, не оказывает каких-либо платных услуг. Мы действуем в разных плоскостях, а если какие-то направления совпадают, например, исследовательская деятельность

НАДО ОТМЕТИТЬ, ФИНЦЕРТ НИКОИМ ОБРАЗОМ НЕ КОНКУРИРУЕТ С КОММЕРЧЕСКИМИ КОМПАНИЯМИ, ПОСКОЛЬКУ, В ОТЛИЧИЕ ОТ НИХ, НЕ ОКАЗЫВАЕТ КАКИХ-ЛИБО ПЛАТНЫХ УСЛУГ

подразделения, то это идет только на пользу общему делу защиты кредитно-финансовой системы.

ПОВЫШЕНИЕ ПРОФЕССИОНАЛИЗМА

Деятельность подразделения технического анализа ФинЦЕРТ способствует повышению грамотности сотрудников коммерческих банков в юридических вопросах компьютерных инцидентов. Сотрудники подразделения, как и многие другие сотрудники ФинЦЕРТ, постоянно участвуют в различных обучающих мероприятиях, проводимых, в том числе, и для сотрудников банков. В частности, в 2017 году несколько раз проводились лекции и семинары для сотрудников МВД России, для представителей национальных банков стран ЕвразЭС. Ряд мероприятий предназначен для сотрудников кредитных организаций.

Однако подчеркнем ещё раз: собственно вопросы права находятся вне компетенции подразделения. Тем не менее, при необходимости мы всегда готовы дать разъяснения по порядку сохранения будущих вещественных доказательств для предоставления правоохранительным органам, проведения криминалистических исследований, трактовке их результатов в свете доказывания по уголовным делам.

Мы настоятельно рекомендуем всем представителям банков, столкнувшимся с инцидентами в сфере информационной безопасности, требующими привлечения правоохранительных органов, применять положения нашего документа — Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств» СТО БР ИББС-1.3-2016.

* * *

В будущем, безусловно, мы продолжим максимально активно набирать опыт, расширять свою информационную и исследовательскую базу, будем стараться оказывать необходимую помощь как участникам информационного обмена, так и правоохранительным органам, ведущим нелёгкую борьбу с преступлениями, направленными против организаций кредитно-финансовой сферы и их клиентов. Одна из задач на следующий год — разработка и утверждение собственных методик исследования вредоносных программ и иной компьютерной информации.



**Александр
ВЕЛИГУРА**
председатель
Комитета по банковской
безопасности АРБ

ГОСТ Р 57580.1-2017. ПЕРВЫЙ НАЦИОНАЛЬНЫЙ И ДРУГИЕ

НОВЫЕ СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В августе 2017 года был издан приказ Росстандарта, вводящий в действие с 1 января 2018 года ГОСТ Р 57580.1-2017¹ — по-видимому, первый оригинальный (не являющийся гармонизированным международным стандартом) национальный стандарт по защите информации в организациях кредитно-финансовой сферы (далее — Стандарт). Его появление было ранее анонсировано в ряде выступлений представителей ГУБиЗИ Банка России, в которых, кроме того, излагался общий замысел использования данного документа. Что представляет собой Стандарт и что ожидает банки, другие финансовые организации, а также поставщиков услуг в области защиты информации после его введения? Что можно и нужно предпринять?

1. НА СТАНДАРТ БУДУТ ССЫЛАТЬСЯ НОРМАТИВНЫЕ ДОКУМЕНТЫ БАНКА РОССИИ

Предлагаемый порядок применения Стандарта изложен в его разделах 1 и 6. Так, в разделе 1 «Область применения» указано:

«Область применения настоящего стандарта, определяющая обязанность финансовых организаций применять меры защиты информации, реализующие один из уровней защиты информации для конкретной совокупности объектов информатизации, ... устанавливается в нормативных актах Банка России путем включения нормативной ссылки на настоящий стандарт».

Таким образом, то, к каким объектам и какие меры защиты, описанные в Стандарте, применять, будет указано в нормативных актах Банка России, которые, возможно, появятся во второй половине 2018 года.

В более развернутом виде предлагаемый порядок применения Стандарта изложен в его разделе 6 «Общие положения». (Раздел 5 «Назначение и структура стандарта» отвечает своему названию только в отношении структуры).

¹ ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер

2. ПРЕДЛАГАЕМЫЙ ПОРЯДОК ПРИМЕНЕНИЯ СТАНДАРТА

2.1 Уровни защиты информации. Вводятся три уровня защиты информации:

- ♦ уровень 3 — минимальный;
- ♦ уровень 2 — стандартный;
- ♦ уровень 1 — усиленный.

2.2 Контур (домены) безопасности. В финансовой организации формируется один или несколько контуров безопасности, для которых могут быть установлены разные уровни защиты информации.

2.3 Уровни защиты информации. Уровень защиты информации финансовой организации для конкретного контура безопасности устанавливается нормативными актами Банка России на основе учета ряда факторов, указанных в Стандарте (определение того, как именно они будут учитываться — прерогатива ЦБ, финансовая организация будет вынуждена принять это как данность).

2.4 Выбор состава мер. Согласно Стандарту, выбор финансовой организацией мер защиты информации включает следующие шаги.

2.4.1 Выбор мер защиты информации из числа приведенных в разделах 7–9 Стандарта. Согласно изложенному, это делается, исходя из заданных в нормативных документах ЦБ требованиях к контурам безопасности и уровням защиты для них.

2.4.2 Адаптация, при необходимости, выбранного состава и содержания мер защиты информации с учетом модели угроз и нарушителей и структурно-функциональных характеристик объектов информатизации. В какой сте-

**ТО, К КАКИМ ОБЪЕКТАМ И КАКИЕ МЕРЫ
ЗАЩИТЫ, ОПИСАННЫЕ В СТАНДАРТЕ,
ПРИМЕНЯТЬ, БУДЕТ УКАЗАНО
В НОРМАТИВНЫХ АКТАХ БАНКА РОССИИ,
КОТОРЫЕ, ВОЗМОЖНО, ПОЯВЯТСЯ ВО
ВТОРОЙ ПОЛОВИНЕ 2018 ГОДА**

пени возможна данная адаптация, кто и как будет оценивать актуальность и адекватность модели угроз и соответствие ей адаптированных мер, пока неясно. Несмотря на то, что Стандарт включает Приложение А «Основные положения базовой модели угроз и нарушителей», данное Приложение, на наш взгляд, не позволяет ответить на указанные вопросы (содержательная часть Приложения представляет собой описание только источников угроз). В отношении учета «структурно-функциональных характеристик объектов информатизации» определенность еще меньше. Отсутствуют и обычные для Стандарта ссылки на грядущие нормативные документы Банка России.

Наряду с этим в разделе 6 Стандарта имеется подраздел 6.4, гласящий:

«При невозможности технической реализации отдельных выбранных мер защиты информации, а также с учетом экономической целесообразности на этапах адаптации (уточнения) базового состава мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию угроз безопасности информации, определенных в модели угроз и нарушителей безопасности информации финансовой организации».

В этом случае финансовой организацией должно быть проведено обоснование применения компенсирующих мер защиты информации».

То есть на этапе адаптации, кроме модели угроз, можно учитывать еще (не)возможность технической реализации тех или иных мер, а также их экономическую (не)целесообразность (!). Здесь, правда, есть некоторая неопределенность в обосновании применения компенсирующих мер.

По-видимому, Банк России, оставляя эти неопределенности, дает финансовым организациям (да и себе), некоторую свободу маневра, чтобы в ходе практического применения Стандарта уточнить эти положения. Пока можно только приветствовать заложенную в Стандарт возможность варьирования состава и содержания мер защиты с учетом модели угроз и экономических соображений.

2.4.3 Исключение ... мер, не связанных с используемыми информационными технологиями. Данное положение в силу очевидной разумности комментариев не требует.

2.4.4 Дополнение, при необходимости... мерами, обеспечивающими выполнение требований к защите информации, установленных нормативно-правовыми актами. Очевидное требование соответствовать правовым нормам, даже если их нет в Стандарте.

3. ТРЕБОВАНИЯ К МЕРАМ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к составу мер защиты информации, приведенные в Стандарте, структурированы следующим образом.

Раздел 7 «Требования к системе защиты информации» содержит 343 меры, объединенные в 8 процессов защиты информации. Раздел 8 «Требования к организации и управлению защитой информации» содержит 37 мер, составляющие 4 направления защиты информации. В разделе 9 «Требования к защите информации на этапах жизненного цикла ав-

томатизированных систем и приложений» приведено 28 мер, процессы и направления здесь не выделяются.

Все меры (итого их 408) имеют трехуровневую градацию в соответствии с уровнем защиты информации, соответствие которому необходимо обеспечить.

Уровень отражается в способе реализации меры. Их предусмотрено три:

- ♦ неприменение;
- ♦ реализация путем применения организационной меры;
- ♦ реализация путем применения технической меры.

Организационные меры можно заменять техническими (но не наоборот).

Более того, в п.6.11 Стандарта указано:

«Финансовой организации рекомендуется обеспечивать автоматизацию предоставляемых финансовых услуг, бизнес-процессов, технологических процессов и (или) обработку защищаемой информации с использованием АС и приложений...»

Обязанность обеспечения финансовой организацией автоматизации бизнес-процессов, технологических процессов и (или) обработки защищаемой информации только с применением АС устанавливается требованиями нормативных актов Банка России».

В приведенных ссылках просматривается общая идея — более высокая степень защищенности связана с более высоким уровнем автоматизации и использованием технических мер вместо организационных. При этом в отношении определенных процессов и обработки информации Банк России может обязать финансовую организацию автоматизировать их.

4. ОЦЕНКА СООТВЕТСТВИЯ ПОЛОЖЕНИЯМ СТАНДАРТА

4.1 Используемый понятийный аппарат. Согласно Стандарту, оценка соответствия, точнее, несоответствия его положениям называется «оценкой остаточного операционного риска (финансового эквивалента возможных потерь), вызванных неполным или некачественным выбором и применением мер защиты информации, требования к содержанию базовому составу которых установлены в разделах 7, 8, 9 настоящего стандарта» (далее — Оценка). Таким образом, речь идет не об остаточном операционном риске вообще, а о той его части, которая связана с (не) применением мер защиты информации, предусмотренных Стандартом. В отличие от терминологии, применяемой в Комплексе стандартов Банка России СТО БР ИББС и других стандартах, например серии ISO 27xxx, здесь изменен акцент — речь идет не о соответствии/несоответствии требованиям рассматриваемого стандарта, а об остаточном риске после применения мер в том виде, как это сделано.

4.2 Схема выполнения Оценки. Согласно Стандарту, Оценка осуществляется в соответствии с процедурой, определенной требованиями нормативных актов Банка России, на основе «оценки показателей соответствия реализации системы защиты информации финансовой организации требованиям Стандарта». В свою очередь, оценку показателей

соответствия реализации системы защиты информации финансовой организации требованиям Стандарта следует осуществлять в соответствии с методикой, приведенной в «соответствующем национальном стандарте».

Таким образом, согласно Стандарту Оценка производится в два этапа — сначала с помощью методики из «соответствующего национального стандарта» оцениваются определенные там показатели, затем из этих показателей согласно процедуре, определенной нормативным актом Банка России, получается собственно оценка остаточного операционного риска (финансового эквивалента возможных потерь).

На момент написания данной статьи проект упомянутого «соответствующего национального стандарта»² разработан и проходит в установленном порядке экспертизу и утверждение.

После Оценки происходит обработка остаточного операционного риска в соответствии с процедурой, определенной требованиями нормативных актов Банка России.

Итак, общая процедура использования Стандарта выглядит следующим образом (см. табл. 1).

5. ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

Приведенный краткий обзор Стандарта показывает, что в практике его будущего применения, несмотря на заложенную в порядок его использования директивность, имеется определенный простор для творчества.

Есть возможность использования моделей угроз, и для выбора моделей имеется достаточная свобода.

Формулировки многих мер защиты допускают варианты их конкретной реализации.

Поскольку одной из основных целей данного стандарта является «достижение адекватности состава и содержания мер защиты информации, применяемых финансовыми организациями, актуальным угрозам безопасности информации и уровню принятого финансовой организацией операционного риска (риск-аппетиту)», то можно считать, что финансовым организациям предоставлена определенная свобода в выборе риск-аппетита, разработки модели угроз и выборе подхода к оценке рисков.

Как отмечалось выше, имеется возможность выполнять «адаптацию (уточнение), при необходимости, выбранного состава и содержания мер защиты информации с учетом модели угроз и нарушителей безопасности информации финансовой организации и структурно-функциональных характеристик объектов информатизации, в том числе АС».

Как известно, одним из решений по инкапсуляции описания угроз (рисков), требований к мерам и средствам защиты для противодействию угрозам (снижения рисков),

В соответствии с актами Банка России

1. Определение области применения
2. Выделение контуров ИБ
3. Установление уровней защиты для контуров

6. Оценка остаточного операционного риска и его обработка

В соответствии с ГОСТ Р 57580.1

4. Применение мер защиты информации

В соответствии с ГОСТ Р 57580.2

5. Оценка показателей соответствия реализации мер

Таблица 1. Общая процедура использования Стандарта

нормативных требований, требований по достижению уверенности в корректности реализации мер и средств защиты, обоснованию необходимости и достаточности предлагаемых мер для противодействия описанным угрозам является использование **заданий по безопасности (ЗБ) и профилей защиты (ПЗ)** для продуктов ИТ и автоматизированных систем, описанных в стандартах ГОСТ Р ИСО/МЭК 15408³ (известных как «Общие критерии») и ГОСТ Р ИСО/МЭК ТО 19791–2008⁴, являющимся дополнением к «Общим критериям».

* * *

Для определения возможности применимости «Общих критериев» и ГОСТ Р ИСО/МЭК ТО 19791–2008 целесообразно подготовить проекты пакетов требований безопасности для включения в будущие ПЗ, изложив требования Стандарта в терминах «Общих критериев». В условиях необходимости подготовки нормативных документов Банка России, регламентирующих целый ряд аспектов применения Стандарта, разработка таких документов может стать одним из направлений взаимодействия профессионального сообщества и регулятора в вопросах практического применения Стандарта и повышения защищенности и киберустойчивости финансовых организаций.

³ ГОСТ Р ИСО/МЭК 15408–2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. ГОСТ Р ИСО/МЭК 15408–2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. ГОСТ Р ИСО/МЭК 15408–2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

⁴ ГОСТ Р ИСО/МЭК ТО 19791–2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем

² Предполагаемое обозначение — ГОСТ Р 57580.2

В ПОИСКАХ СИНЕРГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ ЦИФРОВОЙ ЭКОНОМИКИ

Тема главной дискуссии X Уральского форума — «Информационная безопасность как неотъемлемая часть цифровой экономики». BIS Journal попросил ее ведущую, президента ГК InfoWatch, а по совместительству руководителя рабочей группы по подготовке раздела «Информационная безопасность» государственной программы «Цифровая экономика Российской Федерации» Наталью Касперскую рассказать, как ведется работа над программой. Наталья Ивановна согласилась, но с одним условием: большого материала не будет — только анонс панельной дискуссии на Урале. «Тема настолько большая, важная и непростая, что на данной стадии коллективное мнение нашей отрасли важнее мнений отдельных личностей», — сказала она. Предлагаем вашему вниманию фрагменты интервью, а полный текст вместе с отчетом о дискуссии читайте в BIS Journal № 2/2018.

ЧТО ТАКОЕ ПРОГРАММА «ЦИФРОВАЯ ЭКОНОМИКА»

Это попытка найти синергию между бизнесом, который использует и развивает информационные технологии, и государством, которое тоже хочет эти технологии использовать и развивать. Программа предполагает создание работающего механизма: планы должны быть гибкими, чтобы их можно было корректировать, и при этом осуществлялось бы своевременное и эффективное финансирование. Важная задача «Цифровой экономики» — обозначить на государственном уровне приоритетные направления, куда разработчики и производители программных продуктов направят свои усилия.

МЕХАНИЗМ УПРАВЛЕНИЯ ПРОГРАММОЙ «ЦИФРОВАЯ ЭКОНОМИКА»

На уровне государства и ряда крупнейших предприятий была создана автономная некоммерческая организация «Цифровая экономика», которая координирует всю работу по программе. Также создана специальная правительственная комиссия по цифровой экономике. Программой «Цифровая экономика» предусмотрено пять на-

правлений, одно из которых — информационная безопасность.

Как и по остальным направлениям, работа по ИБ организована следующим образом — существует центр компетенции, это Сбербанк, у которого сильная экспертиза в сфере ИБ и который входит в состав учредителей АНО «Цифровая экономика». Параллельно работает профильная рабочая группа, которая формирует отраслевые заключения на проекты центра компетенции.

КАК БЫЛА ПОСТРОЕНА РАБОТА ПО НАПРАВЛЕНИЮ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Правительство РФ определило 14 направлений деятельности по теме «Информационная безопасность». Центр компетенции собрал пул экспертов, которые принимали непосредственное участие в разработке плана действий. Сформированные планы направлялись в рабочую группу. Рабочая группа — это, с одной стороны, надзорно-контролирующий, с другой — корректирующий орган. Возглавить эту группу предложили мне как представителю индустрии.

В состав рабочей группы вошли представители госорганов, компаний-разработчиков, причем как разработчиков средств информационной безопасности, так и разработчиков IT-систем, и заказчиков. Информационная безопасность тесно связана со всеми другими направлениями программы. По направлению ИБ в программе, утвержденной правительством РФ, особое внимание уделяется трем темам: регулирование в области ИБ, импортозамещение и поддержка отечественных разработчиков программных продуктов, а также международное сотрудничество в области информационной безопасности.

ЦЕНТР КОМПЕТЕНЦИИ

Центр компетенции в лице «Сбербанка» проделал колоссальную работу. Они обладают серьезными ресурсами, по каждому из 14 направлений они определили ответственного человека, который собрал экспертов отрасли. По каждому направлению были написаны планы конкретных мероприятий. Это феноменальная работа, которая была сделана всего за месяц.



Наталья КАСПЕРСКАЯ
президент ГК InfoWatch

ЦИФРОВАЯ ЭКОНОМИКА: ОТ СТРАТЕГИИ К ТАКТИКЕ

КАК РАБОТАЕТ ЦЕНТР КОМПЕТЕНЦИИ ПРОГРАММЫ
«ЦИФРОВАЯ ЭКОНОМИКА РФ» НА БАЗЕ СБЕРБАНКА?



Игорь НОВИКОВ
начальник Центра
внутрикорпоративного
взаимодействия
Департамента
безопасности
ПАО Сбербанк

31 августа 2017 года на заседании подкомиссии по цифровой экономике Правительства РФ Сбербанк был определен центром компетенции по направлению «Информационная безопасность». Сегодня внутри банка за реализацию Программы «Цифровая экономика РФ» отвечает Центр внутрикорпоративного взаимодействия Департамента безопасности. Его сотрудники являются менеджерами экспертных групп Программы, готовят все материалы, организуют встречи экспертов, участвуют в рабочих совещаниях в министерствах и ведомствах.

На вопросы BIS Journal отвечает начальник Центра Игорь Новиков.

— Как вы оцениваете то, что Сбербанк стал центром компетенции Программы «Цифровая экономика РФ» по направлению «Информационная безопасность»?

— Это событие играет значимую роль не только для Сбербанка. С одной стороны, оно свидетельствует о том, что деловое сообщество высоко оценивает компетенции Банка в области кибербезопасности, с другой — активное участие в совещаниях экспертных групп представителей более 200 компаний, представляющих самые разные отрасли экономики, говорит о важности данного направления для современного бизнеса.

— Как это происходило в событийном плане?

— Термин «цифровая экономика» был введен в употребление ещё в 1995 году американским учёным Николасом Негропonte. Сейчас этим термином пользуются повсеместно. Он подразумевает использование цифровых технологий для повышения конкурентоспособности и благосостояния страны. В 2016 году по предложению Всемирного экономического форума было проведено исследование экономических и инновационных результатов использования цифровых технологий. Согласно этому исследованию Россия заняла 38 место с большим отрывом от стран-лидеров, таких, как Финляндия, Швей-

цария, Швеция, Израиль, Сингапур и др. Чтобы переломить эту ситуацию 28 июля 2017 Правительство РФ утвердило программу «Цифровая экономика». А 31 августа Сбербанк был определён центром компетенции по направлению «Информационная безопасность». Руководителем центра компетенции был назначен заместитель Председателя Правления Сбербанка Станислав Кузнецов, а рабочую группу по этому направлению возглавила Наталья Касперская (ГК InfoWatch).

— Расскажите, пожалуйста, о первых впечатлениях после знакомства с тем, чем вам предстояло заниматься?

— Тот факт, что Сбербанк возглавил центр компетенции, куда входят представители наиболее технологических компаний и организаций России для работы по направлению «Информационная безопасность» программы «Цифровая экономика», оставил двойные впечатления. С одной стороны, лестно осознавать, что мы участвуем в работе по обеспечению информационной безопасности цифровой экономики России, а с другой — мы очень хорошо знакомы с проблемами во взаимодействии бизнеса и государства в этой сфере и понимаем всю сложность поставленных перед экспертными группами задач.

— Не кажется ли вам, что одного центра компетенции недостаточно?

— Думаю, что нет. Центр компетенции — это прежде всего открытая площадка, своего рода интегратор для консолидации экспертного сообщества и формирования единого пакета материалов по соответствующему направлению. Фактуру для работы дают компетентные эксперты со всей России, которые самостоятельно изъявили желание работать в составе ЦК.

— Не перекраивает ли Сбербанк программу «под себя»?

— Нет, в данном формате это невозможно. Сбербанк организует работу экспертных групп, а также взаимодействие с другими центрами компетенции и государственными институтами. Стоит подчеркнуть, что совещание экспертных



групп — открытый процесс, в котором принимает участие большое количество представителей разных областей бизнеса. При этом представители Сбербанка являются равноправными участниками экспертного сообщества.

— Можете описать реальный фронт работ, который перед вами открылся?

— Фронт работ по подготовке плана мероприятий был существенно расширен за счет того, что изначально экспертным сообществом была проведена всесторонняя диагностика состояния ИБ на уровне государства. Очевидно, что проделанная на настоящий момент работа является стартовой площадкой для дальнейшего обсуждения развития цифровой экономики страны. Требуют дальнейшей проработки и совместного обсуждения многие вопросы: поиск архитектурных решений и способов внедрения сквозных технологий, совершенствование законодательства. Однако тот факт, что экспертное сообщество эту работу начало, дает нам всем надежду на успех.

— Что составляло главные трудности?

— Самое тяжелое в работе при формировании плана мероприятий — это найти компромисс. В первую очередь это связано с тем, что в этом процессе принимает участие большое количество специалистов. Их точки зрения на предлагаемые мероприятия часто разнятся. Кроме того, нельзя не упомянуть о конфликте интересов представителей бизнеса и государства. Несмотря на эти трудности, нам удалось сформировать сбалансированный план мероприятий, учитывающий позиции различных сторон.

САМОЕ ТЯЖЕЛОЕ В РАБОТЕ ПРИ ФОРМИРОВАНИИ ПЛАНА МЕРОПРИЯТИЙ — ЭТО НАЙТИ КОМПРОМИСС. В ПЕРВУЮ ОЧЕРЕДЬ ЭТО СВЯЗАНО С ТЕМ, ЧТО В ЭТОМ ПРОЦЕССЕ ПРИНИМАЕТ УЧАСТИЕ БОЛЬШОЕ КОЛИЧЕСТВО СПЕЦИАЛИСТОВ

— Говорят, «дьявол в деталях». Много ли их было?

— Мы вынуждены уделять повышенное внимание деталям, чтобы быть однозначно понятыми. Надеюсь, что эта ситуация начнёт меняться к концу 2018 года, когда появятся нормативные правовые акты, закрепляющие терминологию и понятийный аппарат.

— Как строилась работа? Как проходила?

— Конструктивно. Было проведено более 20 заседаний экспертных групп на различных площадках, куда вошли Сбербанк, АНО «Цифровая экономика», Аналитический центр при Правительстве РФ и Минкомсвязь России. Параллельно менеджеры групп Центра компетенции проводили рабочие совещания с экспертами по каждой из задач. В результате проделанной работы был составлен одобренный Правительством РФ 18 декабря 2018 года план мероприятий по направлению «Информационная безопасность».

— Далеко ли, на ваш взгляд, удалось продвинуться в масштабах общей запланированной работы?

— У нас хороший результат. Центр компетенции выполнил все задачи, которые стояли до конца 2017 года: план мероприятий, как я уже сказал ранее, одобрен Правительством РФ. Однако мы не собираемся останавливаться на достигнутом — 2018 год будет не менее насыщенным. Мы будем заниматься уточнением мероприятий, входящих в план, мониторингом их выполнения, прорабатывать с бизнесом новые предложения и направления развития.

— Назначен ли конкретный срок окончания работы над программой и в частности над направлением ИБ?

— Программа «Цифровая экономика» рассчитана на период с 2018 по 2024 годы. Вместе с тем, действующий план мероприятий завершается в 2020 году. Таким образом, нас ждет еще один этап работ по формированию мероприятий на период с 2021 по 2024 годы.

— Можно ли сравнить утвержденную Д. Медведевым программу с эскизом, а то, чем занимаетесь вы, рабочим проектом?

— Я бы так не сказал. Цели и задачи направления «Информационная безопасность» остались неизменными. План мероприятий, конечно, претерпел определенные изменения в ходе работы экспертного сообщества, но в большей степени это уточнения (объединения, удаления, расширения и конкретизация) вех, предусмотренных программой, утвержденной распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р. По нашему мнению, это рабочий документ, к реализации которого необходимо приступить, начиная с 2018 года.

— Как правило, рабочий проект значительно отличается от первоначального. А в вашем случае? Многое ли изменилось? Что конкретно?

— Произошли значительные изменения. Например, в сентябре 2017 года в проекте плана мероприятий было 182 вехи, в декабре 2017 года — уже 136; количество мероприятий, первоначально разработанных экспертным сообществом, сокращено с 585 до 396; предложения по бюджетным затратам снижены более чем в два раза. В настоящее время план содержит 396 мероприятий.

— Что на сегодняшний день представляет собой программа в части «Информационная безопасность»?

— Это достижение трёх целей: по обеспечению единства, устойчивости и безопасности

информационно-телекоммуникационной инфраструктуры; технической, организационной и правовой защиты личности, бизнеса и государственных интересов в условиях цифровой экономики; интересов РФ по вопросам информационной безопасности при интеграции в цифровую экономику.

— Насколько ИБ увязывается с другими частями программы?

— Хороший вопрос. На первоначальном этапе формирования плана мероприятий возникали трудности по согласованию предложений с другими направлениями программы, в частности «Нормативное регулирование», «Информационная инфраструктура», «Кадры и образование». Мы провели совместную работу с курирующими данные направления центрами компетенции, сформулировали и направили для включения в разрабатываемые ими планы свои предложения. В ряде случаев работали компромиссные варианты для решения общих проблем. В дальнейшем для решения спорных вопросов в ходе реализации планов по направлениям программы предполагается регулярно проводить совместные совещания.

— Предусматривается ли программой создание национальной испытательной лаборатории микроэлектроники?

— Нет, план не предусматривает создание такой лаборатории.

— В последнее время ИБ все чаще сравнивают с иммунной системой ИТ-проекта. Насколько корректно такое сравнение? Чем вызвано его появление (раньше оно не звучало)?

— Все достаточно просто. Любой организм нуждается в защите. Лучший образец такой защиты в живой природе — иммунная система, которая способна выявлять опасные для организма объекты до того, как началось заболевание. Поэтому для укрепления иммунной системы ИТ-проекта необходимо развивать и встраивать в его структуру алгоритмы и технологии ИБ. И чем раньше это будет сделано, тем лучше.

— Если сравнение корректно, нашел ли такой подход свое отражение в программе?

— Несомненно. В мероприятиях эта тенденция прослеживается.

— Можно ли говорить о том, что система ИБ Сбербанка — это прообраз цифровой экономики в части ИБ?

— Не совсем так. Сбербанк наравне со всеми участниками рабочих групп вносил свои предложения в план мероприятий, и далеко не все

396

мероприятий
содержатся в плане
направления «Информационная безопасность» программы
«Цифровая экономика»

из них нашли в нём свое отражение. Например, не нашло поддержки предложение Сбербанка по созданию Национального центра киберзащиты. А между тем существует очень серьезная проблема обмена информацией между бизнесом и государством, которую можно было бы с помощью создания такого центра решить. Кроме того, в план мероприятий не было включено предложение по созданию Академии кибербезопасности, которая могла бы помочь с решением проблемы кадрового голода в сфере ИБ.

— **Каким вкладом в программу «Цифровая экономика» вы можете гордиться лично?**

— На настоящий момент нам удалось сделать самое важное — сформировать экспертное сообщество, куда вошли более 400 представителей различных отраслей бизнеса. В ходе работы сообщество определило основные проблемы в сфере ИБ и сформировало «дорожную карту» по их решению. По мере появления и развития новых технологий будет требоваться корректировка программы. У нас есть все для того, чтобы продолжить начатую работу. Мы надеемся на дальнейшее плодотворное сотрудничество экспертного сообщества, государственных структур и АНО «Цифровая экономика» и верим в успех начатого дела.

— **Заложены ли в программу какие-то принципиально новые, фантастические на сегодня для массовой ИБ, решения?**

— В ходе формирования плана мероприятий таких решений постарались избежать.

— **Реальны ли, на ваш взгляд, сроки, обозначенные в программе?**

— Программой предусмотрен период до 2024 года. Кроме того, повторюсь, предполагается внесение соответствующих уточнений и изменений при необходимости. Относительно реальности: в период индустриализации в 20-х годах прошлого века в течение семи лет за счёт энтузиазма общества и поддержки государства были решены куда более значимые для страны задачи.

— **Какие серьезные изменения ждут сферу ИБ в течение этого срока?**

— Изменения будут касаться в первую очередь обеспечения устойчивости и безопасности функционирования информационных систем и технологий, обеспечения защиты прав и законных интересов бизнеса в условиях цифровой экономики. Во-первых, в части создания эффективных механизмов государственного регулирования и поддержки в области ИБ при интеграции национальной цифровой экономики в международную экономи-

НА НАСТОЯЩИЙ МОМЕНТ НАМ УДАЛОСЬ СДЕЛАТЬ САМОЕ ВАЖНОЕ — СФОРМИРОВАТЬ ЭКСПЕРТНОЕ СООБЩЕСТВО, КУДА ВОШЛИ БОЛЕЕ 400 ПРЕДСТАВИТЕЛЕЙ РАЗЛИЧНЫХ ОТРАСЛЕЙ БИЗНЕСА

ку. Во-вторых, в части создания технических инструментов, обеспечивающих безопасное информационное взаимодействие граждан в условиях цифровой экономики. И наконец, в части обеспечения управляемости и надежности функционирования российского сегмента сети Интернет.

— **В состоянии ли, на ваш взгляд, система образования и подготовки кадров обеспечить реализацию программы необходимым количеством компетентных специалистов?**

— Могу вас заверить, что план предусматривает целый ряд мероприятий, направленных на решение проблемы образования и подготовки кадров в области информационной безопасности, в том числе и материально-техническое оснащение образовательных учреждений. Я уверен, что эти цели будут достигнуты.

— **Как влияет ваша работа над программой на деятельность Сбербанка? Планируете ли вы перестроить деятельность компании в соответствии с программой?**

— Несомненно, Сбербанк будет руководствоваться в своей деятельности направлением, заданным программой «Цифровая экономика РФ».

— **Работа над программой — это революция или эволюция в сфере ИБ?**

— Отчасти инновация в сфере информационной безопасности.

— **Можно ли считать Сбербанк первым образцом цифровой экономики?**

— Сбербанк — лидер банковской сферы. Это звание возлагает на нас определенные обязательства, в том числе оставаться первыми и в сфере информационной безопасности при реализации программы «Цифровая экономика». Мы и впредь будем укреплять и расширять наши компетенции в этой области.

— **Смогут ли воплотить подходы Сбербанка в сфере ИБ мелкие банки?**

— Однозначно! Принцип масштабирования является неотъемлемой частью нашей стратегии. Кроме того, Сбербанк всегда открыт для плодотворного сотрудничества.



ПЕТР ЕФИМОВ: «РИСКИ – ЭТО ОБЫДЕННОСТЬ»

В ГОСТЯХ У BIS JOURNAL ПРЕЗИДЕНТ
И СООСНОВАТЕЛЬ КОМПАНИИ «ИНФОРМЗАЩИТА»
ПЕТР ЕФИМОВ

— Петр Валентинович, в июле Премьер-министр России утвердил программу «Цифровая экономика Российской Федерации». Какую роль, на ваш взгляд, это событие играет в истории отечественной ИБ?

— В программе предусмотрено много шагов: от гармонизации законодательства и создания инфраструктурных предпосылок к развитию страны в области информационных технологий до планов по становлению России как мирового лидера в области информационной безопасности. Замечательно здесь то, что впервые в таком программном документе информационной безопасности посвящен отдельный раздел. Это значимая веха в развитии национальной информационной безопасности, обусловленная ростом понимания ответственности государства за безопасность общества и личности в новом цифровом мире, неотвратимости возрастания угроз и уязвимостей. Информационная безопасность из обязательной, но второстепенной дисциплины, становится одной из составляющей будущего цифровой экономики. Лёд тронулся!

— Программа «Цифровая экономика» — это революция или эволюция?

— Новая программа — далеко не первый документ такого рода. Можно вспомнить программы ФЦП «Электронная Россия» (2003–2010 гг.), «Информационное общество» (2011–2020 гг.), Доктрину информационной безопасности, а также совсем свежую «Стратегию развития информационного общества в Российской Федерации на 2017–2030 годы». Существуют и более общие концептуальные и программные документы, также затрагивающие проблему перехода российского общества к цифровым технологиям. С этой точки зрения программа «Цифровая экономика» — документ эволюционный.

По сути эта программа — попытка консолидации уже имеющегося задела. Она нацелена на эволюцию правового и технического регулирования, обеспечивающего рост отечественного интеллектуального и технологического потенциала. Впоследствии это приведет к серьезным изменениям для каждого из нас: от регистрации при рождении до электронного сопровождения в течение всей нашей жизни. Примеров много уже сейчас: госуслуги, платежные и банковские документы, документы, удостоверяющие личность и права собственности, медицинские, пенсионные и социальные права. Всего и не перечислишь. Программа способствует последовательному накоплению больших объемов информации в цифровом виде, росту потребности в ее оперативном поиске и использовании. По-

этому, я считаю, что «Цифровая экономика» — это эволюция с революционными результатами.

— Реальны ли, на Ваш взгляд, сроки (реализация до 2025 г.), обозначенные в программе «Цифровая экономика»?

— Я бы оценил их как амбициозные. В первую очередь, потому, что для выполнения программы требуется гармонизация законодательства, которое пока ориентировано на традиционную модель взаимодействия хозяйствующих субъектов.

Вспомните заявление Google, которое в 2004 году прозвучало как вызов. Компания объявила, что к 2020 году она оцифрует все изданные на тот момент в мире книги. Этого не случилось, и помехой стала правовая ситуация в области авторских прав.

Я уверен, что добиться высоких показателей к указанному сроку — задача вполне реальная. При условии, что на «раскачку» уйдет минимум времени, и реализацию программы начать прямо сейчас.

— Какие, на Ваш взгляд, серьезные изменения ждут сферу ИБ в течение этого срока?

— Давать прогнозы на такой долгий срок — дело неблагодарное, но некоторые тренды не вызывают особых сомнений, поскольку безопасность всегда следует за меняющимся миром. В парадигме развития цифровой экономики будут стираться границы между видами безопасности, поскольку методы и средства работы, скажем, экономической и информационной безопасности будут смешиваться, взаимно дополняя друг друга. Использование технологий «облачных вычислений» и растущая пропускная способность каналов связи потребует повышения функциональности и быстродействия средств защиты. Будет происходить переход к сервисной модели обеспечения безопасности. Существенно повысится роль информационного обмена об уязвимостях в тех или иных системах, о событиях безопасности и другой специ-

ВПЕРВЫЕ В ТАКОМ ПРОГРАММНОМ ДОКУМЕНТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСВЯЩЕН ОТДЕЛЬНЫЙ РАЗДЕЛ. ЭТО — ЗНАЧИМАЯ ВЕХА В РАЗВИТИИ НАЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

фической информации. Безопасность должна стать максимально проактивной.

Кроме того, влиять будут и новые методы атак, предсказать появление которых сложно. Скажем, на конференции Black Hat Europe 2017 был продемонстрирован метод Process Doppelganging — бесфайловых атак. За счет умелого обращения с файловой системой NTFS они могут обманывать существующие антивирусные решения. Это вызов, на который придется реагировать. А сколько их еще предстоит — неизвестно.

— Окажут ли все эти изменения влияние на работу «Информзащиты»?

— Изменения в компании уже идут и достаточно активно. С одной стороны, мы стараемся развивать свои компетенции в различных направлениях безопасности, создавая специализированные центры, например, по противодействию мошенничеству (фроду), по защите АСУТП. Постоянно ищем способы совершенствования этих направлений, занимаемся изучением тех возможностей, которые может дать искусственный интеллект в совокупности с машинным обучением, смотрим на существующие и развиваем собственные сервисы в киберразведке (Threat Intelligence). Сегодняшняя жизнь нам не дает возможности быть в роли наблюдателя и просто следовать за ситуацией, мы обязаны быть готовы к решению любого вызова, вне зависимости от его сложности.

— Как Вы считаете, какое место занимает «Информзащита» в цифровой экономике в части ИБ?

— Давайте будем осторожнее с терминами. Поисковые системы трактуют «цифровую экономику» как экономическую деятельность, основанную на цифровых технологиях. Причем речь идет не столько о разработке и продаже, например, программного обеспечения, сколько об электронных товарах и сервисах, а также их доступности в рамках цифрового пространства. Мы же должны обеспечить безопасность

в цифровом пространстве. При этом не стоит путать обеспечение безопасности и предоставление безопасных сервисов.

ИБ в «Цифровой экономике» — это инструмент, который делает цифровую экономику безопасной. «Информзащита» участвует в обеспечении безопасности этой экономики, а не только лишь предоставляет безопасные сервисы. Если рассуждать в рамках этих терминов, то «Информзащита» движется в направлении вывода части своих услуг в цифровое пространство, оставаясь компанией реального сектора экономики, которая производит осязаемые услуги — от создания организационно-распорядительной и проектной документации до защиты бизнеса наших заказчиков.

— По сути Вы — непосредственный участник формирования отрасли информационной безопасности в России. Как, на ваш взгляд, меняется ее ландшафт?

— Изменений множество. Особо хочется отметить полное и окончательное размытие «периметра» информационных систем, аутсорсинг практически любых функций ИБ, включая администрирование средств защиты. Изменения продолжаются постоянно. Например, те же персональные данные. Сегодня это не только адрес и номер паспорта, но и тот массив информации, который можно собрать о каждом человеке по его поисковым запросам, активности в социальных сетях, выбранным новостным лентам и т.п. Что делать и как защищать эти данные — пока еще предстоит разобраться. Но с другой стороны, подходы к защите глобально не меняются, хотя и начинают базироваться на все более совершенных технологиях. Главное, сегодня ни у кого нет сомнений, что ИБ — неразрывная часть современного ИТ-ландшафта. В том числе, важность этого вопроса для государства подтверждается принятой в декабре 2016 года Доктриной информационной безопасности РФ.

— Можете дать прогноз ситуации в Вашей компании и отрасли на ближайшие 5–10 лет?

— Наиболее значимые изменения, на мой взгляд, могут произойти в области правового регулирования. Сейчас вышли в свет требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры (КИИ), строится ГосСОПКА, ужесточаются требования по защите персональных данных (GDPR), усиливается контроль за действиями пользователей в сети Интернет. Сейчас, пожалуй, мы являемся участниками чрезвычайно интересного процесса.

Сегодня нам недостаточно быть просто высококвалифицированными специалистами в об-

ПОДХОДЫ К ЗАЩИТЕ ГЛОБАЛЬНО НЕ МЕНЯЮТСЯ, ХОТЯ И НАЧИНАЮТ БАЗИРОВАТЬСЯ НА ВСЕ БОЛЕЕ СОВЕРШЕННЫХ ТЕХНОЛОГИЯХ. ГЛАВНОЕ, СЕГОДНЯ НИ У КОГО НЕТ СОМНЕНИЙ, ЧТО ИБ — НЕРАЗРЫВНАЯ ЧАСТЬ СОВРЕМЕННОГО ИТ-ЛАНДШАФТА



ласти информационной безопасности. Нам необходимо хорошо разбираться в специфике бизнеса наших клиентов, т.к. безопасность информационных систем и бизнес-процессов неразделимы.

Достичь этого можно только глубоким погружением в бизнес-процессы наших заказчиков с точки зрения их уязвимости. Для этого мы сегодня строим нашу компанию как некоторый набор профильных и отраслевых центров, специализирующихся в тех или иных областях.

— Вы стоите у руля компании 22 года. Расскажите, пожалуйста, о ключевых моментах ее развития? Что в тот или иной период становилось драйвером роста? Какие моменты остро запомнились?

— Мы начинали бизнес в качестве вендора — разработчика системы Secret Net. На первом этапе нам повезло с тем, что у нас было сразу несколько интересных и крупных клиентов. Тогда еще не было современных конкурсных процедур, и борьба за право реализации проекта была иной. Во главе угла стояло не предложение меньшей цены, а качество предлагаемого решения. И главным было убедить — оно лучшее. Через живое общение мы неоднократно

доказывали, что наши средства лучше всего подходят для защиты той или иной конкретной системы. Большое число крупных компаний страны стало нам доверять.

Спустя какое-то время на рынке появилась потребность в системной интеграции — когда заказчики поняли, что помимо покупки средств защиты их еще нужно правильно установить и настроить. Так мы превратились в системного интегратора, и стали наращивать свои компетенции, оказывать консалтинговые услуги. А затем поняли, что быть одновременно разработчиками и консультантами с элементами интеграции — тяжело. Направления нужно было разделить. В то время было принято решение выделить разработку в отдельную компанию. Так появился «Код Безопасности».

После этого была череда и других перемен. Со временем мы также поняли, что оказание услуг по внедрению, технической поддержке и т.п. может и должно быть самостоятельным бизнесом. Подразделение, которое раньше внутри «Информзащиты» занималось сервисом, выделилось в отдельную компанию — «Информзащита-Сервис». Следующим важным этапом стало осознание перспективности сервисной



СИТУАЦИЯ СЕЙЧАС ТАКОВА, ЧТО ОСТРО ВОСТРЕБОВАНЫ ИМЕННО ПРАКТИЧЕСКИЕ КОМПЕТЕНЦИИ, Т.Е. ЗНАНИЯ И УМЕНИЕ ДЕЛАТЬ ЧТО-ТО КОНКРЕТНОЕ, А НЕ РАЗВОДИТЬ ТЕОРИЮ

модели и создание своего Security Operation Center. А это подразумевает, что заказчики стали давать нам на аутсорсинг процесс управления своей информационной безопасностью.

— Что Вы лично привнесли в развитие «Информзащиты»? Чем искренне гордитесь?

— Еще в юности мне хотелось создать и развивать свою компанию. У меня это получилось. И я горжусь, что, невзирая на многочисленные кризисы, когда многие компании уходили с рынка или сокращали штат, «Информзащита» всегда преодолевала критические ситуации и доросла до компании с историей почти в четверть века. Пожалуй, горжусь тем, что принимаю на себя ответственность за принятие сложных решений. Был ряд судьбоносных

для компании ситуаций, из которых удавалось выходить достойно. И не просто преодолевать трудности, но при этом непрерывно развиваться, двигаться по восходящей. Ну и, наверное, стоит отметить, что с моей подачи в компании привита такая система ценностей, при которой дело — прежде всего. Многие компании на словах заявляют о своей клиенто-ориентированности. Мы же стараемся в первую очередь решить проблему заказчика. Очень сложно предусмотреть всё, и так нередко случается, что мы делаем в рамках проектов больше, чем было прописано в договоре.

— Можно ли утверждать, что Вы обладаете чутьём на возможные риски и можете предугадывать исход тех или иных событий на рынке ИБ, в ИТ-отрасли и экономике страны в целом?

— Хотелось бы верить, что да. В «экономике страны» — громко сказано, но если говорить о рисках для нашей компании, то их я стараюсь избегать. Перед принятием тех или иных сложных решений приходится руководствоваться известной русской пословицей «... — один раз отрежь». При планировании мы прорабатываем возможные сценарии развития ситуации и в результате можем гибко подстра-

иваться под любые изменения. В памяти достаточно случаев, когда приходилось отказываться от заманчивых предложений и после об этом не пожалеть.

— Существует мнение, что на рынке ИБ не хватает кадров. Согласны ли Вы с этим, и является ли это для Вас проблемой?

— Да, это действительно проблема, квалифицированных кадров на рынке не хватает. Но это больше связано с тем, что информационные технологии развиваются очень быстро, а задачи по информационной безопасности сейчас стоят очень остро. Заказчикам требуется квалифицированное построение и эксплуатация систем защиты. Если вузам сегодня дать команду увеличить набор, то мы получим существенную прибавку специалистов только через 5–6 лет.

Тем не менее в количественном выражении число специалистов сферы ИБ возросло, чего, к сожалению, нельзя сказать об их качестве. Могу заявить определенно: настоящим специалистом становится тот, кто постоянно ищет возможности самосовершенствования в профессии, учится, понимает, чего и в какой области он хочет добиться. Ситуация сейчас такова, что остро востребованы именно практические компетенции, т.е. знания и умение делать что-то конкретное, а не разводить теорию.

— В состоянии ли, на Ваш взгляд, сложившаяся система образования и подготовки кадров обеспечить потребности отрасли в специалистах?

— Ничего нет невозможного при правильном построении учебного процесса и грамотном подборе преподавателей. Задача учебных заведений правильно и гибко подходить к учебным программам. В современных реалиях необходимо больше обсуждения практических и актуальных проблем и меньше лекций, как мы их называем, об истории предмета. Мир меняется быстро, и образование должно поспевать за этими изменениями. Хорошо зарекомендовала себя практика, когда лекторами выступают «практикующие» специалисты из профильных компаний и структур.

— Как Ваша компания вкладывается в обучение и развитие молодых неопытных специалистов?

Мы вкладываемся в обучение не только новичков: у нас на каждый год принимается план обучения для всех специалистов разных категорий. Выделяются необходимые средства, которые становятся защищенной строкой в бюджете компании. Мы отправляем сотрудников на разные курсы, развиваем систему наставничества. Хотелось бы еще отметить, что из-за вы-

сокой экспертизы наших работников у других компаний есть соблазн переманить их, и нам очень неприятно, когда наших специалистов заполучают не совсем честным путем.

— Какими инструментами Вы стараетесь удерживать сильных экспертов от ухода к конкурентам?

Прежде всего, формируем многоступенчатую мотивацию. Просто платить хорошую зарплату уже недостаточно. У нынешних молодых специалистов есть потребность в самореализации, получении признания, самоутверждения. Таким людям нужно ставить интересные, масштабные задачи. Стараемся это делать регулярно. Также всеми способами поддерживаем здоровый климат в коллективе и заботимся о сотрудниках. Например, мы были одной из первых в России ИТ-компаний, которая полностью покрывает медицинскую страховку персонала.

— Напоследок, хочется задать Вам несколько блиц-вопросов, чтобы лучше узнать вас. Считаете ли Вы себя добрым человеком?

— О моей доброте лучше спросить у других людей. Точно считаю себя человеком порядочным.

— Какие личные качества в людях для Вас неприемлемы?

— Не терплю предательства и подлость. Даже глупость могу простить, а предательство — никогда. Особенно от тех, от кого этого точно не ожидал.

— У Вас когда-нибудь были кумиры?

— Первое, что в связи с этим вспоминается, фраза «не создай себе кумира». Нет, у меня не было кумиров. Не умею настолько сильно очаровываться. Мы видим лишь внешнюю сторону известных людей, но не знаем их лично. А если бы узнали, то неизвестно, хотели бы на них быть похожими.

Многие любили Стива Джобса, его презентации. Им нравился его стиль, и они захотели его повторить. Я считаю, что лучше быть самим собой, а если хочешь выделиться, то придумай что-то свое.

— Есть ли современные технологии, которые Вам не нравятся?

— Вы удивитесь, но я не люблю Интернет. Для меня есть «хороший» Интернет, который мне помогает в работе, учебе, поиске нужной информации и тот, который лишает нас живого общения. Из-за второго у многих отпала необходимость личных встреч с друзьями. Сегодня не выходя из дома можно связаться с кем угодно. Но без живого общения наша речь становится все более непонятной и примитивной. Я не готов обменивать свои эмоции на пиктограммки.

Беседовала
Алёна Подкорытова

Фотограф
Михаил Муравьев

УМНЫЙ БАНК В БОЛЬШОМ ГОРОДЕ

ОБЗОР ВЫЗОВОВ ИБ ЦИФРОВОЙ ЭПОХИ



Тимур АИТОВ

заместитель председателя
Подкомитета по платеж-
ным технологиям и инфор-
мационной безопасности
ТПП РФ, заместитель
генерального директора
ГК «Программный
Продукт»

Новые идеи и концепции заполнили общественное сознание — умный город, искусственный интеллект, Big-Data. Огромные потоки данных аккумулируют знания обо всем — о рынках, клиентах, о конкурентах. Коммерческие банки в принимаемых решениях уже не просто банки, это «банки, управляемые данными». Какие актуальные вызовы придется преодолевать банковским службам ИБ в цифровую эпоху?

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Большие данные BigData в банк поступают из многочисленных источников — их поставляют телеком-операторы, объекты финансовой инфраструктуры, социальные сети, коммуникаторы, сенсоры и др. Технологические проблемы работы с BigData связаны с адекватной интеграцией поступающих потоков и построением качественных прогнозных моделей. С точки зрения задач информационной безопасности (ИБ) процессы обработки и хранения BigData в банках должны быть защищены, а системы с персональными данными (ПД) должны сохранять необходимую конфиденциальность

Один из ключевых и актуальных вызовов в ближайшее время в сфере ПД — новый свод законов по защите ПД — GDPR, General Data Protection Regulation, вступающий в силу в странах ЕЭЗ в мае 2018 года. Суммы штрафов за нарушения норм GDPR доходят до 20 млн евро или 4% от оборота компании-нарушителя, причем в качестве суммы штрафа выбирается боль-

шее значение из приведенных двух. Многим банкам придется соблюдать новый набор правил — если в числе клиентов у них найдется хотя бы один гражданин ЕЭЗ. Нормы жесткие — запрещен мониторинг перемещений и предпочтений граждан ЕЭЗ без их согласия. Гражданин ЕЭЗ имеет права на удаление персональной информации о себе и на «перенесение» своих ПД другому поставщику услуг (ст. 20 GDPR). Сама возможность переносить ПД мало что дает для их защиты (она скорее служит функциональным требованием для социальных сетей и облачных провайдеров). Но обеспечивать эту возможность — дело тонкое и придумать к этому легко. Банкам придется разработать «аккуратные» процедуры для реагирования на подобные запросы или попросту отказаться от обслуживания европейцев.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Методы искусственного интеллекта (ИИ) и MachineLearning (что на данной стадии по сути одно и то же) находят все более широкое применение в умных банках, включая процессы ИБ. Развивается новое направление ИИ по борьбе с киберпреступниками. Не везде активность в этом направлении радикально помогает, но освобождает от рутинных операций на 100%. Абсолютно все новые системы SIEM уже используют методы ИИ. Системы передают предупреждения-alarm, вычисляют типовые (средние) состояния работы банка и систем, ищут отклонения от средних значений (аномалии) — все эти операции даже теоретически выполнить человеку в real time невозможно. В перечень перспективных систем, работающих с использованием ИИ кроме SIEM, включены системы обнаружения (IDS) и системы предотвращения вторжений (IPS), системы управления идентификацией и доступом (IAM), вся аналитика BI, системы продвинутой антивирусной защиты, весь комплаенс в банке. Эффект от ИИ можно сравнить с ковшом экскаватора, который удесятерит силы землекопа и позволяет перелопатить огромные объемы информации там, где

**СУММЫ ШТРАФОВ ЗА НАРУШЕНИЯ
НОРМ GDPR ДОХОДЯТ ДО
20 МЛН ЕВРО ИЛИ 4% ОТ ОБОРОТА
КОМПАНИИ-НАРУШИТЕЛЯ,
ПРИЧЕМ В КАЧЕСТВЕ СУММЫ
ШТРАФА ВЫБИРАЕТСЯ БОЛЬШЕЕ
ЗНАЧЕНИЕ ИЗ ПРИВЕДЕННЫХ ДВУХ**

ОБСУЖДЕНИЕ В ТПП РФ

«Вопросы регулирования эмиссии и обращения криптовалют в цифровой экономике» – так была сформулирована тема заседания, прошедшего недавно в ТПП РФ. Ключевые моменты комментирует модератор этого заседания, заместитель председателя Подкомитета по платежным технологиям и информационной безопасности Тимур Аитов.

— Повестка отражает объективные тренды платежного ландшафта, и в первую очередь обусловлена, конечно, появлением поручений Президента. Напомню, 10 октября 2017 года глава государства поручил Правительству РФ совместно с Банком России обеспечить внесение в законодательство РФ изменений, касающихся проработки вопросов налогообложения майнинга, статуса цифровых технологий, применяемых в финансовой сфере, их понятий и т.д.

Вопросы, связанные с цифровыми технологиями и инновациями в платежах, в ТПП РФ обсуждают не впервые. Еще летом представители Ассоциации «Финансовые инновации» вынесли на общественный суд обстоятельную «Концепцию совершенствования регулирования в национальной платежной системе», что потребовало глубокого погружения в тему. Обсуждение вопросов обращения криптовалют стало ее развитием.

Задачу совершенствования законодательства эксперты в целом поддержали, но призвали тщательно и аккуратно подходить ко всем вопросам внедрения новых платежных инструментов и технологий. Что имеется в виду?

Прежде всего, это высокие риски, сопровождающие появление всего нового, и защита прав инвесторов.

Если говорить о криптоактивах и ICO (Initial coin offering, с англ. – «первичное предложение монет, первичное размещение монет»), многие, если не большинство из них, оказались провальными. Примеров много. Инвесторы не дождались операционной системы от Razormind, из сервиса знакомств Matchpool все средства вы-

вели сами организаторы ICO. По сведениям Group-IB, ICO-проекты 2017 года в Ethereum на сумму в \$225 млн украдены хакерами. И никого не удивляет, что в Китае и Южной Корее ICO запрещены, а в США на них наложены серьезные ограничения.

С другой стороны, существует масса плюсов, связанных с блокчейном – технологической основой криптовалют. Эта технология позволяет решать нужные и важные практические задачи. Это и умные контракты, и электронные закладные, и цифровые банковские гарантии, и аккредитивы... Перед законодателем сегодня стоит непростая задача. С одной стороны, не торопиться и просчитать все риски, связанные с переходом на новые технологии. С другой – не опоздать и не «проспать» ту самую технологию, которая способна радикально изменить экономику и, возможно, поднять уровень жизни россиян в XXI веке.

Участники заседания посчитали первоочередной задачей построение понятийного аппарата, связанного с криптоактивами. Что такое цифровая валюта? Каковы правила ее обращения? Каковы правила деятельности субъектов, выпускающих цифровую валюту? и т.д. Все эти понятия требуют определений. В отношении негосударственных цифровых валют (НЦВ) также предложено определить тех, кто вправе осуществлять майнинг, установить необходимое лицензирование бирж и сервисов, осуществляющих обмен НЦВ на российские рубли, сформулировать требования к субъектам – участникам торгов.

Также участники заседания рекомендовали в дальнейшем осуществлять «мягкое» регулирование ICO в РФ. Цель – возможное привлечение инвестиций, в том числе зарубежных, в российские компании в условиях санкций.

Станет ли блокчейн новой национальной идеей России, способной обеспечить экономический рывок? Однозначного ответа на этот вопрос участники заседания не дали.



ethereum

\$225 млн

сумма ICO-проектов
2017 года в Ethereum,
украденных хакерами

есть BigData. Но человек при сопровождении этих процессов пока всегда нужен.

Особых барьеров для инсталляции новых систем ИИ нет. Однако, проблемы возникают с распределением зон ответственности. В какой мере можно делегировать системам ИИ принятие важнейших решений? Кто именно будет нести ответственность за принимаемые системой решения? Четких ответов нет. Проблема

снимается, если система ИИ всегда работает «в связке» с оператором-человеком, который принимает (акцептует) важнейшие решения. Присутствие оператора важно — он и берет ответственность за все последствия.

В то же время нельзя ограничивать участие человека только сопровождением инфраструктуры ИИ и принятием решений. На данном этапе развития этих технологий человек факти-

ГРЯДЁТ НОВАЯ ЭРА — ЭРА ФИНТЕХА — СОЕДИНЕНИЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ И ЦИФРОВОГО БАНКИНГА

чески закладывает образ мышления в машину, не позволяя тем самым интеллекту быть самостоятельно мыслящим и по-настоящему самообучаемым.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Успех хищений на базе методов социальной инженерии (СИ) сегодня окрылил злоумышленников — эти методы сегодня активно совершенствуются, а объемы хищений растут. Сегодня до трех четвертей всех хищений со счетов клиентов-физиков осуществляются именно методами СИ. Личность клиента все в большей мере определяет ситуацию с ИБ в банке — личность в центре внимания злоумышленников, всех ключевых процессов ИБ.

Коммуникации с клиентами становятся все более персонифицированными, а технологии BigData придают им большую гибкость по сравнению с классическими технологиями, позволяя обеспечить контроль и не нарушать нормы законодательства, например, при контактах в конфликтных ситуациях (с должниками).

На первом плане — качество кадрового состава офицеров ИБ, здесь важна не только текущая квалификация, но и способность к постоянному переобучению. ИИ помогает повысить эффективность кадровой службы: все эксперты, как правило, высокооплачиваемая категория, их часто не хватает. А возможности офицера ИБ многократно усиливаются, если под его началом функционируют системы ИИ — труд эксперта становится более производительным, квалифицированных сотрудников нужно уже меньше.

Тем не менее, проблема высококвалифицированных кадров — проблема вечная. Эксперты с аналитических задач, часть из которых будет решаться автоматизировано, перераспределятся на разработку и программирование логики искусственного интеллекта. И тут специалисты потребуются в большом количестве.

ДИСТАНЦИОННОЕ ОБСЛУЖИВАНИЕ И БИОИДЕНТИФИКАЦИЯ

Эти методы активно развиваются и запущены пилотные проекты. Однако пока неясны реальные уровни угроз и рисков, сопровождающих новые технологии. Неясно, кто ответит за возможную компрометацию биоидентификацион-

ных данных граждан на платформах с государственным участием типа проекта ЕСИА? Кто будет покрывать возможные убытки?

Банковские технологии все больше усложняются, идет активное создание различного рода экосистем, увеличивается специализация провайдеров и число их растет. Грядёт новая эра — эра финтеха — соединение инновационных технологий и цифрового банкинга. Для обслуживания клиентов все шире используются облачные технологии. Как распределить ответственность за сбой в цепочке провайдеров, создающих «облачную» услугу? Вычисление «крайнего» и ответственного за сбой становится для банка важной и самостоятельной задачей, даже если сбой неумышленный. Однако сбои случаются и подставные — в том числе, для выдавливания конкурентов, и тут концы найти сложнее. На рынке уже появилась новая услуга — технический арбитраж от компании, позволяющий разобраться с зонами ответственности провайдеров облачных сервисов и технологий.

МЕЖДУНАРОДНЫЕ АСПЕКТЫ ИБ

Информационная безопасность в текущей геополитической обстановке все в большей мере приобретает международный характер. Атаки по ключевым финансовым объектам могут быть организованы на уровне недружественных стран. ИИ будет использоваться для просчета вариантов, прогнозной аналитики, других задач, сопровождающих обработку BigData. Такие системы уже работают. А вот кто кого победит в кибервойне — это вопрос качества разработки. Здесь многое будет зависеть и от быстрой реакции машин и от самих алгоритмов. Наши отечественные разработчики всегда отличались в лучшую сторону — у нас много решений, позволяющих на машинах меньшей производительности добиться нужного результата.

* * *

Нельзя забывать и традиционные аспекты, связанные с зависимостью от иностранных технологий и необходимостью внимания к рискам наличия недеklarированных возможностей технических средств. Санкции в отношении РФ стали реалиями бизнеса и с ними нам жить, видимо, еще долго. А банки, особенно с иностранными корнями, могут оказаться даже под противоречивым набором требований по комплаенс в отношении некоторых своих клиентов и ключевым вызовом — потерять российский рынок вообще.



Кибербезопасность крупных организаций и предприятий

Комплексная платформа для защиты
крупных IT-инфраструктур и промышленных сред

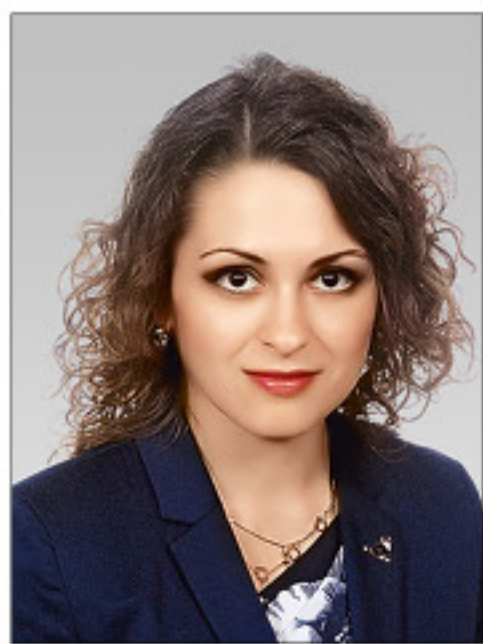
- Контроль и защита рабочих мест
- Защита виртуальных сред
- Защита центров обработки данных
- Экспертные сервисы в области кибербезопасности
- Защита от целевых и DDoS-атак
- Кибербезопасность критических инфраструктур
- Защита мобильного и онлайн-банкинга

kaspersky.ru/enterprise

© АО «Лаборатория Касперского», 2017. Зарегистрированные товарные знаки
и знаки обслуживания являются собственностью их правообладателей.

К ЕДИНОМУ ИДЕНТИФИКАТОРУ

«ФЕДЕРАЛЬНЫЙ РЕСУРС О НАСЕЛЕНИИ» —
МАЛЕНЬКИЙ ШАГ ДЛЯ ЧЕЛОВЕКА, БОЛЬШОЙ —
ДЛЯ СУБЪЕКТА ЦИФРОВОЙ ЭКОНОМИКИ



**Екатерина
КАЛАШНИКОВА**
заместитель руководителя
службы защиты
автоматизированных
банковских систем
Управления
по обеспечению
информационной
безопасности
Банка ВТБ (ПАО)

ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ — ОБЩЕСТВЕННЫЙ ЗАПРОС

Процедуры проверки идентичности уже давно стали неотъемлемой частью нашей повседневной жизни. Субъект доказывает, что он — это он, вводя пароль от электронной почты, PIN-код от банковской карты, предъявляя паспорт и билет на самолет, водительские права.

При этом в России субъекту (даже физическому лицу) присвоено одновременно много идентификаторов, таких как номер свидетельства о рождении, номер паспорта (внутреннего и заграничного), ИНН, номер полиса ОМС, СНИЛС и т.д. Это необходимо для того, чтобы сделать его участником и стороной экономических и социальных отношений, предоставлять ему товары или услуги, производя при этом учет осуществленных действий и изменений, связанных с данным субъектом, в соответствующих системах. Отдельного рассмотрения требует процесс аутентификации субъекта, но здесь важно отметить, что систему аутентификации без системы идентификации создать невозможно.

Обязательным требованием к цифровому идентификатору является его уникальность на множестве всех когда-либо идентифицируемых субъектов, а также неизменность на протяжении жизни человека. Кроме того, идентификатор должен быть легко запоминаем и пригоден для осуществления операций с применением различных каналов ввода данных и для автоматической обработки. Оптимальным решением с учетом этих условий является использование цифровой последовательности с контрольными разрядами.

На данный момент в нашей стране практически каждой категории идентичностей субъекта соответствует отдельно созданная информационная инфраструктура, что делает процесс их интеграции и взаимодействия (не говоря уже

о совокупной стоимости владения) очень затратным, как по времени, так и с финансовой точки зрения.

А ЧТО ЖЕ ГОСУДАРСТВО?

Тот факт, что в России инициатива реформ и модернизаций в экономической и общественной сфере традиционно принадлежит государству, как самому крупному «заказчику», обладающему достаточным ресурсом, чтобы как реализовать, так и продвинуть в дальнейшем то или иное нововведение, обуславливает начало развития цифровой экономики с трансформации именно в государственном секторе.

Мы уже прошли ту стадию, когда под «цифровизацией» понималось только электронное Правительство или автоматизация деятельности чиновников. Перед нами стоят глобальные вызовы, на которые вынуждено отвечать сейчас мировое экономическое сообщество в целом и экономика России в частности. В текущих обстоятельствах сложно разом преодолеть все сложившиеся в классической экономике препятствия, мешающие бизнесу в России развиваться теми темпами, которые могли бы обеспечить нам активный устойчивый рост. Но экономика цифровая — это та область, где наш потенциал роста практически неограничен, рынок еще не сложился и не поделен, и есть шанс, включившись в гонку на ранних этапах, грамотно используя и развивая все доступные инструменты, быстро оказаться в лидерах.

Особенности цифровой экономики, такие как глобализация, необходимость проведения сделок как локального, так и трансграничного характера, дистанционно, в режиме реального времени и непрерывно, между любыми правоспособными субъектами, не известными друг другу, заставляют отказаться от традиционных «аналоговых» систем установления идентично-

Сведения о физическом лице	настоящие и предыдущие (при наличии) фамилия, имя и отчество	пол	
	даты рождения и смерти	дата выезда на постоянное место жительства в другую страну (для эмигрантов)	
	места рождения и смерти	дата прибытия в Российскую Федерацию на постоянное место жительства (для иммигрантов)	
Идентификаторы сведений о физическом лице	реквизиты свидетельства о рождении (реквизиты записи акта гражданского состояния о рождении)	реквизиты свидетельства о смерти (реквизиты записи акта гражданского состояния о смерти)	виды, номера и иные сведения о документах, удостоверяющих личность физических лиц
	виды, номера и иные сведения о документах, удостоверяющих право физических лиц осуществлять определенную деятельность (в случаях, установленных законодательством Российской Федерации)	идентификаторы сведений о постановке на регистрационный учет по месту жительства или месту пребывания	идентификаторы сведений о регистрации в системах обязательного пенсионного, медицинского, социального страхования
	идентификаторы сведений о постановке на регистрационный учет по месту жительства или месту пребывания	идентификатор сведений о постановке на учет в налоговых органах	идентификаторы сведений о постановке на учет в качестве нуждающегося в социальной защите
		идентификаторы сведений о постановке на учет в органах занятости	

сти (или идентификации) в виде различных физических, в т.ч. бумажных, носителей.

Уже есть четкое осознание, что переход к цифровым отношениям приносит наибольшие плоды там, где на этот процесс смотрят максимально широко, прорабатывают решения глубоко и системно, используя ресурсы государства и понимая, что изначально электронное государство в цифровой экономике — это оптимальные отношения с электронными образами людей, организаций и любых других типов правоспособных субъектов экономических отношений.

ЗАКОНОДАТЕЛЬНАЯ ПОДДЕРЖКА

11 июля 2017 г. опубликовано Распоряжение Правительства России от 4 июля 2017 г. № 1418-р «Об утверждении концепции и плана мероприятий («дорожной карты») по формированию и ведению единого федерального информационного ресурса, содержащего сведения о населении РФ».

Напомним, что данный ресурс создается в соответствии с указом президента России от 15 января 2016 г. № 13, которым было поручено создать единый реестр населения РФ и объединить функции администрирования страховых

сборов, в том числе сведения о регистрации актов гражданского состояния и по администрированию платежей в пенсионный фонд, фонд социального страхования и фонд обязательного медицинского страхования.

ФРН — ВАЖНЫЙ ШАГ К БОЛЬШОЙ ЦЕЛИ

В соответствии с представленной концепцией, в ФРН будут храниться данные только о физических лицах: гражданах России (в т.ч. эмигрантах) и иммигрантах. Указанная информация будет включать в себя как непосредственно хранимые в ФРН сведения о физическом лице (пол, фамилия, имя, отчество, даты и места рождения и смерти) и идентификаторы сведений (реквизиты документов) о нем, хранящихся в других базовых государственных информационных ресурсах. Для иммигрантов и эмигрантов будут также фиксироваться даты прибытия в Россию на постоянное место жительства и выезда на постоянное место жительства в другую страну (рис. 1).

Во избежание возможности нанесения ущерба личности в ФРН не предусмотрено включение информации о расовом или этническом

Рисунок 1. Состав Федерального ресурса о населении. Материал взят из презентации Министерства финансов РФ (04.06.2017 г., Ханты-Мансийск)



Рисунок 2.
Информационное взаимодействие. Материал взят из презентации Министерства финансов РФ (04.06.2017 г., Ханты-Мансийск)

происхождении, политических, религиозных убеждениях, принадлежности к профсоюзным объединениям и обществам, состоянии здоровья.

Доступ к сведениям из ФРН смогут получить совершеннолетние физические лица (в части сведений о себе и лицах, находящихся на их иждивении) через единый портал государственных и муниципальных услуг (ЕПГУ). Органы власти и местного самоуправления, организации, осуществляющие предоставление государственных и муниципальных услуг, включая многофункциональные центры оказания услуг (в объеме, необходимом для осуществления указанной деятельности) смогут получить доступ через специализированные государственные и муниципальные информационные системы на основании регламента обмена информацией, или по запросу в установленных законодательством случаях.

Также предполагается ведение журналов обмена информацией при взаимодействии

ФРН с иными информационными системами, в отдельных случаях будут фиксироваться факт и цели направления запросов.

Согласно утвержденной концепции, ФРН будет создаваться только на основании сведений государственных и муниципальных информационных систем, уже существующих или вновь создаваемых в будущем. Непосредственное внесение в него сведений о населении, ранее не учтенных в других информационных системах, не предусматривается. При этом данные из иных информационных систем должны поступать в ФРН в автоматизированном режиме через единую систему межведомственного электронного взаимодействия, а каждая такая специализированная государственная и муниципальная информационная система-источник должна функционировать децентрализованно по отношению к ФРН и обеспечивать хранение первичных персональных данных о населении (рис. 2).

Как вышеупомянутый указ, так и Распоряжение № 1418-р продолжают цепочку шагов,

последовательно вот уже почти 20 лет принимаемых государством для цифровизации экономики, упрощения и повышения прозрачности и эффективности системы принятия решений в сфере государственного и муниципального управления, социального обеспечения, планирования и предоставления социальных льгот и государственных услуг населению (фактически с 1996 г. гражданам России уже присваивается уникальный идентификатор — страховой номер индивидуального лицевого счета (СНИЛС), представляющий собой 11 последовательно записанных цифр, где последние две являются контрольной суммой, вычисляемой по особому алгоритму).

Утвержденная Распоряжением № 1418-р концепция предполагает, что сведения о каждом физическом лице в федеральном ресурсе о населении будут формировать запись ФРН, которой будет присвоен уникальный номер, структура которого будет содержать в закодированном виде информацию об отдельных сведениях, включенных в запись федерального ресурса о населении, например день, месяц и год рождения физического лица, номер записи в ФРН и иные сведения (по заявлениям некоторых

ФРН БУДЕТ СОЗДАВАТЬСЯ ТОЛЬКО НА ОСНОВАНИИ СВЕДЕНИЙ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ, УЖЕ СУЩЕСТВУЮЩИХ ИЛИ ВНОВЬ СОЗДАВАЕМЫХ В БУДУЩЕМ

СМИ, это будет неизменяемый 12-разрядный код, а не СНИЛС, как многие предполагали до недавнего времени).

В соответствии с представленной «дорожной картой», проект должен быть реализован к 2025 году.

ФРН в том виде, в котором он представлен, не решит задачу идентификации всех субъектов цифровой экономики России, но он и не должен. ФРН решает только определенное подмножество задач для узкого круга заказчиков. Неоправданное расширение множеств решаемых задач и заказчиков, а также внесение в эти множества элемента разнородности скорее по-

BIS-КОММЕНТАРИЙ

В связи с фундаментальными изменениями экономического характера, прежде всего, эталонной договоренностью в области цифровой идентификации является правовая база, необходимая для функционирования цифровой системы. Принципы превентивности, открытости и диалога между различными структурами могут стать залогом создания и развития перспективной, безопасной и комфортной экосистемы для населения.

В настоящее время уже существует ЕСИА, которая позволяет решить ряд вопросов с идентификацией, и уже успешно работает, позволяя получать многие государственные услуги посредством сети Интернет. Также ведется работа по направлению удаленной идентификации в рамках определения требований и изменения необходимых законодательных актов, в частности 115-ФЗ.

Сейчас Единый «Цифровой идентификатор» на каждого из нас создается государством в рамках проекта «Реестр населения» — распоряжение Правительства № 1418р от 04.07.2017. Планируется, что к концу 2025 года всё население будет заведено в общий Реестр, каждый со

своим ID. Международные модели демонстрируют три варианта цифровой идентификации: на уровне отдельных финансовых и нефинансовых компаний, национальные системы на уровне государства и консолидированные системы как результат взаимодействия частных организаций и государственных органов. Уникальная система, реализованная в Индии, позволила миллиардному населению получить идентификационный документ и получить доступ к банковским, страховым, социальным услугам. Основными драйверами внедрения Aadhaar были высокий уровень поддельных идентификаторов, теневой экономики, отсутствие доступа к базовым социальным услугам для большинства населения.

Российские условия предполагают иную модель и цель цифровой идентификации, с сохранением уже имеющихся идентификаторов и формирования возможности прохождения удаленной идентификации для упрощения гражданам получения финансовых и иных услуг, а также открытие новых возможностей для бизнеса и предоставления более качественных и удобных продуктов.



Иван БАСОВ
главный аналитик
Ассоциации ФинТех

родит проблемы и затормозит, нежели ускорит процесс, усложнит интеграцию. Поэтому необходим разумный баланс между универсальностью и специализацией.

Ограничения, установленные для ФРН в подклассах субъектов (в ФРН будут учитываться только физические лица: резиденты РФ — граждане России и зарегистрированные мигранты, а также нерезиденты, но только эмигранты), а также отсутствие всей необходимой для совершения сделок информации, не позволят проекту стать всеобъемлющим, но сделают его более доступным, прозрачным и управляемым, что на первом этапе формирования института цифровой идентификации в стране вполне разумно.

Впоследствии ФРН сможет использоваться как доверенный источник данных более глобального образования — федерального реестра субъектов цифровой экономики, если таковой будет создан.

ЧТО С БЕЗОПАСНОСТЬЮ?

Если утвержденная распоряжением Правительства РФ № 1418-р «дорожная карта» будет реализована и создан ФРН, то, по сути, статус гражданина, как лица, имеющего права и возможности осуществлять юридически значимые действия и получать государственные и социальные услуги, напрямую окажется связан со

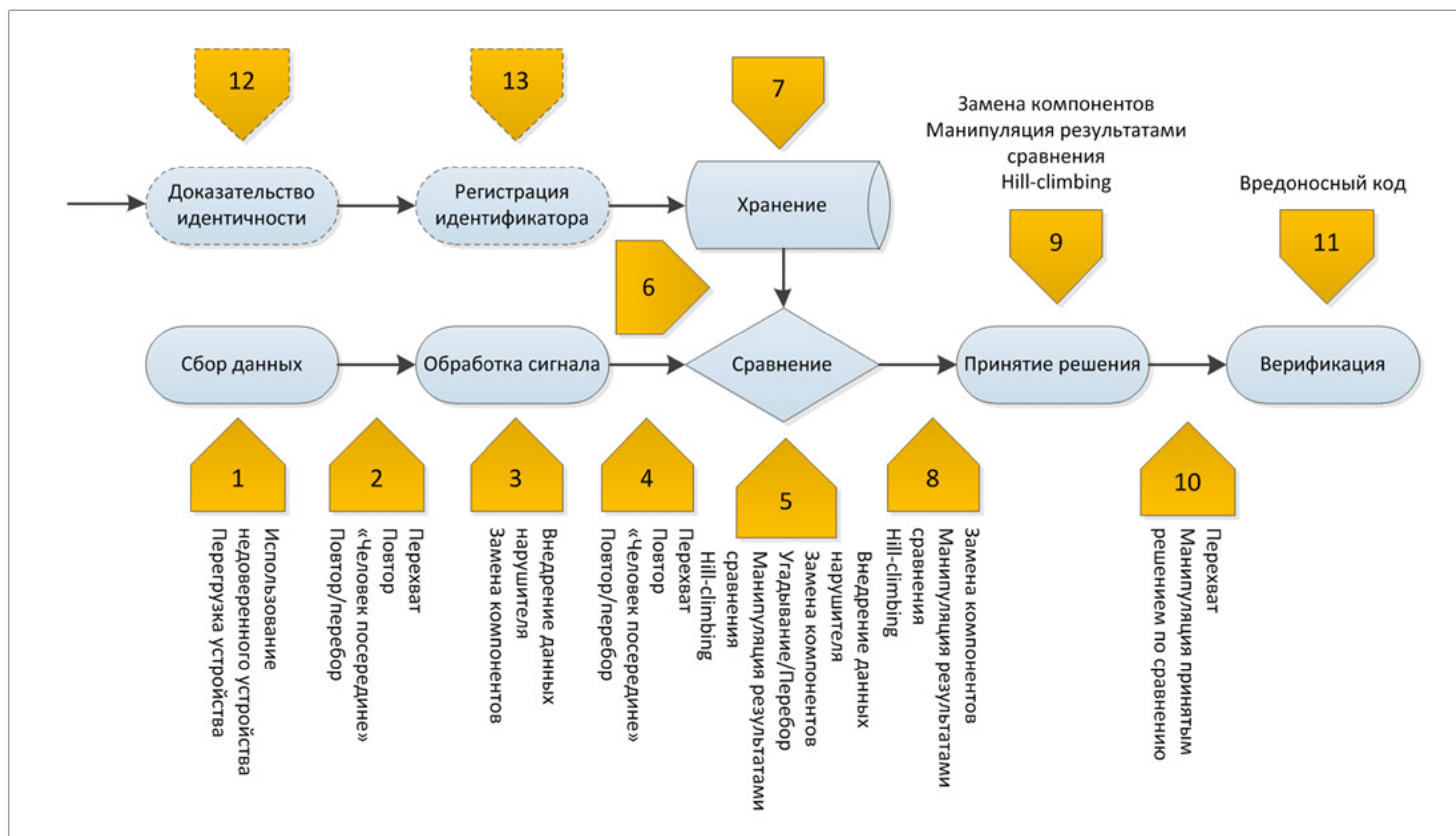
статусом зарегистрированного лица в государственной информационной системе. А это поле для мошенничества и кибератак уже совершенно иного масштаба, нежели все тот же СНИЛС, с использованием которого самое большее, что можно было сделать злоумышленнику, так это перевести пенсионные накопления владельца СНИЛС в негосударственный пенсионный фонд без его ведома.

Атаки на системы идентификации и аутентификации можно разделить на следующие группы:

- ♦ пассивное наблюдение — самый простой в реализации, и сложный для обнаружения со стороны системы безопасности, однако при использовании криптографических методов защиты — неэффективный способ атаки. Может применяться совместно с другими методами для получения максимально возможного количества информации, как об участниках, так и о конкретном протоколе идентификации/аутентификации;

- ♦ воздействие на передаваемую информацию. Злоумышленник перехватывает информацию, видоизменяет ее и отправляет получателю. В итоге получатель уверен, что он аутентифицировался с законным участником протокола, а на самом деле — со злоумышленником. Также возможна реализация данной атаки, пред-

Рисунок 3. По материалам доклада А. Лукацкого «Модель угроз биометрическим системам» на конференции AntiFraud Russia — 2016



полагающая попытки генерации идентификационных/аутентификационных данных для успешного прохождения проверки на основании статистики анализа перехваченных запросов на доступ легальных пользователей и результатов проверки их данных;

- ♦ изменение структуры протокола идентификации/аутентификации. Злоумышленник видоизменяет структуру протоколов, после чего законные участники в процессе аутентификации не могут закончить протокол;

- ♦ изменение механизмов принятия решений. Реализуется посредством модификации механизмов принятия решений. Данный метод наиболее эффективен, если атака нацелена на конкретного участника системы (рис. 3).

В качестве мер противодействия указанным атакам могут использоваться:

- ♦ обнаружение «живости» (например, использование «капчи», запрос/ответ, оценка времени отклика);

- ♦ взаимная аутентификация, использование многофакторной аутентификации;

- ♦ использование устройств в защищенном исполнении (исключая устройства на стороне физических лиц);

- ♦ использование проверенных алгоритмов, «подписанных» компонент систем/кода, защита от отладки;

- ♦ защита каналов передачи данных;

- ♦ использование электронной подписи для данных, использование временных меток/Time-to-Live;

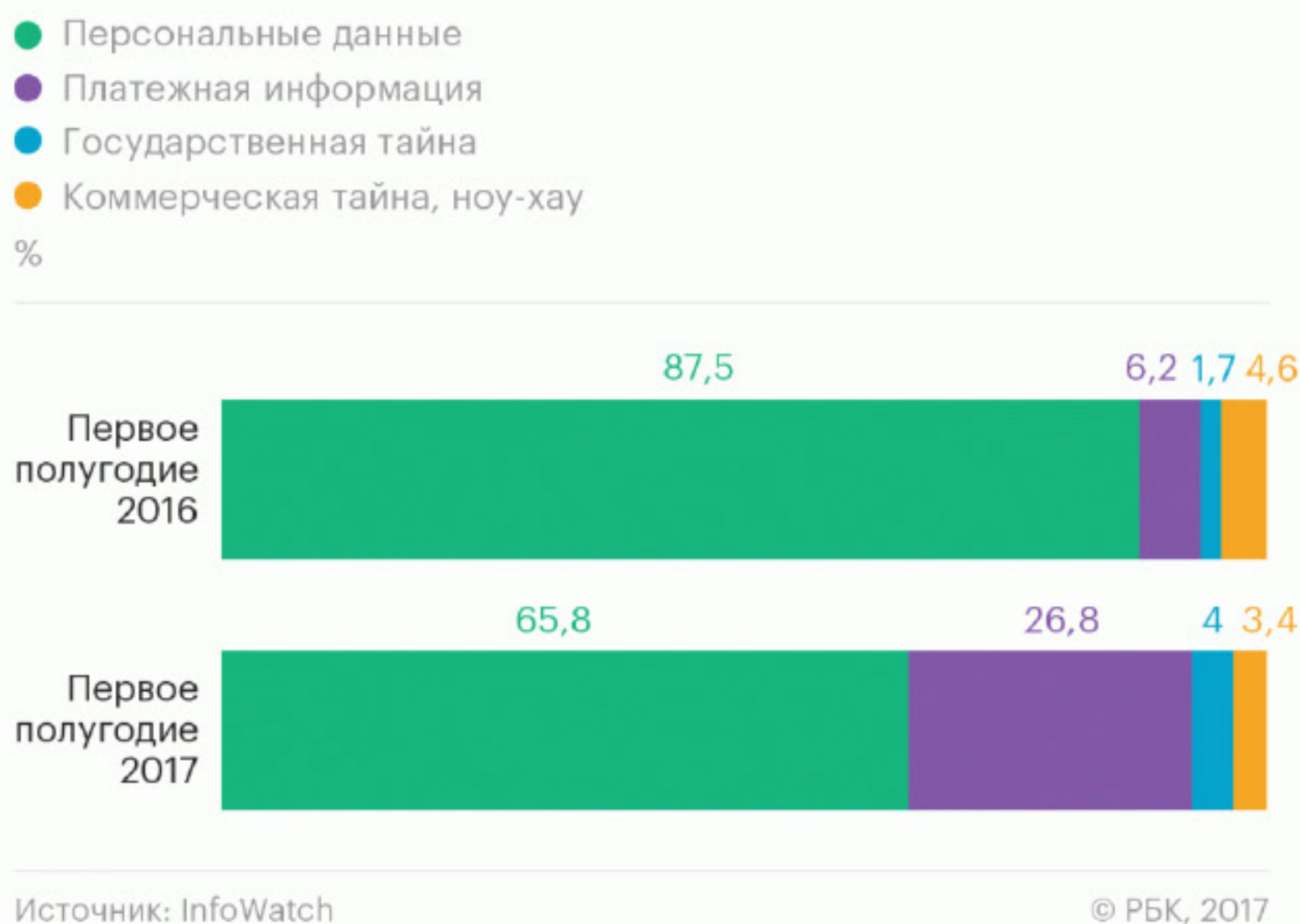
- ♦ контроль доступа к базам данных, защита серверов;

- ♦ хранение данных в зашифрованном виде, на смарт-картах и иных устройствах.

Однако, готово ли сейчас государство обеспечить защиту настолько глобальной критичной системы со столь чувствительными данными, являющейся естественной и очевидной целью для атак злоумышленников? Есть ли ресурсы и возможности для воздействия на риски, связанные с использованием ИТ-решений иностранных производителей?

Определенные шаги в направлении импортозамещения делаются. В ноябре 2015 г. Д.А. Медведевым подписано постановление о запрете на покупку зарубежного программного обеспечения для государственных и муниципальных нужд, а 26.07.2016 г. утвержден трехлетний план внедрения отечественных программных продуктов. Но даже с учетом этого, прогнозировать, будет ли возможность реализовать на основе открытого программного обеспечения и отечественных программно-аппаратных средств весь необходи-

Распределение утечек по типам данных



мый функционал ФРН, который, безусловно, станет значимым объектом критической информационной инфраструктуры РФ, пока сложно.

Другой не менее, а может, и более важный вопрос — готово ли население к ответственности за сохранность своих аутентификационных данных, к тому, что всю информацию о человеке можно будет получить на основании негласного персонального идентификатора. Для обеспечения безопасности информации одних физических мер защиты будет недостаточно (как паспорт запереть в сейф не получится, а если и получится, то все векторы атак на систему идентификации, которых более десятка, подобные меры не закроют).

По данным компании РБК, приведенным со ссылкой на исследование InfoWatch, в первом полугодии 2017 г. в мире произошла утечка 7,78 млрд записей с персональной и платежной информацией. Этот показатель почти в восемь раз выше, чем за аналогичный период 2016 г. (1,06 млрд записей), и более чем вдвое превышает количество данных, которые попали в руки третьих лиц за весь 2016 г. (3 млрд записей) (рис. 4).

По итогам 2016 г. по числу утечек Россия занимала второе место после США с 838 случаями утечек. Данные за 2017 г. на момент подготовки статьи еще не опубликованы. Будем надеяться, что в наших силах при поддержке регуляторов в новом 2018 году эту статистику переломить.

Рисунок 4. Распределение утечек по типам данных

ПОСЛЕ ПЕРВОГО ШАГА

ОТ РЕЕСТРА НАСЕЛЕНИЯ К РЕЕСТРУ СУБЪЕКТОВ



Карл СУММАНЕН
вице-президент Банка
ВТБ (ПАО), кандидат
физико-математических
наук

4 июля 2017 г. вышло распоряжение правительства РФ № 1418-р, утвердившее концепцию формирования и ведения единого федерального информационного ресурса, содержащего сведения о населении Российской Федерации (далее «Федеральный реестр населения», ФРН).

Как следует из декларируемой в концепции цели — «создание системы учета сведений о населении, обеспечивающей их достоверность и непротиворечивость, направленной на совершенствование контроля за начислением и поступлением страховых взносов на персонифицированные счета физических лиц», — ФРН ориентирован на решение конкретных частных задач электронного государства. Приоритетные стратегические задачи развития технологической инфраструктуры национальной экономики концепцией не затрагиваются и созданием ФРН не решаются.

В частности, внедрение ФРН, хотя и облегчает, но не обеспечивает решение задачи создания одного из ключевых компонентов технологической инфраструктуры, обеспечивающей представление субъектов в цифровом пространстве, без которого невозможно нормальное функционирование цифровой экономики. Таким компонентом является реестр субъектов, участвующих в экономических процессах, правоспособность которых признается национальным законодательством, независимо от категории (физическое или юридическое лицо, организация без образования юридического лица, индивидуальный предприниматель, киберсубъект¹ и т.д.), резидентности, места проживания или нахождения.

Представляется поэтому правильным рассматривать ФРН не как «конечную станцию», а как первый шаг в направлении создания полноценного реестра субъектов, удовлетворяющего требованиям как классической (аналоговой), так и цифровой экономики, и параллельно с внедрением ФРН начать разработку концепции такого реестра, приняв за отправную точку принципы, сформулированные в настоящей статье.

¹ Под киберсубъектом понимается программный алгоритм, самостоятельно (в автоматическом режиме), на основании полномочий, делегированных человеком, участвующий в экономических процессах

РЕЕСТР СУБЪЕКТОВ. РОЛЬ И МЕСТО В ЭКОНОМИКЕ

Экономику можно рассматривать как систему, состоящую из большого числа взаимодействующих² субъектов. При таком подходе субъект становится «центром мира», а система учета субъектов одним из ключевых элементов экономики. Рассмотрим общие требования к организации учета субъектов более подробно³:

Прежде всего, для взаимодействия субъектов в общем случае необходимо, чтобы каждое, участвующее в экономических процессах лицо, было юридически значимо определено как отдельный правоспособный субъект.

Общепринятым в современной экономике способом определения субъектов является регистрация — внесение записи о лице в реестр субъектов, признаваемый законодательством в качестве источника юридически значимой информации. Такой реестр является основой системы учета субъектов экономики. Подчеркнем, что реестр в данном случае понимается в самом общем смысле как совокупность носителей записей без указания на форму представления данных и архитектуру реестра. Т.е. реестр не обязательно централизованный или цифровой, например, совокупность переписных книг XVII века — это тоже реестр субъектов.

Далее, каждый субъект, участвующий во взаимодействии, в общем случае должен быть идентифицирован — однозначно выделен на полном множестве субъектов экономики. Для этого каждому субъекту, внесенному в реестр, должен быть присвоен постоянный в течении всей его жизни уникальный идентификатор, позволяющий однозначно отличить его от всех остальных субъектов.

Наконец, каждый участник взаимодействия должен иметь возможность получить о любом другом участнике взаимодействия всю необходимую ему информацию, например, о полномочиях и правоспособности, причем эта информа-

² Взаимодействие понимается в максимально широком смысле как любая одно-, двух- или многосторонняя сделка или операция, обмен сообщениями или материальными объектами между субъектами

³ Мы не рассматриваем другие условия, необходимые для взаимодействия, такие, как аутентификация, подтверждение сообщений или иные

ция должна быть достоверной. Это значит, что реестр субъектов должен быть полным, актуальным и доверенным источником данных. Кроме того, реестр должен обеспечивать возможность получения информации во всех режимах, которые могут возникать в процессах взаимодействия субъектов, например в режиме реального времени и с постоянной доступностью.

За время существования человечества сформировались различные способы ведения реестров субъектов. До настоящего времени эти способы в основном основывались на физическом контакте и использовании аналоговых (бумажных) документов, что, впрочем, не создавало особых проблем, поскольку экономика также была контактной и аналоговой. Ситуация изменилась, когда начался переход к цифровой экономике, которая предъявила к реестру субъектов дополнительные требования. Выяснилось, что классические способы ведения реестров субъектов этим требованиям удовлетворяют не полностью.

Основное отличие цифровой экономики от аналоговой состоит в преимущественном использовании цифровых документов, которые могут передаваться по телекоммуникационным каналам и заверяться электронной подписью. Благодаря этому в цифровом пространстве взаимодействия могут осуществляться дистанционно без физического контакта между их участниками. Это в свою очередь расширило возможности трансграничных взаимодействий между субъектами, находящимися в различных точках земного шара.

Трансграничность, цифровая форма и дистанционный характер взаимодействий выдвинули на первый план новые требования, которые существовали, но не были приоритетными в аналоговой экономике, — возникла потребность осуществлять взаимодействия в реальном времени, в любое время и с любыми контрагентами.

Учитывая, что взаимодействия в цифровом пространстве невозможны без обращений к реестру субъектов, который обеспечивает представление субъектов в цифровом пространстве, эти требования распространяются на реестр субъектов, который также должен предоставлять сервисы постоянно, в реальном времени и для всех категорий субъектов. Очевидно, что унаследованные от аналоговой экономики способы ведения реестров субъектов этим новым требованиям в полной мере не отвечают, как, к сожалению, не отвечают им и существующие информационные ресурсы электронного государства, включая, судя по концепции, ФРН.

Таким образом, для построения полноценной технологической инфраструктуры цифровой экономики необходимо создание отдельного специализированного федерального реестра субъектов (ФРС), удовлетворяющего всем перечисленным выше требованиям. Предлагаемые принципы организации такого реестра описываются ниже.

ПРИНЦИПЫ ОРГАНИЗАЦИИ ФРС

Предлагается реализовать ФРС (рис. 1) в виде централизованной на федеральном уровне базы данных⁴. Архитектурно ФРС должен рассматриваться как компонент технологической инфраструктуры, предоставляющий другим компонентам инфраструктуры и внешним потребителям сервисы по управлению субъектами экономики. ФРС также должен иметь возможность при необходимости использовать сервисы, предоставляемые другими компонентами инфраструктуры.

С организационной точки зрения ФРС, учитывая его роль и место в технологической инфраструктуре национальной экономики, должен иметь статус государственной информационной системы федерального уровня и находиться под управлением государства в лице уполномоченной организации (Оператора ФРС).

Основной задачей ФРС будет ведение реестра субъектов, включая поддержку процессов их регистрации, редактирования и подтверждения данных субъектов, хранение данных субъектов и предоставление информационных сервисов и сервисов управления субъектами внешним потребителям. ФРС должен обеспечить возможность регистрации любых субъектов, взаимодействующих в рамках национальной экономики, независимо от категории, резидентности, места проживания и места нахождения.

Регистрация субъектов в ФРС должна производиться добровольно по решению субъекта, например при возникновении необходимости в сервисах, доступ к которым возможен только при условии регистрации в ФРС, в частности, когда сервис требует указания Национального идентификационного кода (НИК) — универ-

⁴ В настоящей статье мы ограничимся рассмотрением централизованной архитектуры. Такая архитектура не является единственно возможной, существуют и заслуживают рассмотрения другие варианты архитектуры, имеющие свои преимущества и недостатки, например ФРС может быть организован в виде совокупности территориальных баз, объединенных федеральным компонентом. Окончательное решение о выборе архитектуры ФРС должно быть сделано на этапе проектирования

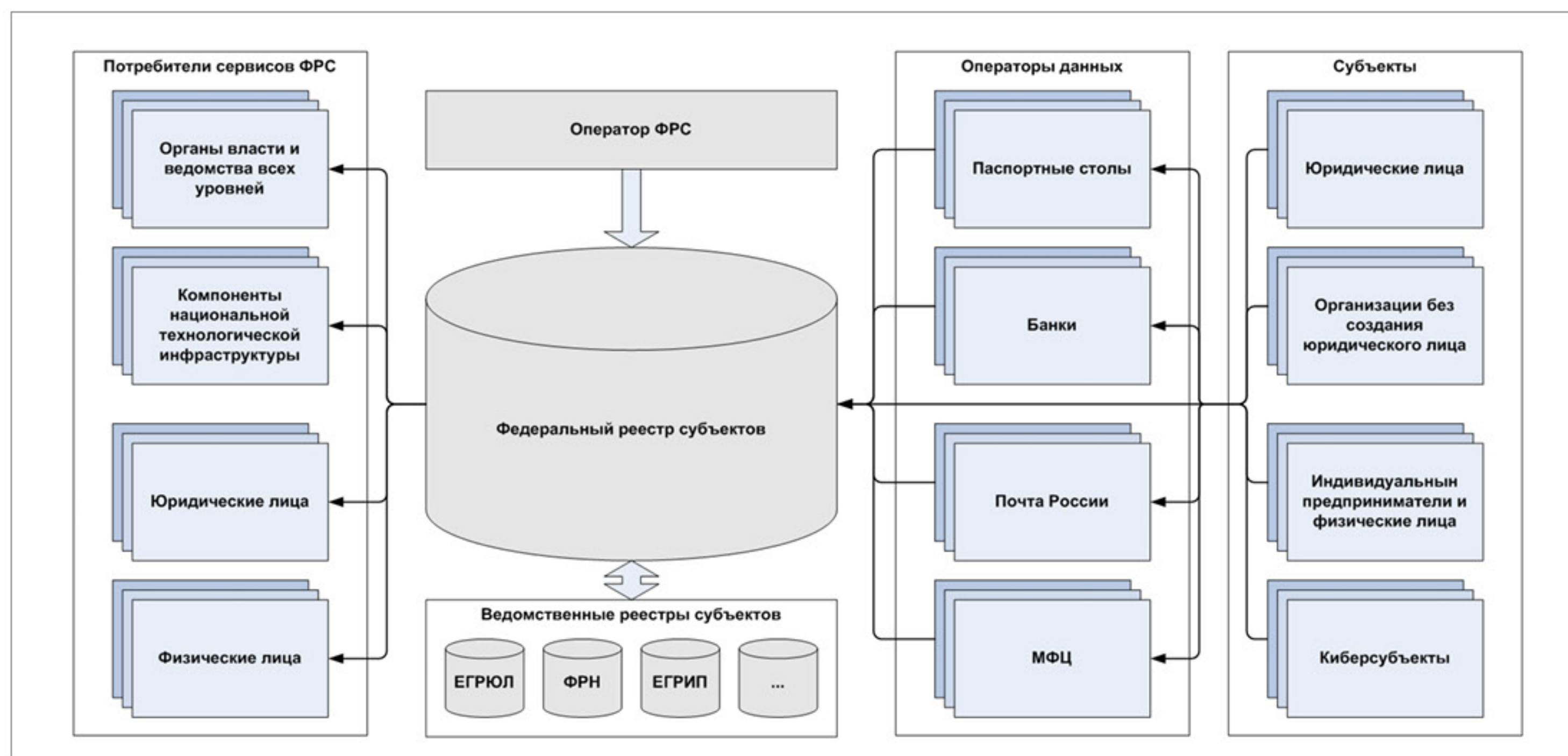


Рисунок 1. Логическая архитектура ФРС

сального идентификатора субъекта в рамках национальной экономики.

Должна разрешаться только однократная регистрация субъекта в ФРС, создание более чем одной учетной записи одного субъекта должно быть запрещено. Для выполнения этого требования при попытке регистрации должен производиться автоматический контроль по идентифицирующим атрибутам субъекта наличия в реестре учетной записи.

Должна быть предусмотрена возможность автоматического обращения ФРС с запросами к другим ресурсам для, получения дополнительных данных, контроля корректности или непротиворечивости и/или подтверждения введенных данных.

Возможность регистрации субъектов и управления данными субъектов должна быть предоставлена самим субъектам и уполномоченным организациям (Операторам данных), заключившим с Оператором ФРС соответствующее соглашение. Операторами данных могут быть любые организации обслуживающие субъектов, например ФНС, МФЦ, банки, Почта России, страховые компании, нотариусы, удостоверяющие центры.

Функции Операторов данных в зависимости от соглашения могут включать регистрацию субъектов, изменение, проверку и/или подтверждение данных субъектов, идентификацию субъектов в режиме личного присутствия, контроль документов субъекта на бумажном носителе, сбор от субъектов документов, заверенных личной подписью (подписями уполномо-

ченных лиц) субъекта, получение и обработку биометрической информации.

Данные субъекта в ФРС должны характеризоваться уровнем подтверждения, на основании которого потребители данных могли бы принять решение об их достоверности. Уровень подтверждения должен, в частности, содержать информацию об условиях подтверждения данных, например, лице, подтвердившем данные, режиме доступа, средствах аутентификации и источниках информации, использованных для подтверждения данных. Должен быть также реализован механизм автоматического подтверждения данных без участия Оператора путем сверки данных с внешними доверенными источниками информации.

Должна быть возможность назначать разным данным одного субъекта разные уровни подтверждения и одному набору данных одновременно несколько уровней подтверждения, например, от нескольких Операторов данных. Информация об уровне подтверждения должна храниться в базе данных ФРС и быть доступной потребителям данных. Анализ полученной информации об уровне подтверждения данных и принятие решения о доверии данным, а также ответственность за риск их недостоверности должны быть возложены на потребителя данных.

Генерация и назначение субъекту НИК должны происходить при регистрации последнего в ФРС. НИК должен назначаться субъекту один раз, не меняться в течение всего времени жизни субъекта и сохраняться после прекра-

щения его существования. Повторное использование НИК для других субъектов должно быть запрещено.

Алгоритм генерации НИК должен обеспечивать гарантированную уникальность в пределах полного множества субъектов национальной экономики. НИК должен использоваться для идентификации любых категорий субъектов и для всех видов и режимов взаимодействий, как дистанционных, так и контактных. При этом НИК не должен рассматриваться как секретная информация или персональные данные.

Чтобы обеспечить пожизненную неизменность, НИК должен быть как минимум инвариантен по отношению к атрибутам субъекта, в современном обществе подверженным частым изменениям, таким, как категория, резидентность, название, место жительства, пол. Для гарантированной неизменности желательно исключить зависимость НИК от любых атрибутов субъекта вообще.

НИК должен быть «социально доступным» и обеспечивать национально-языковую нейтральность, в том числе допускать возможность использования субъектами любой национальности, говорящими на любых языках, и возможность использования любыми категориями потребителей, в частности быть машино- и человекочитаемым.

НИК должен быть «технически доступным» и обеспечивать нейтральность по отношению к каналам и средствам доступа, допускать возможность передачи по любым каналам доступа, в средах с любой кодировкой символов, с применением любых средств доступа, в том числе с ограничениями по символам, в частности допускающим только ввод цифр.

С учетом использования человеком, НИК должен легко запоминаться и вводиться, в частности, иметь минимально необходимую длину. Для минимизации последствий совершения непреднамеренных ошибок при ручном вводе НИК должен иметь механизм их обнаружения с достаточной вероятностью в локальном режиме без обращения к ФРС. Для этого в состав НИК предлагается включить два контрольных разряда.

Поскольку единственное подмножество символов, единообразно понимаемое в разных языках и культурах, знакомое максимально широкому спектру потенциальных владельцев, минимально зависящее от кодировки и национальной специфики, — это арабские цифры, предлагается использовать в качестве НИК их последовательности.

Учитывая существование незначительного числа субъектов, по религиозным соображениям не согласных с присвоением числовых идентификаторов, предлагается разрешить в порядке исключения по просьбе субъекта создавать буквенные или буквенно-цифровые НИК произвольной длины (с обязательным соблюдением уникальности) при условии предоставления официального подтверждения принадлежности соответствующей религии и согласия с возможными ограничениями при получении сервисов⁵.

С учетом вероятного увеличения числа субъектов алгоритм генерации НИК должен обеспечивать возможность назначения НИК неограниченному числу субъектов для чего длину НИК предлагается не ограничивать⁶. Можно рассмотреть возможность назначения коротких НИК за плату по принципу «чем удобнее, тем дороже» (уменьшение длины, легко запоминаемые комбинации цифр и т.п.), наиболее короткие НИК можно продавать на аукционе.

КАК ПОСТРОИТЬ ФРС

Теоретически ФРС можно было бы создать на основе одного или нескольких существующих государственных информационных ресурсов, например путем расширения функциональности ФРН или ЕСИА. Очевидным преимуществом такого подхода является снижение расходов за счет частичного сохранения ранее сделанных инвестиций.

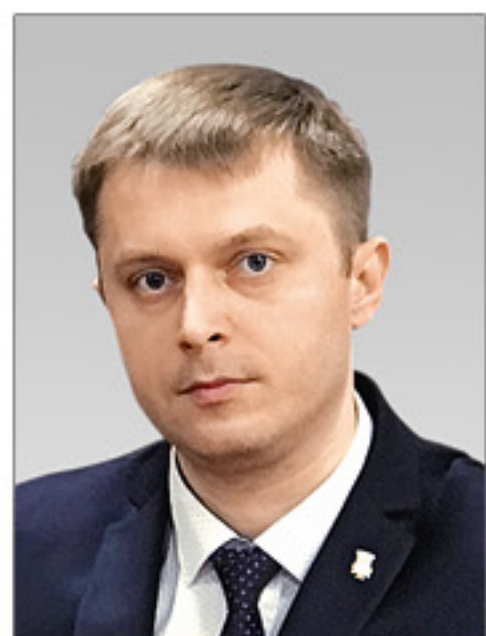
Однако, существующие реестры спроектированы для решения определенного класса задач и используются владеющими ими ведомствами для выполнения их функций. Попытка переориентировать их под новый класс задач с новыми требованиями (режим реального времени, постоянная доступность, расширение перечня категорий субъектов и состава информации и круга поставщиков и потребителей информации) потребовала бы радикального перепроектирования и неизбежно привела бы к конфликту интересов.

* * *

С учетом этого представляется более целесообразным создание ФРС как отдельного государственного информационного ресурса.

⁵ Провайдеры сервисов не обязаны поддерживать нецифровые НИК

⁶ Оценка показывает, что в случае использования двух контрольных разрядов и загрузки в ФРС всех живущих граждан РФ длина НИК будет составлять 11 разрядов, что вполне приемлемо с точки зрения возможности запоминания



**Алексей
ОЛЬШАНИКОВ**
ведущий специалист
отдела криптографической
защиты Управления
информационной
безопасности
АО «Гринатом»

КАК ОБУСТРОИТЬ ФУНКЦИЮ

ИНФОРМАЦИОННАЯ СИСТЕМА ОРГАНА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ГОСКОРПОРАЦИИ «РОСАТОМ»

Большинство крупнейших российских и мировых компаний используют модель бизнеса, при которой типовые транзакционные процессы передаются из организации в специализированный общий центр обслуживания. Придерживаясь данного принципа, госкорпорация «Росатом» создала многофункциональный общий центр обслуживания АО «Гринатом».

ДЛЯ ЧЕГО?

АО «Гринатом» создано для решения вопросов обслуживания предприятий атомной отрасли по информационным технологиям, бухгалтерским услугам, кадровому администрированию, а также становится новым центром компетенций по вопросам криптографической защиты информации.

АО «Гринатом», являясь лицензиатом ФСБ России, исполняет все требования действующих регламентирующих документов. Аккредитованный удостоверяющий центр АО «Гринатом» не просто выдаёт сертификаты на сертифицированных ключевых носителях, но и обеспечивает безопасность применения СКЗИ на рабочих местах пользователей атомной отрасли.

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

В атомной отрасли криптографическая защита применяется для многих аспектов защиты конфиденциальной информации: шифрования Корпоративной сети передачи данных, для до-

ступа к ИТ-ресурсам Госкорпорации «Росатом», для шифрования и подписи электронных сообщений, передаваемых через защищенную корпоративную почтовую систему и деловую почту, для подписи электронных сообщений при взаимодействии с межведомственным электронным документооборотом, отраслевой системе закупок. В Госкорпорации «Росатом» применяются все виды электронной подписи, начиная с простой подписи для ускорения переписки между предприятиями и заканчивая усовершенствованной квалифицированной подписью под юридически значимыми электронными документами.

Основой защиты конфиденциальной информации криптографическими методами является работа Администратора безопасности Органа криптографической защиты. Требования 152 инструкции ФАПСИ возлагают на него множество обязанностей. В тоже время обладатели конфиденциальной информации не уделяют должного внимания учёту этих трудозатрат. Для реализации всех необходимых мер АО «Гринатом» создало собственный орган криптографической защиты, который предлагает услугу «Администратор безопасности ОКЗ».

ДЕКОМПОЗИЦИЯ ТРЕБОВАНИЙ

Отдел криптографической защиты АО «Гринатом» произвёл декомпозицию требований регламентирующих документов к применению СКЗИ. Процессы деятельности органа криптографической защиты опубликованы в общем доступе на сайте crypto.rosatom.ru.

1200 АДМИНИСТРАТОРОВ ИБ

Объём работ администратора безопасности ОКЗ при использовании стандартных методов настолько велик, что один Администратор безопасности может обслужить не более 250 рабочих мест с СКЗИ без потери качества. При плановом объёме в 300 000 СКЗИ, используемых в отрасли, для выполнения всех требова-

**ПОЛЬЗОВАТЕЛЯМ ПРИХОДИТСЯ
ЗАПОЛНЯТЬ ЗАЯВЛЕНИЯ НА
СОЗДАНИЕ СЕРТИФИКАТА,
ДОВЕРЕННОСТЬ, ЗАВЕРЯТЬ КОПИИ
ПАСПОРТА И СНИЛС, ЕХАТЬ В УЦ
ДЛЯ ПОЛУЧЕНИЯ СЕРТИФИКАТА**

ний регулятора требуется 1 200 администраторов безопасности.

Проблемой использования услуг ОКЗ и удостоверяющих центров является то, что пользователи вовлечены в процесс криптографической защиты. Пользователям приходится заполнять заявления на создание сертификата, доверенность, заверять копии паспорта и СНИЛС, ехать в УЦ для получения сертификата.

ИСОКЗ

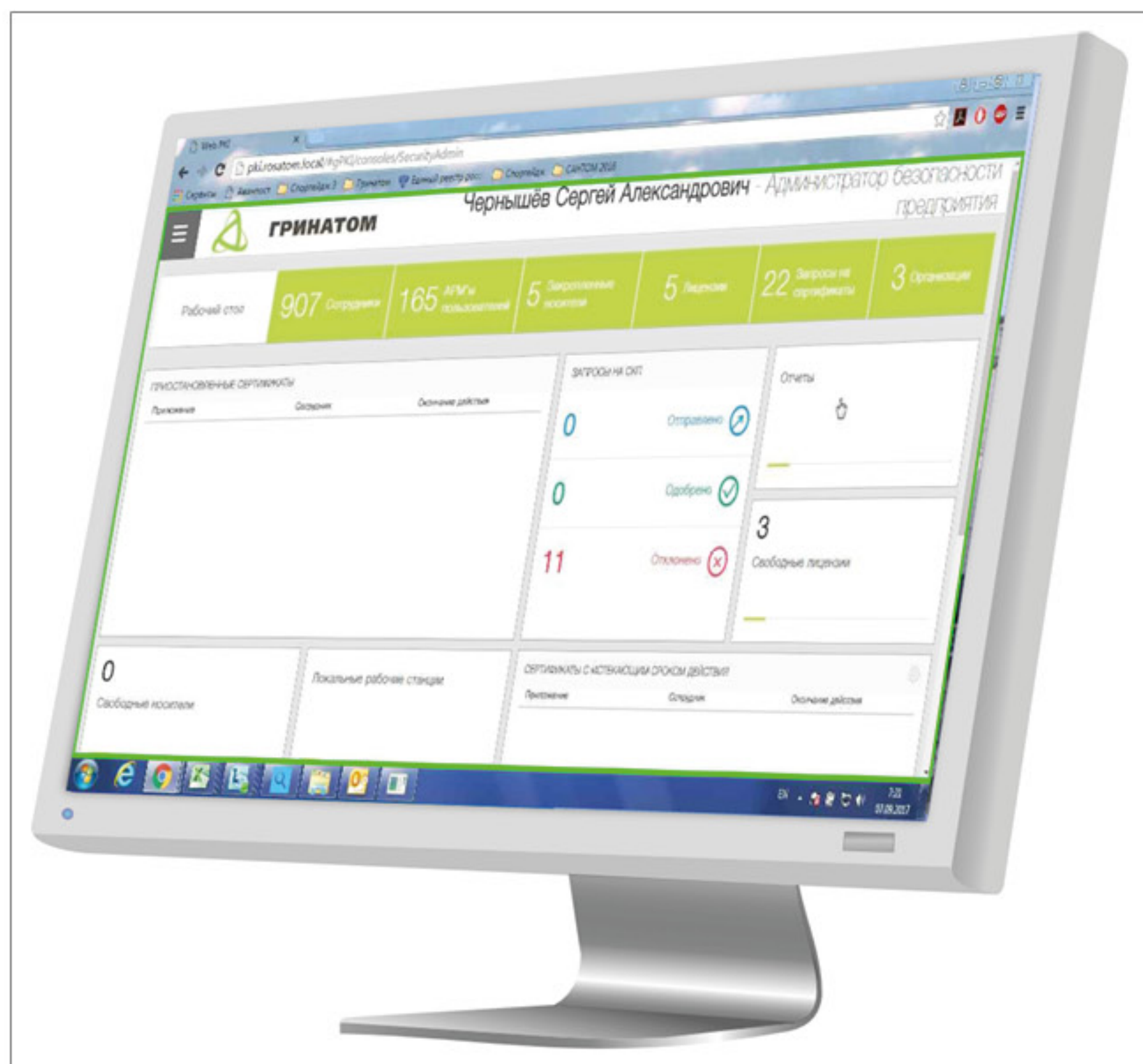
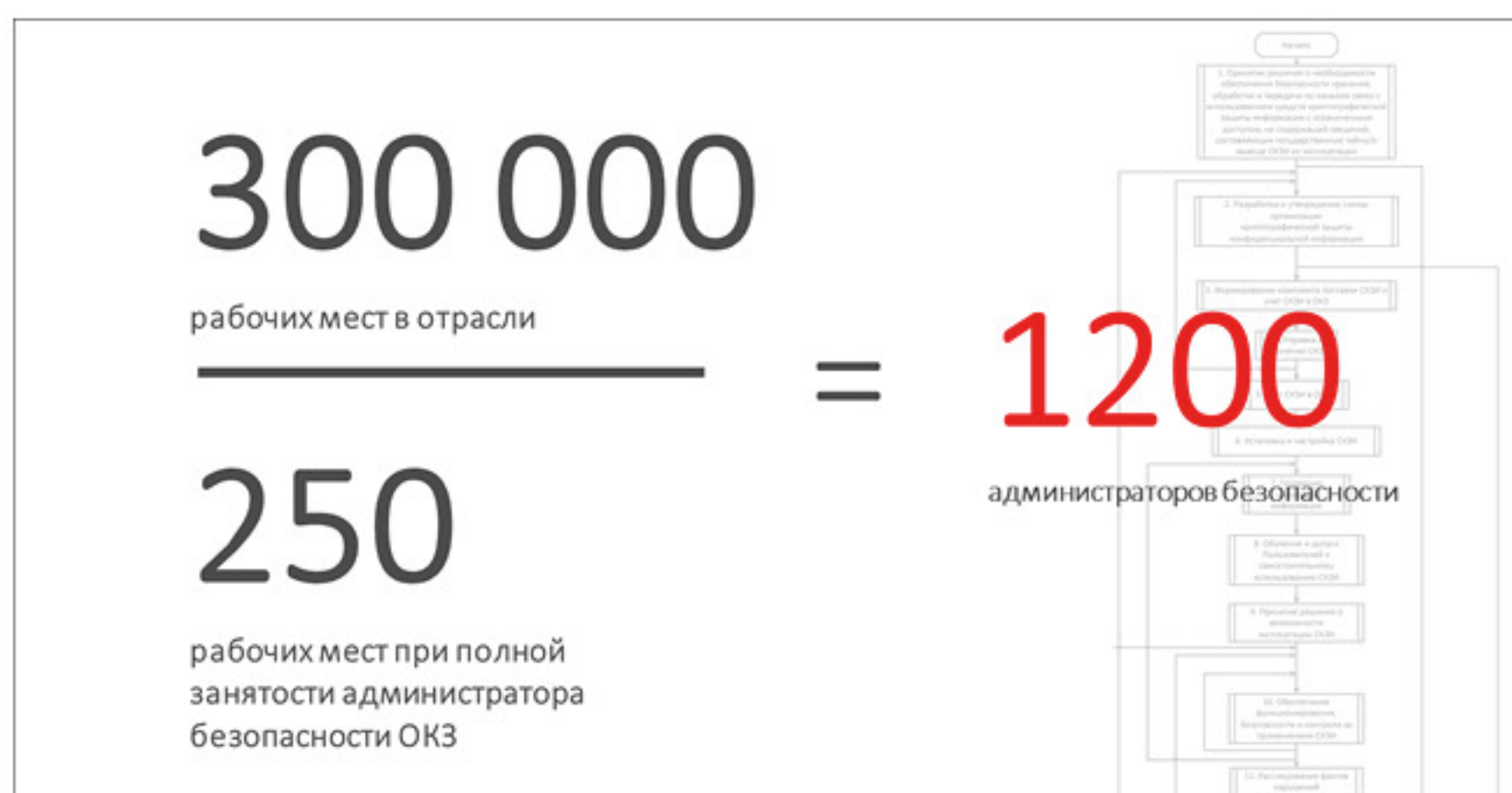
Анализируя стоящие перед нами вызовы, с 1 января 2017 года стартовали работы по созданию Информационной системы Органа криптографической защиты (ИС ОКЗ). Основными задачами которой являлись: снижение трудоёмкости администраторов безопасности на типовые операции, формирование и передача запросов на СКЗИ и сертификаты ЭП в ИС, создание единой схемы криптографической защиты Госкорпорации, уход от бумажного документооборота при распространении СКЗИ, создание единого архива дистрибутивов СКЗИ и документации, осуществление функций по управлению и контролю за деятельностью администраторов безопасности, предоставление заказчикам актуальной информации по состоянию криптографической защиты.

В качестве базовой платформы после оценки присутствующих на рынке решений была выбрана платформа Аванпост. Базовый функционал системы Аванпост РКІ был направлен на процесс выпуска сертификатов и учёта ключевых носителей, поэтому имеющийся продукт подвергся полной переработке. Новое решение направленно на управление работами администраторов ОКЗ.

ИНСТРУМЕНТ УПРАВЛЕНИЯ

Всем предприятиям, находящимся на обслуживании АО «Гринатом» по услугам лицензируемых видов деятельности в области криптографической защиты информации ИС ОКЗ предоставляется как бесплатный инструмент. С помощью ИС ОКЗ Администратор безопасности Органа криптографической защиты получает инструмент управления над СКЗИ заказчика, а заказчик сможет самостоятельно оформить подписку на нужную услугу по криптографической защите для пользователя и контролировать их выполнение.

Задачей ИС ОКЗ является отстранение пользователя от процесса криптографической защиты. Срок действия сертификата электронной подписи — последнее, о чём должен задуматься пользователь. Потребность пользовате-



ля в сертификатах ЭП и СКЗИ направляется на обученного администратора безопасности на предприятии. ИС ОКЗ реализует сервис подготовки заявлений и доверенностей пользователей на получение СКЗИ и сертификатов ЭП. Обучение и оформление допуска пользователя производятся так же системой ИС ОКЗ.

ТРИ РОЛИ

Предприятие, подписывающееся на услуги ОКЗ АО «Гринатом» в обязательном порядке должно определить три роли участников процесса криптографической защиты и указывает имена ответственных сотрудников в договоре присоединения, а также подтверждает соответствующие полномочия: Администраторы безопасности, Сотрудники кадровой службы,

Рисунок 1.
Информационная
система Органа
криптографической
защиты (ИС ОКЗ)

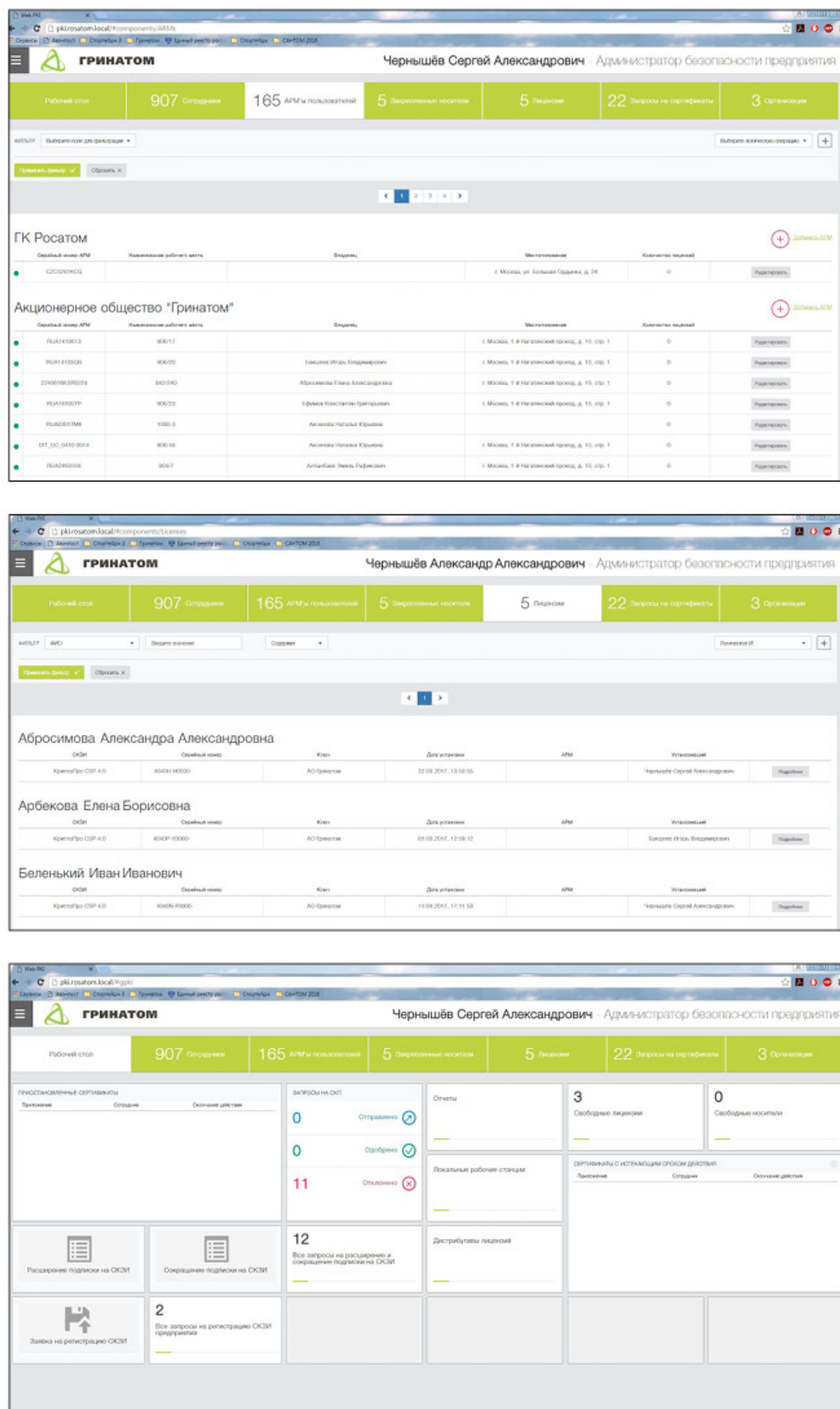


Рисунок 2. Три роли участников процесса криптографической защиты

Уполномоченные должностные лица. Для каждого типа пользователя в ИС ОКЗ существует рабочий стол, на котором отражаются задачи, решаемые пользователями.

Первичным справочником данных является база корпоративного Active Directory. Администратор безопасности указывает параметры запроса на сертификат или СКЗИ. Кадровая служба дополняет запрос проверенными достоверными данными пользователя СНИЛС и паспортными данными пользователя. Уполномоченное лицо согласует запрос и подтверждает

полномочия пользователя по получению сертификата ЭП. Полученные данные ИС ОКЗ направляет для проверки в Систему межведомственного электронного взаимодействия.

БЕЗ ПОДПИСКИ НИКАК

После успешной цепочки проверок формируется основной объект в ИС ОКЗ — подписка. Подписка является основанием для ежегодного выпуска сертификата ЭП и обслуживания СКЗИ пользователя и содержит все необходимые исходные данные.

ИС ОКЗ способна создавать различные маршруты для квалифицированных и неквалифицированных сертификатов и способна взаимодействовать с разными центрами сертификации.

В случае необходимости выпуска сертификата ИС ОКЗ формирует соответствующее задание Оператору УЦ. Запрос на сертификат подготавливается для переноса в ИС Корпоративного удостоверяющего центра. Если используемое СКЗИ предусматривает плановые регламентные работы (например проверку датчика случайных чисел), ИС ОКЗ планирует соответствующую работу для Администратора безопасности.

ИС ОКЗ имеет встроенную подсистему обучения на базе решения российской компании Websoft — «Web tutor», выполняющую следующие задачи: обучение администраторов, обучение пользователей, приём зачётов, допуск пользователей, периодический контроль и допуск к работе с СКЗИ.

БЛАГОРОДНАЯ ЦЕЛЬ

Бытует мнение, что при внедрении массовой криптографии, широкий круг пользователей будет неквалифицированным. Целью ИС ОКЗ является сформировать массового квалифицированного пользователя. Как показал опыт, презентации или текстовой инструкции по использованию СКЗИ недостаточно. Совместно с Центральным институтом повышения квалификации Росатома и Учебным центром «Информзащита» разработаны специализированные курсы для администраторов ОКЗ Росатома, планируется создание адаптивного курса для пользователей СКЗИ и руководителей — владельцев конфиденциальной информации.

ИС ОКЗ имеет интерфейс аудитора и сервис построения отчётов для проведения контрольных мероприятий аудиторами ОКЗ и внешних проверяющих органов. Внутренние аудиторы имеют постоянные учётные записи и используют сервис при плановых проверках, которые проходят более 40 предприятий ежегодно.

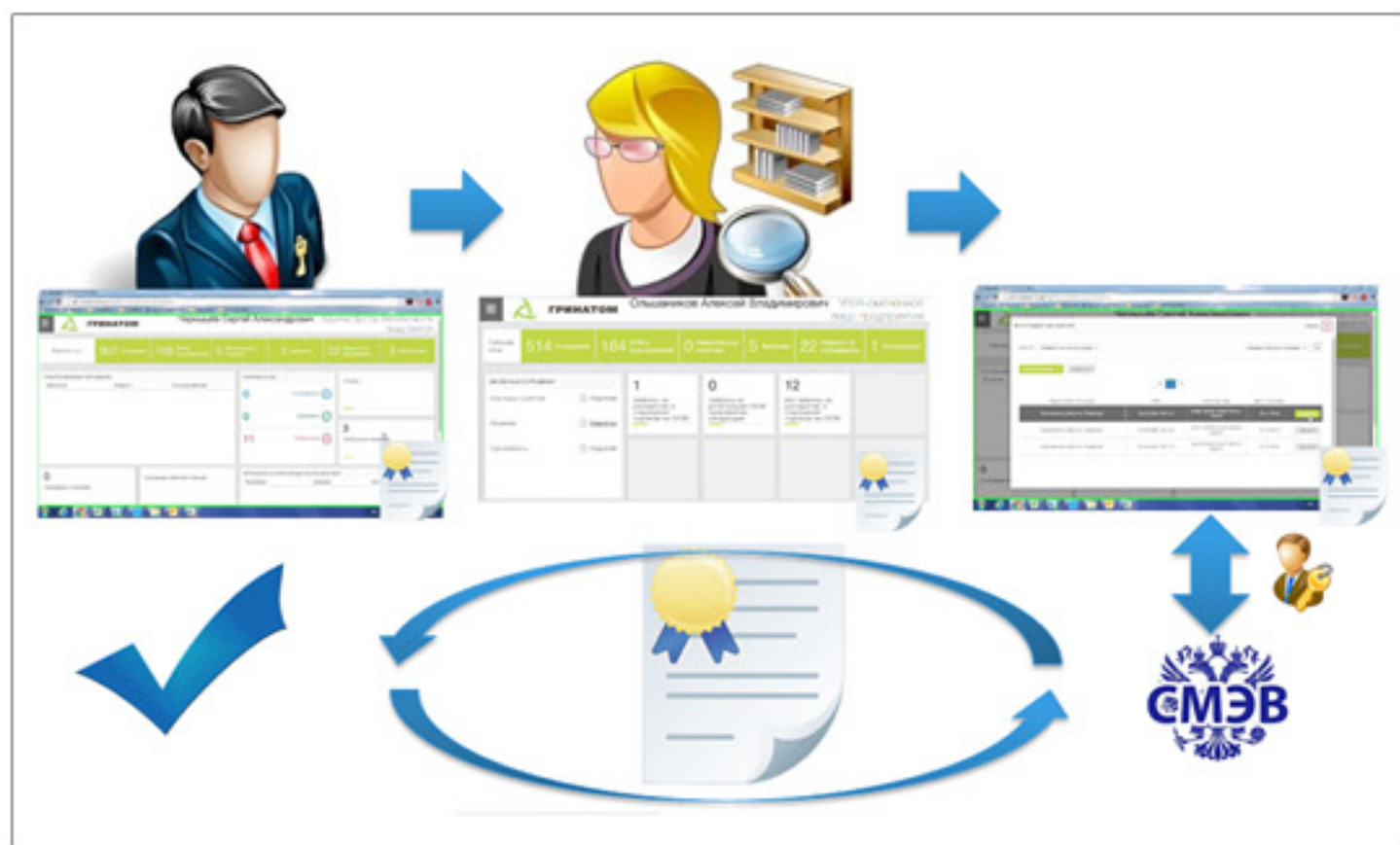


Рисунок 3. Схема работы ИС ОКЗ



Рисунок 4. Агент ИС ОКЗ

АГЕНТ В РАЗРАБОТКЕ

В разработке также находится Агент ИС ОКЗ, который устанавливается на рабочее место с СКЗИ и добавляет новые возможности:

- ◆ подтверждение факта владения ключом на основании входа в учётную запись пользователя в домене Госкорпорации;
- ◆ подтверждение внесения изменений в среду функционирования СКЗИ;
- ◆ осуществление допуска пользователя к работе с СКЗИ после успешной сдачи зачётов

и допуска к работе с СКЗИ;

- ◆ контроль ключевой информации.

* * *

ИС ОКЗ находится в опытной эксплуатации. Переход в промышленную эксплуатацию запланирован после финальных доработок, сертификации продукции и аттестации по требованиям информационной безопасности и запланирован на третий квартал 2018 года.

XI Межотраслевой Форум CISO FORUM 2020: взгляд в будущее

23–24 апреля 2018 г. • Москва



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

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



Александр БОДРИК
заместитель генерального директора
ANGARA Professional Assistance



Лев ПАЛЕЙ
независимый эксперт



Виктор ФЕДОТОВ
руководитель отдела сервисных проектов
ANGARA Professional Assistance

УРОКИ ПРОСТОТЫ

ИНЦИДЕНТ ПОКАЗАЛ, ЧТО ПРИ ЗАЩИТЕ ТЕХНОЛОГИИ ВТОРИЧНЫ

Всеобщее увлечение популярными продуктами обеспечения ИБ — Sandbox, UEBA, SIEM, DLP — удивляет, ведь такие продукты могут быть эффективны только в операционной среде определенного уровня. В среде с четко заданными понятиями «хорошо» и «плохо», с регламентированными ИТ-процессами. Дабы не быть голословными, приведем пример одного из дней, когда, несмотря на наличие целого спектра систем ИБ (SIEM, host Anti-APT и многих других), инцидент ИБ реализовался и был обработан. Возьмем самый показательный пример — заражение вредоносом типа «ransomware» или попросту шифровальщиком-вымогателем.

Система координат: государственная компания, распределенная инфраструктура, десятки тысяч ПК, установленные и используемые средства ведущего российского производителя в качестве защиты конечных точек, известный российский сканер как система сканирования уязвимостей, еще

десяток других средств защиты информации (СЗИ) (накопленный размер инвестиций в системы защиты информации за несколько лет составил более 500 миллионов рублей) и команда Managed Services (поддержка СЗИ) из 15 человек сервис-провайдера услуг безопасности (MSSP).

Дата: 15 сентября 2017 года.

Последовательность событий.

♦ В 10:00 в MSSP поступило сообщение о возможном вирусном заражении в государственной организации с компьютерным парком более 30 000 точек.

♦ По результатам генерирования отчетности о сетевых атаках средствами Kaspersky Security Centre было выявлено 82 зараженных ПК в сети, 38 из которых принадлежали одному из филиалов. Первая атака датировалась 13 сентября и была принята как точка отсчета.

♦ Инструмент атакующих в соответствии с отчетом Kaspersky Security Centre фиксировался как «Kintrusion.win.ms17-tcp010.o», использующий нашу-мевшую уязвимость в SMBv1, закрытую Microsoft в патче MS-17010.

♦ Причиной заражения и долгого периода обнаружения стало отсутствие ПК в домене, и как следствие — нераспространение политик по установке обновлений ОС и агентов антивирусного ПО на такие ПК.

♦ Отсутствие ПК в домене, равно как и отсутствие антивирусного ПО, было вызвано недостаточной аппаратной мощностью десятков ПК.

♦ Процесс реагирования был начат с 38 ПК, сосредоточенных в одном из удаленных филиалов (ЦФО). Производилось обновление ОС и установка антивирусных средств там, где позволяли мощности машин. При невозможности подключения к зараженным машинам, проблема эскалировалась выше с просьбой оказать содействие в отключении. Аналогичные рекомендации были переданы в другие филиалы компании, в которых были обнаружены зараженные ПК (еще 44 единицы).

♦ Для выявления других зараженных машин также использовалось сканирование сканером защищенности на уязвимость к WannaCry. Полученный список был передан инженерам на объекте для установки обновлений.

♦ В 15:00 появилась информация от работников пострадавшей компании, что выявленный вредонос не является WannaCry и не шифрует данные, а приводит к перезапуску серверов, вызванному ошибками операционной системы.

НЕСМОТЯ НА НАЛИЧИЕ ЦЕЛОГО СПЕКТРА СИСТЕМ ИБ (SIEM, HOST ANTI-APT И МНОГИХ ДРУГИХ), ИНЦИДЕНТ ИБ РЕАЛИЗОВАЛСЯ И БЫЛ ОБРАБОТАН



♦ В 15:00 представители MSSP стали создавать групповую политику, отключающую службу mssecsvc2.0. Отключение этой службы заставляло вредонос «засыпать», т. е. обезвреживать вредонос даже на машинах без современного антивируса.

♦ В 17:00 представителями MSSP предложено отключить все зараженные машины от сети. IP-адреса были известны, необходимо было вычислить MAC-адреса и отключить порты, на которых были зарегистрированы такие MAC.

Тело вредоноса было получено 18-го сентября с ПК с нестандартной политикой и без установленного антивируса. По итогам расследования были отмечены интересные моменты, дополняющие общую картину развития инцидента.

♦ Файл на исходной машине в карантине детектируется как wapna.a, но при сохранении на другом ПК определяется как wapna.m.

♦ Исходя из данных по результатам проверки файла на VirusTotal, лишь 48 из 63 антивирусных движков находят вирус (при этом с разными номенкла-

ДАЖЕ В УСЛОВИЯХ ОТСУТСТВИЯ СОВРЕМЕННОГО АНТИВИРУСА, ЭКСПЕРТИЗА ПРОФЕССИОНАЛЬНОЙ КОМАНДЫ МОЖЕТ ПОМОЧЬ ОСТАНОВИТЬ АТАКУ

турами: и «m», и «a», и «h»), а сигнатурный анализ от 2-х из 4-х лидеров рынка NGFW (по версии Gartner) с актуальными базами определяет файл как «чистый».

Полученный опыт позволил сделать ряд однозначных выводов:

1. «Снова к основам». Никакие, даже самые дорогостоящие и функциональные средства защиты, не спасут, если нет основ — установленных обновлений, безопасной конфигурации рабочих станций и серверов, установленных и обновленных антивирусов.

2. «Подковать блоху». Даже в условиях отсутствия современного антивируса, экспертиза профессиональной команды может помочь остановить атаку.

3. «Время — деньги». Несмотря на предотвращенный ущерб от инциден-

та, атака длилась минимум 7 часов. Ее можно было остановить быстрее, будь у Заказчика свой SOC или подключение к сервисному SOC. В данном случае пришлось использовать традиционную команду Managed Services с несколько иным фокусом на администрирование СЗИ и без SLA на реагирование.

* * *

Общий вывод. Защищенная корпоративная инфраструктура основывается на работе профессиональной команды защитников (желательно внутренней) и отлаженных процессах управления стандартами ИТ-инфраструктуры и взаимодействия ИТ и ИБ-подразделений. А уж технологии — фундаментально вторичны.



Вадим ЩЕМЕЛИНИН
руководитель отдела ООО «ЦРТ»,
кандидат технических наук



Галина ЛАВРЕНТЬЕВА
научный сотрудник ООО «ЦРТ-инновации»

ПРОДУКТ ПОБЕДЫ

ПОСЛЕДНЕЕ ДОСТИЖЕНИЕ ОТЕЧЕСТВЕННОЙ
ГОЛОСОВОЙ БИОМЕТРИИ – ПОБЕДА КОМАНДЫ
ЦРТ В МЕЖДУНАРОДНОМ КОНКУРСЕ СРЕДИ
РАЗРАБОТЧИКОВ ДЕТЕКТОРОВ СПУФИНГ АТАК

Биометрия давно привлекает внимание BIS Journal, в каждом номере публикуется хотя бы один заметный материал на эту тему. Из последних — статьи А. Митрофанова («Объект опознан! Использование биометрии в банковской сфере» № 3/2017) и Г. Маршалко («Не панацея. Угрозы безопасности биометрических систем» № 4/2017), в которых дан квалифицированный анализ тенденций развития биометрических технологий.

В развитие темы предлагаем статью о последних достижениях в области голосовой биометрии. Этот материал примечателен еще и тем, что представляет систему, одержавшую победу в международном конкурсе среди разработчиков детекторов спуфинг атак «Automatic Speaker Verification Spoofing and Countermeasures Challenge 2017». Стоит отметить, что в конкурсе участвовало 113 команд, до финала дошли 43, в том числе и команды компаний Samsung и Pindrop, являющиеся признанными лидерами на мировом рынке голосовой биометрии.

О СПУФИНГ АТАКАХ

Развитие компьютерных технологий в последние десятилетия дало возможность совершить прорыв в области об-

работки речевого сигнала. Современный мир уже сложно представить без повседневного использования речевых технологий. Системы распознава-

ния речи позволяют не отвлекаться на управление мобильными устройствами во время движения за рулём, системы синтеза речи оповещают нас по телефону, в метро, на вокзалах и офисах, голосовые биометрические системы обеспечивают доступ к защищенным персональным данным или помогают в поиске нарушителей. Исследования голосовых биометрических технологий занимают одно из ведущих мест в области обработки речевого сигнала.

Однако в последнее время потребители биометрических систем озабочены не только качеством непосредственно алгоритмов голосовой биометрии, но и устойчивостью систем к специфичным для голосовой биометрии видам атак, проводимых с целью получения несанкционированного доступа к защищаемой информации.

Ранее основные виды атак на голосовые биометрические системы и методы противодействия им уже рассматривались (С. Мельников «Верификация по голосу: надежно ли? Впечатления, наблюдения и размышления участника конференции Interspeech-2013», BIS Journal № 1/2014; К. Симончик, Д. Щетинин «Защита от подделки голоса в биометрических системах: со-

ПОТРЕБИТЕЛИ БИОМЕТРИЧЕСКИХ СИСТЕМ ОЗАБОЧЕНЫ НЕ ТОЛЬКО КАЧЕСТВОМ НЕПОСРЕДСТВЕННО АЛГОРИТМОВ ГОЛОСОВОЙ БИОМЕТРИИ, НО И УСТОЙЧИВОСТЬЮ СИСТЕМ К СПЕЦИФИЧНЫМ ДЛЯ ГОЛОСОВОЙ БИОМЕТРИИ ВИДАМ АТАК



Рисунок 1. Схема направленных спуфинг атак на голосовую биометрическую систему

временное состояние дел», BIS Journal № 4/2016). Напомним, виды спуфинг атак на биометрическое устройство ввода (рис. 1) можно разделить следующим образом:

- ♦ методы имперсонализации путём пародирования речи;
- ♦ методы записи речи и дальнейшего повторного воспроизведения при атаке, к примеру, запись и воспроизведение с диктофона;
- ♦ методы автоматического преобразования речи, основанные на технологии конвертации речевых характеристик злоумышленника в целевые речевые характеристики;
- ♦ методы автоматического синтеза речи, основанные на технологии преобразования текста в речь.

Несмотря на успехи [1] в решении данной задачи, вопрос поиска новых, надежных методов противодействия таким видам спуфинг атак остаётся актуальным. Действительно, с точки зрения злоумышленников, за последние время не получили развития только методы атак, основанные на имперсонализации. Ведь пародисты преимущественно изменяют тональность и манеру речи, но не могут изменить свой голосовой тракт, индивидуальные особенности строения которого и лежат в основе технологии голосовой биометрии. Методы атак, основанные на записи и повторном воспроизведении «replay attacks», не эффективны при использовании динамической парольной фразы. Однако, использование статической парольной фразы, такой как «Ok Google» или «Привет Siri», позволяет пользователю пройти аутентификацию быстрее и удобнее.

Активное развитие технологий синтеза и преобразования речи, лежащих в основе двух оставшихся видов атак, также позволяет злоумышленникам обучать систему спуфинга на меньшем объёме данных и с лучшим качеством. Актуальность такой задачи подтверждается не только проведением большого объема исследований в этом направлении, но и выходом новых стандартов оценки биометрических систем. Так в 2016 и 2017 годах национальный институт стандартов и технологий США NIST подготовил и ввел пакет стандартов ISO/IEC 30107, описывающих порядок оценки устойчивости системы к подобным атакам.

Большая часть существующих алгоритмов противодействия спуфинг атак, в силу ограниченного количества записанных баз, обучена защите от атак конкретного типа, а также от атак, подготовленных с использованием или ограниченного числа устройств воспроизведения или записи, выполненной в определенных акустических условиях. В то же время, реальные атаки основаны на неизвестных методах фальсификации индивидуальных биометрических характеристик человека.

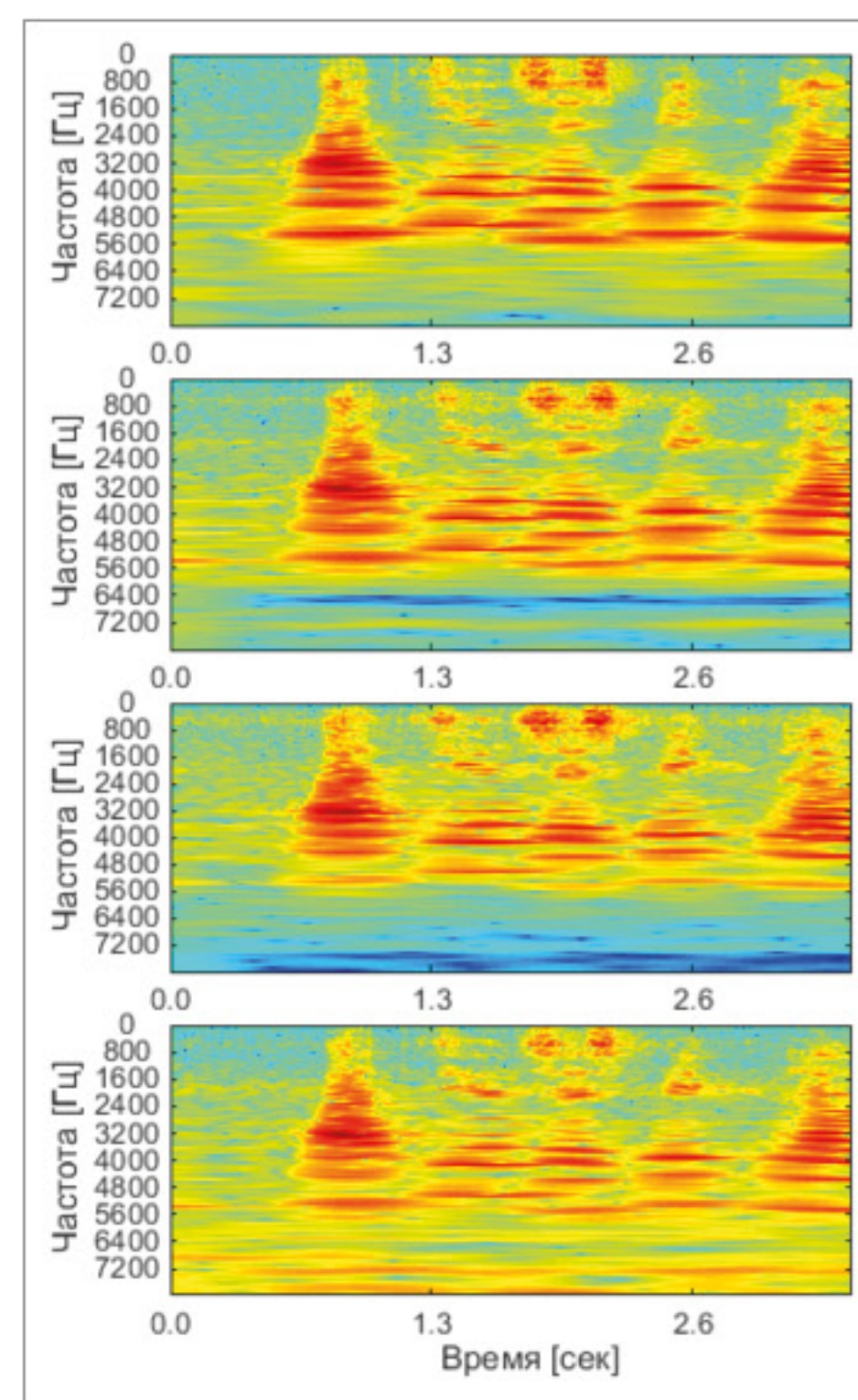


Рисунок 2. Амплитудные спектры реального сигнала (верхний) и трех атак повторного воспроизведения записи фразы «Actions speak louder than words», записанной на различные мобильные устройства

Задача выявления атак может быть сведена к детектированию локальных артефактов, специфических для тех или иных методов спуфинга и отличающих их от реальной речи.

На рисунке 2 приведены отображения амплитудных спектров реального сигнала для реальной записи (верхний) и трех атак повторного воспроизведения этой записи, записанных на разные мобильные устройства. Мы можем видеть некоторые изменения спектра в области высоких частот, однако выделить определенную особенность атаки, которая позволила бы надежно определить повторную запись, практически невозможно. Справиться с такой задачей могут помочь мощные современные средства ана-

ИСПОЛЬЗОВАНИЕ СТАТИЧЕСКОЙ ПАРОЛЬНОЙ ФРАЗЫ, ТАКОЙ КАК «OK GOOGLE» ИЛИ «ПРИВЕТ SIRI», ПОЗВОЛЯЕТ ПОЛЬЗОВАТЕЛЮ ПРОЙТИ АУТЕНТИФИКАЦИЮ БЫСТРЕЕ И УДОБНЕЕ



Рисунок 3. Обобщенная структура системы детектирования спуфинг атак на голосовые биометрические системы

лиза данных, такие как метод статистического факторного анализа и нейронные сети.

СИСТЕМА АВТОМАТИЧЕСКОГО ДЕТЕКТИРОВАНИЯ АТАК

Обобщенная система автоматического детектирования атак может содержать четыре основных модуля: модуль предварительной обработки сигнала, модуль выделения информативных акустических признаков, модуль выделения признаков высокого уровня и классификатор (рис. 3).

Модуль предварительной обработки является первым шагом работы алгоритма и используется для детектирования атак низкого уровня. Специфические артефакты в таких атаках легко можно обнаружить простыми методами фильтрации.

Вторым шагом является извлечение акустических признаков из входного сигнала, то есть речевых характеристик, надежно отличающих спуфинг атаку от реальной речи. Успех работы системы напрямую зависит от информативности этих признаков и их дискриминирующей (разрешающей) способности. Как показали предварительные исследования, для различных типов атак более информативными являются признаки, содержащие разную информацию. Так, для детектирования синтезированной речи используются признаки, содержащие фазовую информацию сигнала, т.к. синтезированная речь не восстанавливает фазу сигнала естественной речи человека при построении, а для атак повторного воспроизведения такие признаки являются бесполезными, т.к. фазовые признаки для перезаписанного сигнала соответствуют оригиналу. Для детектирования повторного воспроизведения наилучшие результаты показали

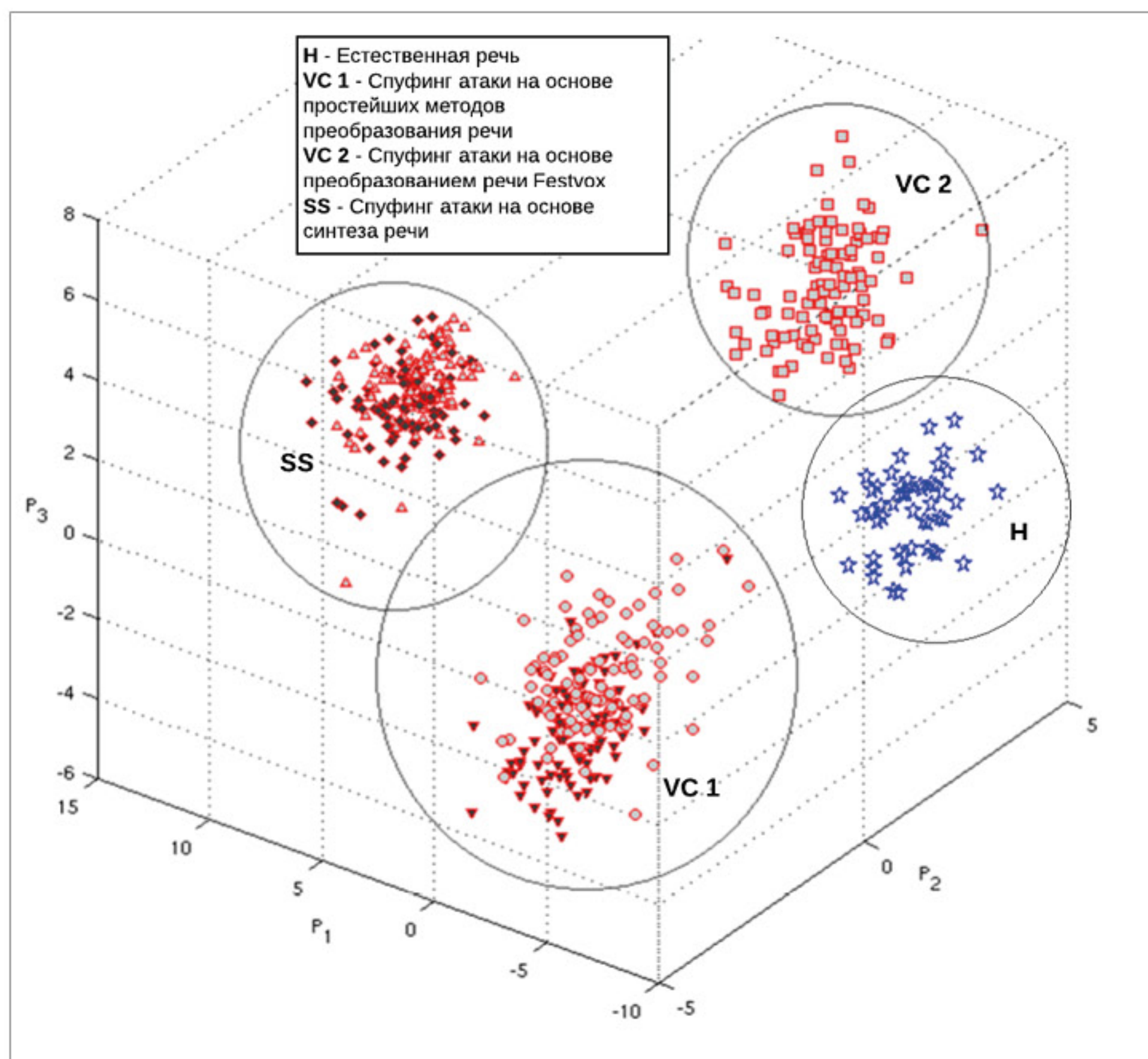


Рисунок 4. LDA проекции MWPC векторов на первые три оси главных компонент

системы на основе использования графического представления амплитудного спектра входного сигнала.

По этой причине модуль извлечения акустических признаков представляет собой комбинацию нескольких методов извлечения речевых характеристик из входного сигнала.

Полученные векторы информативных акустических признаков подаются на вход следующего модуля, который позволяет извлечь признаки высокого порядка.

Такой подход позволяет определить проекцию пространства акустических признаков на пространство новых признаков высшего порядка таким образом,

чтобы минимизировать внутриклассовое и максимизировать межклассовое расстояние в новом пространстве. Благодаря этому можно перейти в пространство, где класс реальных записей лучше отделим от класса спуфинга. На рисунке 4 представлены LDA проекции на первые три главные компоненты, полученные с помощью применения линейного дискриминантного анализа. В качестве акустических признаков здесь могут быть использованы мел-кепстральные коэффициенты на основе вейвлет-пакетного преобразования (MWPC) [2]. Здесь наглядно видно как хорошо распределены признаки для классов реальной речи, синтеза и преобразованной речи.

Для извлечения высокоуровневых аудио признаков из спектрограмм сигнала использовались конволюционные нейронные сети. Такой подход показал хорошие результаты для детектирования атак повторного воспроизведения.

На следующем шаге полученные признаки подаются классификатору, который принимает решение о том, является ли входной сигнал реальной речью или попыткой взлома. В качестве классификаторов для различных признаков высокого уровня могут быть использованы методы опорных векторов, классификатор на основе гауссовых распределений, а также нейронные сети.

В силу того, что для детектирования различных типов атак используются различные акустические признаки, и как следствие различные классификаторы, в результате подготавливается несколько подсистем, нацеленных на детектирование тех или иных типов атак. Обобщенное решение системы строится как линейная комбинация решений этих подсистем, где вклад каждой подсистемы регулировался соответствующим весовым коэффициентом.

МЕЖДУНАРОДНЫЙ КОНКУРС

Большой вклад в развитие данного направления вносит команда исследователей под руководством Tomi Kinnunen из University of Eastern Finland и Nicholas Evans из EURECOM, Финляндия. В 2017 году ими был организован меж-

дународный конкурс «Automatic Speaker Verification Spoofing and Countermeasures Challenge 2017» среди разработчиков детекторов спуфинг атак [3]. В этот раз основной упор был сделан на детектирование спуфинг атак методом записи и повтора. Особое внимание было уделено реалистичности имитируемых атак. Для этой задачи организаторы использовали различные устройства записи и воспроизведения сигнала, сформировав тем самым 110 уникальных конфигураций для проведения спуфинг атаки.

До финала конкурса дошло 49 команд из 113 подавших заявки. Система, основанная на методах, описанных в начале данной статьи и разработанная компанией ЦРТ, заняла первое место с результатом равновероятной ошибки детектора EER=6,73% [3], что почти в два раза лучше, чем результат системы занявшей второе место (EER=12,34%) и в четыре раза лучше, чем базовая система организаторов (EER=24,77%) [4].

Среди участников конкурса также были исследователи из таких известных компаний как Samsung [5] и Pin-drop [6]. Последняя является компанией номер один на американском рынке голосовой биометрии по данным Orus Research 2017 года.

Результаты конкурса наглядно показали, что простые спуфинг атаки, основанные на записи и повторе, требуют ничуть не меньше внимания, чем ата-

ки, основанные на синтезе и преобразовании речи, и эффективно детектировать их значительно сложнее.

НЕ ВСЕ ЕЩЕ ОТРАБОТАНО

Несмотря на достигнутые успехи, на данный момент задача по-прежнему остаётся крайне актуальной. Имеющиеся решения хотя и показывают высокий результат в конкурсных условиях, но могут снижать качество своей работы при существенном изменении канала или сценария работы системы. Вместе с этим, важно помнить, что конечная эффективность биометрической системы, должна оцениваться комплексно, с учетом одновременной работы детектора спуфинг атак и биометрического распознавания по всем доступным модальностям. Ведь одновременное применение нескольких биометрических модальностей, не только повышает надёжность распознавания, но и усложняет реализацию спуфинг атаки.

* * *

В настоящий момент исследования, направленные на решение данных проблем, активно продолжаются. Организаторы международного конкурса Automatic Speaker Verification Spoofing and Countermeasures Challenge начали подготовку к следующему этапу и планируют провести его в 2019 году.

ЛИТЕРАТУРА

1. Wu Z., Kinnunen T., Evans N., Yamagishi J., Hanilci C., Sahidullah M., Sizov A., «ASVspoof 2015: the First Automatic Speaker Verification Spoofing and Countermeasures Challenge», Interspeech 2015, http://www.asvspoof.org/is2015_asvspoof.pdf
2. Novoselov S., Kozlov A., Lavrentyeva G., Simonchik K., Shchemelinin V.: Stc anti-spoofing systems for the asvspoof 2015 challenge. 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2016)
3. Galina Lavrentyeva, Novoselov S., Malykh E., Kozlov A., Kudashev O., Shchemelinin V., «Audio replay attack detection with deep learning frameworks», Interspeech 2017, http://www.isca-speech.org/archive/Interspeech_2017/pdfs/0360.PDF
4. Kinnunen T., Sahidullah M., Delgado H., Todisco M., Evans N., Yamagishi J., Lee K., «The ASVspoof 2017 Challenge: Assessing the Limits of Replay Spoofing Attack Detection», Interspeech 2017, http://www.asvspoof.org/asvspoof2017overview_cameraReady.pdf
5. Wang X., Xiao Y., Zhu X., «Feature selection based on CQCCs for automatic speaker verification spoofing», Interspeech 2017 http://www.isca-speech.org/archive/Interspeech_2017/pdfs/0304.PDF
6. Nagarsheth P., Khoury E., Patil K., Garland M., «Replay Attack Detection using DNN for Channel Discrimination» Interspeech 2017, http://www.isca-speech.org/archive/Interspeech_2017/pdfs/1377.PDF

СТИМУЛ В ДЕЙСТВИИ

ПЛАТЕЖИ ПОД ЗАЩИТОЙ ПОЛОЖЕНИЯ БАНКА РОССИИ №382-П



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

Как мы знаем, банковская отрасль России является одной из наиболее продвинутых в части регламентации со стороны регуляторов в вопросах обеспечения информационной безопасности. Уже начиная с 2006 года активно развивается комплекс документов Банка России по обеспечению информационной безопасности, а с 2015 года стал функционировать центр реагирования на инциденты FinCERT.

Положение Банка России от 9 июня 2012 года № 382-П устанавливает требования к защите информации при осуществлении переводов денежных средств. Этот документ существует с 2012 года и его требования неоднократно актуализировались и пересматривались для соответствия с текущими реалиями. Положение предполагает, в том числе, проведение регулярной оценки соответствия участника платежной системы определенным требованиям. Компания «ДиалогНаука» проводит аудит в соответствии с этим Положением достаточно давно — за прошедшие 5 лет компания провела более 50 аудитов, поэтому нам хотелось бы поделиться полученными результатами этих работ.

ПРОБЛЕМА КАДРОВ

Основной проблемой, приводящей к недостаточно высокому уровню соответствия организации требованиям Положения 382-П, по нашему опыту, является недостаточность кадровых ресурсов, необходимых для выполнения всех задач в области информационной безопасности (ИБ). Так, например, в 25% случаев в кредитной организации (именно кредитные организации

являются основным заказчиком проведения внешней оценки соответствия) количество сотрудников, задействованных в реализации процессов обеспечения ИБ, не превышало трех специалистов, а чаще всего был просто один человек, ответственный за безопасность. Он занимался всем и решал все задачи, связанные с ИБ. В основном это была разработка документов, иногда согласование правил доступа, также на него была возложена проверка соответствия требованиям регулятора и учет носителей ключевой информации. При этом администрирование средств защиты информации в этом случае находилось в ведении ИТ-подразделений.

ДРУГИЕ ПРОБЛЕМЫ

Однако даже в случаях, когда сотрудников, отвечающих за информационную безопасность своей компании, было 10–15 человек, они не решали задач, связанных с глубокой интеграцией процессов обеспечения ИБ в банковские технологические процессы и задач, связанных с выявлением инцидентов — обрабатывались только простые инциденты, не затрагивающие технологические и бизнес-процессы организации.

Среди выявленных «ДиалогНаукой» несоответствий можно выделить следующие группы, которые оказывали непосредственное влияние при формировании оценки уровня соответствия:

I. Нереализованные (не формализованные) требования по обеспечению информационной безопасности в системах ДБО: в первую очередь это отсутствие внутренних документов, определяющих требования к таким системам, в том числе требования к регистрации событий безопасности. В половине проектов представители кредитной организации не смогли продемонстрировать журналы регистрации событий, содержащие всю необходимую в соответствии с требованиями Положения 382-П информацию.

II. Отсутствующие свидетельства вовлеченности ответственных за обеспечение информационной безопасности в процессы разработки/приобретения/модернизации автоматизированных банковских систем и компонент среды обработки защищаемой информации: в основном это отсутствие технических заданий (требований), содержащих формализованные требования по необходимым к реализации мерам защиты информации, а так-

**ОСНОВНОЙ ПРОБЛЕМОЙ,
ПО НАШЕМУ ОПЫТУ, ЯВЛЯЕТСЯ
НЕДОСТАТОЧНОСТЬ КАДРОВЫХ
РЕСУРСОВ, НЕОБХОДИМЫХ ДЛЯ
ВЫПОЛНЕНИЯ ВСЕХ ЗАДАЧ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

же отсутствие контроля реализованных мер защиты при вводе в эксплуатацию.

СТАТИСТИКА

Ниже приведена статистика по используемым средствам защиты, полученная по результатам проведенных аудитов:

- ♦ только 60% заказчиков используют продукты двух и более вендоров для организации антивирусной защиты. Самый популярный антивирус — это продукты «Лаборатории Касперского», но также встречаются ESET, Trend Micro и Sophos. У большинства заказчиков антивирус также выполняет задачи контроля периферийных устройств. Дополнительные системы контроля USB и периферийных устройств используются крайне редко;

- ♦ системы защиты от утечек информации (DLP) по факту используются редко, а если и используются, то не самым эффективным образом — мониторинг (не блокировка) по общим правилам, таким как отслеживание номеров карт или паспортных данных, в отдельных случаях — оцифровка типовых договоров. Полностью настроенных процессов практически не встречается. Используются в основном решения

трех производителей: InfoWatch, McAfee и Forcepoint (WebSense);

- ♦ межсетевые экраны — это в основном либо Cisco ASA, либо встроенные механизмы сетевого оборудования, хотя в последнее время все больше клиентов начинают применять специализированные межсетевые экраны;

- ♦ только 40% заказчиков используют сертифицированные средства криптографической защиты информации для защиты каналов связи;

- ♦ средства анализа защищенности, которые должны проверять наличие уязвимостей, используются у не более чем 60% заказчиков. По сканерам безопасности лидерами являются Nessus, Qualys, XSpider и MaxPatrol. В каждом пятом проекте сканирование безопасности было отдано на аутсорсинг;

- ♦ наконец, тесты на проникновение проводят менее половины заказчиков. При этом со следующей редакции 382-П проведение тестов на проникновение становится обязательным.

Другие средства защиты используются крайне редко. Единицы используют WAF (Web Application Firewall) и только в рамках выполнения требований PCI DSS.

В завершение хотелось бы обратить внимание на то, что в новой редакции Положения 382-П усиливаются требования в части контроля состояния информационной безопасности: предполагается формализация необходимости проведения ежегодных тестирований на проникновение, аудита кода приложений на уязвимость и оценки только в форме внешней оценки соответствия, выполняемой лицензиатами ФСТЭК России. Данный фактор дает возможность за счет привлечения сторонней специализированной компании-интегратора даже при небольшом количестве сотрудников в отделе информационной безопасности реализовать полный спектр требований Банка России. В целом, с нашей точки зрения, принятие Банком России Положения № 382-П позволило повысить внимание кредитных организаций к вопросам информационной безопасности и послужило стимулом в реализации мероприятий, направленных на повышение уровня защищенности как от внешних, так и внутренних угроз.





**Андрей
ДАВИДОВИЧ**
генеральный директор
ГК «Смарт-Софт»

В СТОРОНУ ЦЕНТРА

ПРОБЛЕМЫ СЕТЕВОЙ БЕЗОПАСНОСТИ В БАНКОВСКОМ СЕКТОРЕ

Сложная экономическая ситуация в стране заставила банки сокращать расходы. Сервера и рабочие места виртуализуются, переезжая в арендованные облака или частные датацентры, приложения и сервисы становятся централизованными, а техническая поддержка — дистанционной.

Важнейшим фактором бесперебойной работы банка становится защита сети, а одной из главных задач ИТ-службы — её организация и поддержание в актуальном состоянии.

По данным ФинЦЕРТ основными источниками угроз для банков в 2016–2017 году были атаки на отказ в обслуживании (DDoS), фишинговые рассылки с вредоносным ПО и атаки на банкоматы. Кроме того, серьёзный ущерб нанесли утечки данных, вызванные уязвимостями в ПО и действиями сотрудников.

DDOS-АТАКИ

Избежать полной остановки работы банка на время DDoS-атаки можно путём разделения внутренней сети банка и интернет-сегмента с помощью Traffic Inspector Enterprise или других фаерволлов. Это не защитит интернет-сервисы от атаки, но позволит работать с банковскими приложениями во внутренней сети.

При интенсивных DDoS-атаках поток паразитного трафика полностью забивает канал, и возможностей фаерволла или UTM-решения может оказаться недостаточно. Для защиты от таких атак существуют специализированные сервисы: CloudFlare, Akamai и другие.

ФИШИНГОВЫЕ РАССЫЛКИ

Централизация и виртуализация позволяют уменьшить ущерб от вредо-

носного ПО, которое распространяется с помощью фишинговых рассылок. И всё же, если пользователь виртуального рабочего места запустит вымогатель-шифровальщик, под угрозой окажутся не только его документы, но и все файлы на доступных ресурсах.

Оптимальным способом предотвратить попадание фишинговых писем с вредоносным содержимым в банковскую сеть является совместное использование антивируса на почтовом сервере и UTM-решения, например, Traffic Inspector Next Generation. Это обеспечит комплексную защиту в виде контроля доступа в интернет и блокировки вредоносного контента в письмах.

АТАКИ НА БАНКОМАТЫ

Наличие уязвимостей в операционных системах и софте банкоматов позволяет преступникам подключиться к устройству через интернет и установить ПО для джекпоттинга — удалённого управления выдачей денег. Если банкоматы недоступны из интернета, злоумышленники могут получить доступ к управлению, проникнув в сеть банка. После этого они могут в нужный момент дать команду на выдачу денег и забрать все наличные.

УТЕЧКИ ДАННЫХ

Утечка информации, содержащей конфиденциальные сведения, персональные данные или сведения, содержащие банковскую тайну — серьёзное нарушение и удар по репутации банка. Наиболее распространённые причины утечек — умышленные или неумышленные действия сотрудников и проникновение вредоносного ПО.

Использование UTM-решения может исключить утечки связанные, с вредоносным ПО, а также часть рисков, связанных с действиями сотрудников. Для полноценной борьбы с хищением данных требуется продуманное сочетание административных процедур и средств обеспечения безопасности, поскольку UTM-система не помешает сотруднику распечатать конфиденциальный документ и унести его домой.

Банковские ИТ-системы РФ развиваются в направлении централизации и виртуализации сервисов. Клиентов переводят на дистанционный банкинг, увеличивается количество систем самообслуживания. Работа банка становится невозможной без сетевых сервисов и каналов связи, поэтому важнейшими задачами становятся защита периметра от атак и контроль трафика между сегментами банковской сети.

Использование отдельных решений для антивирусной защиты, детектора вторжений и фаерволла становится неэффективным ввиду растущей сложности атак, использования многокомпонентного вредоносного ПО и изощрённых приёмов социальной инженерии.

Обеспечить комплексную защиту сети банка от проникновений, фишинговых атак и утечек данных позволяют UTM-системы, подобные Traffic Inspector Next Generation. Присутствие Traffic Inspector Next Generation в реестре российского ПО Минкомсвязи позволяет использовать его банкам, попавшим в санкционный список.

МИР

Платежная система



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

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

Удобный, выгодный и надежный инструмент для совершения платежных операций.

mironline.ru

КТО БРЕЕТ БРАДОБРЕЯ?

НАБЛЮДЕНИЯ ЗА ИСПОЛЬЗОВАНИЕМ СИСТЕМ КОНТРОЛЯ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ



Дмитрий МИХЕЕВ
технический директор
компании «АйТи
БАСТИОН»

Не так давно я поймал себя на том, что опять провожу вечер, пытаюсь разобраться в тексте федерального закона. Не то чтобы я никогда этого не делал, но я вдруг понял, что в последнее время для ответа на возникающие вопросы наших уважаемых клиентов приходится заниматься этим регулярно, и чем дальше, тем чаще и подробнее. Такое время, такие особенности окружающей действительности. Какие еще особенности обратили на себя внимание за те несколько лет, что мы внедряем Систему контроля действий поставщиков услуг?

ЧИСЛО УЧАСТНИКОВ РАСТЕТ

В прошедшем 2017 году можно было увидеть, что в проектах заметно выросло число участников: к пользователям, администраторам и администраторам безопасности стали прибавляться исполнители-сотрудники, внешние специалисты от интеграторов, партнеры по сервису, служб мониторинга... Теперь еще некоторым придется принимать у себя плановых или внеплановых проверяющих в связи с ФЗ-187 о критически важных элементах информационной инфраструктуры.

В самом деле, если еще год назад 10–15 участников было вполне стандартным числом для проекта, то сейчас — это скорее несколько десятков или даже сотен живых людей. С одной стороны, такое увеличение связано с вниманием регулирующих органов и законодательством последних лет. С другой, под контроль переходят крупные инфраструктурные узлы, целые датацентры. Ну, и, наверное, так как мы говорим о крупном бизнесе, — на данную тен-

денцию влияет также и обоснованное желание управлять рисками, не полагаясь на моральные качества персонала.

МЕСТНАЯ ОСОБЕННОСТЬ

Об этом примерно было упомянуто в отчете Gartner о РАМ системах 2016 года, но можно заметить местную культурную особенность. Западные коллеги говорят и пишут о массивных внедрениях РИМ систем в облачных сервисах (например, на основе сервиса Azure), тогда как у нас это обычно внедрения на собственном оборудовании, на самый крайний случай — частные облака на собственных или сильно обособленных ресурсах. Например, в защищенных дата-центрах от крупных игроков рынка ИТ и безопасности. Финансовых организаций это касается в первую очередь — очень немногие банки или страховые компании полагаются на внешние инфраструктуры в своей работе.

НОВЫЕ СИСТЕМЫ

Растущие объемы проектов не могут не радовать нас, как разработчиков системы, но надо понимать, что чем больше задач мы решаем, тем интереснее жить. Опять же, локальные культурные особенности добавляют радости каждый день, куда ж без них. Если раньше для систем виртуализации было два основных кандидата в виде VmWare и Hyper-V,

то сейчас все больше крупных клиентов запускают виртуальные инфраструктуры на различных локализованных решениях, работающих на основе систем виртуализации KVM и других подобных. Это относится и к работе на этих платформах, и к управлению доступом к ним в целях контроля действий администраторов. В основном речь идет об окологосударственных компаниях, но и в банках мы наблюдаем эту тенденцию.

Похожая история с системами SIEM и другими — некоторые привычные и, казалось бы, вечные торговые марки пропадают из технических документов, заменяясь вдруг совсем новыми и незнакомыми, что требует определенных усилий по знакомству и интеграции с ними.

ДВОЙНОЙ-ТРОЙНОЙ-ВСТРЕЧНЫЙ КОНТРОЛЬ

Растущее внимание к задачам защиты ключевых систем ИТ и ИБ приводит к тому, что за одними и теми же администраторами идет контроль с нескольких решений, как шлюзовых, так и агентских, на уровне входа в ОС, на уровне DLP систем... Легкость внедрения и скорость работы иногда от таких эшелонированных защит, конечно, страдает.

К сожалению, надо быть готовыми к таким проблемам, теперь они тоже никуда от нас не уйдут.

**ЕСЛИ ЕЩЕ ГОД НАЗАД 10–15 УЧАСТНИКОВ
БЫЛО ВПОЛНЕ СТАНДАРТНЫМ
ЧИСЛОМ ДЛЯ ПРОЕКТА, ТО СЕЙЧАС —
ЭТО СКОРЕЕ НЕСКОЛЬКО ДЕСЯТКОВ
ИЛИ ДАЖЕ СОТЕН ЖИВЫХ ЛЮДЕЙ**

Пару лет назад, на одном из проектов мы обнаружили, что сервисная компания и ее крупный заказчик внедрила каждый свою систему контроля действий администраторов и используют их для организации доступа сервисных инженеров к инфраструктуре, а также для того, чтобы со стороны сервисной компании контролировать реальную работу исполнителей и показатели SLA. Подобный встречный контроль позволил этим уважаемым компаниям также успешно разбирать рабочие конфликты по качеству обслуживания, что не может не радовать. Но, честно говоря, рассказывая потом на презентациях о данной ситуации, я до некоторой степени воспринимал ее как некоторый выброс, может, даже пример чрезмерного контроля и управления. Но в настоящее время с подобным запросом компании приходят на первые установочные встречи по задачам, связанным с управлением рисками внешнего доступа. И это уже видится как стандартное решение.

ТОТАЛЬНАЯ АВТОМАТИЗАЦИЯ

Еще один признак, по которому этот год отличается от предыдущих, — это желание повсеместной автоматизации. Пожелания типа «а вот хочется, чтобы само, по заявке из сервис-деска, на «три зеленых свистка» все стало хорошо» были всегда, сколько существуют ИТ системы и системы безопасности. Но раньше было достаточно уверенно ответить: да, можно, есть программный интерфейс и т.д. В этом году мы сделали для нескольких проектов в банковских организациях специальные доработки в процессе развертывания — чтобы процесс управления правами доступа администраторов был провязан через IdM систему и систему заявок, чтобы входы на виртуальные машины сразу после создания вставали под контроль действий уже по команде от ПО оркестратора виртуальной фермы. По сути, можно сказать, что контроль действий администраторов занимает уже вполне уверенную позицию как один из стандартных механизмов обеспечения безопасности и управляемости ИТ-инфраструктуры.

СКОРОСТЬ ПРИНЯТИЯ ЗАКОНОВ ТАКОВА, ЧТО ПРАКТИКА ИХ ПРИМЕНЕНИЯ НЕ УСПЕВАЕТ СКЛАДЫВАТЬСЯ И ЭТИ ПРАКТИКИ ПРИХОДИТСЯ ВЫРАБАТЫВАТЬ В РАБОЧЕМ ПОРЯДКЕ

НОВЫЕ ЗАКОНЫ

Разговор об ИТ безопасности сегодня не может обойти вопросы ответственности, в том числе о соответствии требованиям регулирующих органов. Кроме уже действующего приказа 135 от 04.04.2016 Минкомсвязи, законов по защите ПдН, средств АСУТП и других законов по данной теме, в ближайшее время вступят в силу закон и подзаконные акты о КИИ — критической информационной инфраструктуре (187-ФЗ). Практически каждый из этих законов подразумевает требования о контроле доступа к системам ИТ, фиксации действий, выполняемых на элементах инфраструктуры, регистрации событий, связанных прямо или косвенно с деятельностью привилегированных пользователей и администраторов. Все эти требования законодательно закрепляют право контролирующих органов на доступ к данной информации. Владельцам объектов инфраструктуры вменяется в обязанность оперативное уведомление контролирующих организаций о тех или иных событиях.

Согласно новому закону критерии отнесения систем к критически важным сформулированы достаточно открыто — социальная значимость, предоставление значительного объема информационных услуг, а банки и финансовая сфера в целом — явно обозначены как сфера применения данного закона и сопровождающих его подзаконных актов. Учитывая потенциальные риски уголовного преследования за ненадлежащую эксплуатацию КИИ, обойти данные законодательные новшества вниманием не получится.

ПРАКТИКА НЕ ПОСПЕВАЕТ ЗА ЗАКОНОТВОРЧЕСТВОМ

За предыдущие годы мы реализовали несколько проектов, связанных с обеспечением доступа специалистов кон-

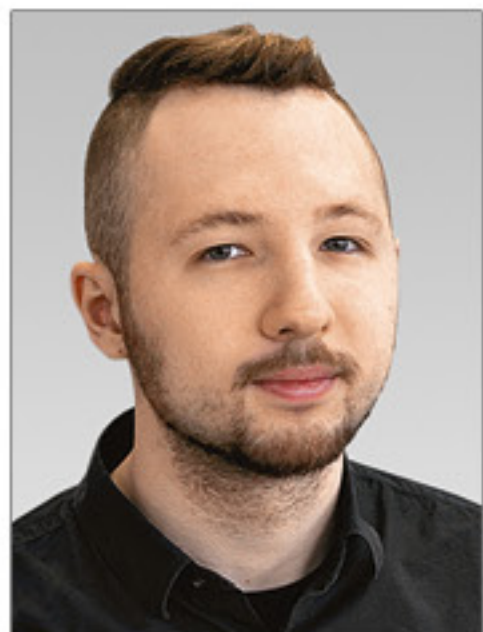
тролирующих органов к отчетным данным, обеспечивая, по возможности, данный процесс с точки зрения предоставления доступа, фиксирования фактов обращения и передаваемых данных. Конечно, в настоящий момент не до конца понятны критерии и практика отнесения тех или иных элементов информационной инфраструктуры к критическим, но даже те документы, которые уже доступны для изучения, показывают, что под данную категорию легко могут попасть большинство банков, хотя бы по объему оказываемых информационных услуг и использованию сетей электросвязи.

За несколько лет подобного рода законодательные практики проходили стандартный путь от проектов законов до явных требований законодательства с ответственностью за невыполнение. Скорость принятия этих законов такова, что практика их применения не успевает складываться и эти практики приходится вырабатывать в рабочем порядке. Для обеспечения данных законодательных инициатив в настоящее время реализуются крупные проекты в самых разных областях, но при этом можно перефразировать старую шутку: «Кто бреет браздобрея? Сертифицированный браздобрей!»

А кто же бреет сертифицированного браздобрея? Данный вопрос пока в разработке.

* * *

Развивающаяся практика применения, по опыту предыдущих лет показывает тенденцию к ужесточению требований и ответственности за невыполнение требований. Таким образом, в ближайшее время данный сценарий использования может оказаться популярным и востребованным, как никогда.



Павел ГОЛОВИСТИКОВ
инженер Департамента
информационной безопасности
АМТ-ГРУП

VULNERABILITY MANAGEMENT

БОРЕМСЯ С УЯЗВИМОСТЯМИ СИЛАМИ КОМАНДЫ SOC

Каждая организация хочет защитить свои информационные ресурсы и делает это согласно собственной политике безопасности. Типовая служба ИБ имеет свое видение того, какими организационно-правовыми мерами и техническими средствами она будет оберегать информационное пространство, вверенное под ее надзор. Для достижения этой цели выстраивается множество сложенных и взаимосвязанных процессов. Об одном из них и пойдет речь, а именно, об управлении уязвимостями. Я расскажу о значимых аспектах процесса Vulnerability Management, информация о которых накоплена нами за время работы с заказчиками при оказании услуги SOC.

МИНИМИЗИРОВАТЬ ВРЕМЯ СКАНИРОВАНИЯ

Первое, что хотелось бы отметить, — крайне важно минимизировать время сканирования уязвимостей без ущерба для полноты исследования. Достигается это различными методами. На

мой взгляд, проводить поиск брешей следует лишь после предварительной качественной инвентаризации инфраструктуры, которая, помимо данных от применяемого программного продукта, должна содержать дополнительную информацию от служб ИТ. Необходимо доходчиво донести до потребителей услуг, насколько запрашиваемые сведения об инфраструктуре ускоряют процесс исследований, и что мы не требуем от них избыточных конфиденциальных данных. Искомая информация может быть получена инструментальным путем, однако временные рамки сканирования лишь увеличатся, как и, соответственно, риски для заказчика.

НАРУШЕНИЯ СЕТЕВОЙ ТОПОЛОГИИ

Также внимания заслуживает то, что во время проведения сканирования можно, помимо уязвимостей хостов, найти неизвестные для служб ИТ нарушения сетевой топологии. Например, один из наших заказчиков обеспокоился чрезмерным трафиком от сканера уязвимостей. В ходе исследования

проблемы мы выяснили, что сетевые инженеры ошибочно создали петлю маршрутизации в собственной сети. Схожая ситуация произошла в другой организации. Представители заказчика были встревожены тем, что трафик сканера был замечен в сети, не исследуемой в рамках договора. Совместно с ИТ-службой заказчика мы установили, что одно из сетевых устройств перенаправляло трафик в дополнительную сеть из-за ошибки в ACL, которая могла негативно сказаться на защищенности инфраструктуры в целом.

ПРОБЛЕМЫ ОТЧЕТНОСТИ

После завершения процедуры сканирования наступает этап создания отчетной документации. Необходимо понимать, что для предоставления качественного сервиса одной лишь необработанной выгрузкой сканера нельзя обойтись. Помимо того, что стандартные шаблоны отчетов производителя сканера уязвимостей могут не устраивать ИТ/ИБ службы ввиду недостаточной информативности, существуют и более важные проблемы отчетности в рамках Vulnerability Management.

Во-первых, выгрузки могут содержать неверные или устаревшие патчи, ссылки на уже не существующие или неактуальные статьи по устранению уязвимостей. Да, процент ошибок невелик, однако никто не может

ПРОВОДИТЬ ПОИСК БРЕШЕЙ СЛЕДУЕТ ЛИШЬ ПОСЛЕ ПРЕДВАРИТЕЛЬНОЙ КАЧЕСТВЕННОЙ ИНВЕНТАРИЗАЦИИ ИНФРАСТРУКТУРЫ

гарантировать, что они не произойдут в той самой уязвимости, которая будет проэксплуатирована злоумышленником. Поэтому необходима тщательная проверка результатов работы сканера. Это, по сути, задача борьбы с False Positive.

Во-вторых, необходимо обозначить приоритет устранения уязвимостей. Этот параметр играет немаловажную роль в информационной безопасности организации. Даже если мы будем руководствоваться CVSS-метрикой (популярный принцип классификации критичности, который, в частности, применяется в PCI DSS), может возникнуть ситуация, при которой ИТ-службам придется обрабатывать слишком большое число запросов, имеющих равный вес согласно CVSS, однако разный для заказчика. Это, в свою очередь, может привести к тому, что не будут своевременно закрыты определенные бреши.

Несложно устранить несколько уязвимостей в кратчайший срок. Однако, что же делать, если их не одна, не две, а тысячи, десятки тысяч? Процесс закрытия найденных брешей может занять продолжительное время. Безусловно, все мы понимаем очевидную зависимость: чем меньше время реагирования на наиболее вероятные угрозы, тем меньше риски для организации. Поэтому необходима дополнительная классификация обнаруженных уязвимостей по уровню значимости для компании-заказчика. Для этого нужно численно оценить критичность активов, вероятность эксплуатации бреши с учетом применяемых средств ИБ, топологии, отключенных служб, наличия в открытом доступе реализованного эксплойта и прочих параметров.

В-третьих, рекомендации, генерируемые сканерами, в ряде случаев неприменимы из-за особенностей инфраструктуры заказчика. Также в бюллетене производителя ПО может не быть патча или workaround'a. Тогда возникает вопрос о выработке другого решения для закрытия уязвимости или минимизации риска ее эксплуатации.

Все упомянутые выше факторы приводят к тому, что выгрузка сканера уязвимостей подвергается тщательному

анализу со стороны исполнителя работ. Делать это исключительно вручную не представляется возможным. Процесс требует слишком больших трудозатрат. Поэтому качественный и, в тоже время, своевременный отчет с хорошей визуализацией ИБ-процессов требует авторской автоматизированной обработки помимо той, что предоставляют разработчики средств детектирования уязвимостей.

СОГЛАСОВАНИЕ ОТЧЕТНОЙ ДОКУМЕНТАЦИИ

Далее наступает следующий этап взаимодействия заказчика и исполнителя — согласование предоставленной отчетной документации. Необходимо ответить заказчику на все интересующие его вопросы. К примеру, как же вышло, что в инфраструктуре так много уязвимостей (в том числе и далеко не свежих), несмотря на якобы регулярные обновления. В итоге выясняется, что часть их не была применена или рекомендации бюллетеней выполнены не полностью. Помимо установки указанных в них патчей, иногда требуются и иные мероприятия, которые необходимо выполнить, чтобы закрыть брешь (например, изменить в реестре некоторую запись). Нередко сотрудники забывают и про то, что при прекращении поддержки производителем программного обеспечения необходимо в срочном порядке осуществлять переход на актуальные версии ПО, искать аналогичные продукты. Дальнейшая его эксплуатация является серьезной угрозой информационной безопасности.

ПОИСК УЯЗВИМОСТЕЙ — НЕ РАЗОВАЯ ПРОЦЕДУРА

К сожалению, до сих пор существует мнение, что поиск уязвимостей — разовая процедура. Провели мероприятия по сканированию, получили отчеты и рекомендации, дали задание сотрудникам ИТ служб и успокоились на год-другой. Данный подход в корне неверный, о чем говорят большинство общепринятых стандартов ИБ в разных областях: от PCI DSS, NIST до требований российских регуляторов. Управление уязвимостями — весомая часть политики безопасности, которая долж-

на быть глубоко проработана с целью достичь:

- ♦ установленной периодичности, зависящей в том числе от критичности сегмента;
- ♦ регулярной инвентаризации активов, оценки их критичности;
- ♦ постоянного совершенствования методов в целом;
- ♦ качественного мониторинга и устранения брешей.

ПРО SOC

На последнем пункте хотел бы остановиться чуть подробнее. При повторных сканированиях инфраструктуры замечаешь, что остается довольно много невыполненных рекомендаций, незакрытых уязвимостей. Далеко не всегда речь идет о халатности сотрудников. Управление уязвимостями — процесс борьбы с хаосом, которым сложно управлять своими силами. Нужна централизованная платформа, предоставляющая разносторонний взгляд на то, как протекает выполнение поставленных задач по закрытию брешей или иных связанных мероприятий. На мой взгляд, один из выходов для тех, у кого нет достаточных ресурсов, — услуга коммерческого сервиса Security Operations Center (SOC). Сервис SOC как нельзя лучше решает данную задачу, так как это одна из главных его функций (помимо мониторинга и расследований инцидентов).

* * *

Мониторинг ИБ и управление уязвимостями — понятия, безусловно, разные, однако взаимосвязанные, так как последнее является одним из важнейших поставщиков событий для процессов мониторинга. Результаты инструментальных исследований инфраструктуры на наличие брешей можно, к примеру, использовать для более тонкой и точной настройки SIEM'a. На рынке уже можно встретить решения, которые объединяют в себе SIEM и сканер уязвимостей. Полагаю, что тенденция к объединению подобных продуктов сохранится. Большинство из громких угроз современности обнаруживается связкой Vulnerability Management и мониторингом SOC.

ANTI-APT: МУКИ ВЫБОРА

Тенденцией последнего десятилетия стал рост количества направленных атак, которые разрабатываются с учетом уникального ИТ-ландшафта и организационной структуры компании-жертвы. Такие атаки сложно выявить: среднее время обнаружения успешного взлома — полгода, а многие жертвы не знают о том, что их системы скомпрометированы, многие годы. Зачастую компании узнают о компрометации лишь из внешних источников (СМИ, контрагентов и т.д.). Целью могут быть как денежные средства, так и информационные активы, которые можно продать на черном рынке, — персональные данные, коммерческая информация и т.д. Кроме того, ни одна организация не застрахована от попыток вымогательства, например, посредством криптолокера, блокирующего работу важного приложения.

В ответ на существующие угрозы целевых атак на рынке несколько лет назад появились Anti-APT решения, обеспечивающие раннее выявление аномальных активностей в инфраструктуре. Если в предыдущие годы многие компании «присматривались» к решениям данного класса, то в 2016–2017 годах рынок пришел к пониманию того, что Anti-APT является неотъемлемым компонентом системы информационной безопасности. И здесь важно рассматривать средства защиты от целевых атак не как решения «из коробки». Их внедрение — это комплексный проект по информационной безопасности. Без тонкой настройки под конкретные цели и задачи, интеграции с существующими средствами защиты в инфраструктуре и обучения персона-

ла, инвестиции в решения по защите от направленных атак можно считать выброшенными на ветер.

Внедрения решений класса Anti-APT мы относим к проектам средней и высокой сложности. В список внедряемых продуктов могут входить и средства для мониторинга сетевого трафика, и решения для динамического анализа файлов, и системы для защиты рабочих станций. Обычно проект выполняется поэтапно. Например, сначала защищают почту как основной источник угроз. Далее уже переходят к анализу веб-трафика и внутренних активностей, защите рабочих станций.

По нашему опыту, сегодня заказчики очень щепетильно подходят к выбору Anti-APT решений. И не приобретают их, пока не протестируют на своей инфраструктуре, в условиях, максимально приближенных к боевым. Это позволяет говорить о том, что если компания выбирает для себя решение того или иного производителя, то делает это абсолютно обоснованно и со знанием дела. Поэтому почти любому проекту предшествует пилот или серия пилотов. Причем, для правильного выбора решений под конкретные задачи заказчик тестирует сразу несколько решений. На пилотах стараются максимально приблизиться к продуктивному внедрению. Чем качественнее проработан пилот, тем проще внедрение.

В 2016 году мы инвестировали в направление Anti-APT и активно наращивали экспертизу работы с различными продуктами. Мы сформировали критерии «отбора» на основании часто задаваемых вопросов наших заказчиков и сделали большой обзор по Anti-APT, включающий более 30 пара-



Александр РУСЕЦКИЙ
руководитель направления защиты
от направленных атак компании
«Инфосистемы Джет»

метров, своими силами провели многочисленные тестирования на реальном трафике. В конце 2017 года мы выпустили обновленную версию нашего обзора по Anti-APT решениям: добавили новые «фишки», появившиеся в продуктах вендоров, увеличили число рассматриваемых решений, расширили набор параметров, по которым сравниваем продукты.

ANTI-APT ПОЛИГОН НА УРАЛЬСКОМ ФОРУМЕ

Более подробно об Anti-APT решениях мы расскажем на мастер-классе компании «Инфосистемы Джет» ANTI-APT ПОЛИГОН в рамках Уральского форума. Эксперты компании на практике продемонстрируют работу продуктов различных вендоров сразу по нескольким сценариям: анализ почтового трафика, обнаружение web-угроз, защита от загрузки вредоносных flash-носителей. Главная цель мастер-класса — оценить возможности каждого из продуктов и выбрать оптимальное Anti-APT решение для защиты своей компании. В ANTI-APT ПОЛИГОН подтвердили свое участие вендоры: Check Point, Fortinet, «Лаборатория Касперского». Каждого участника мастер-класса ждет бонус — свежий обзор-сравнение по Anti-APT решениям!

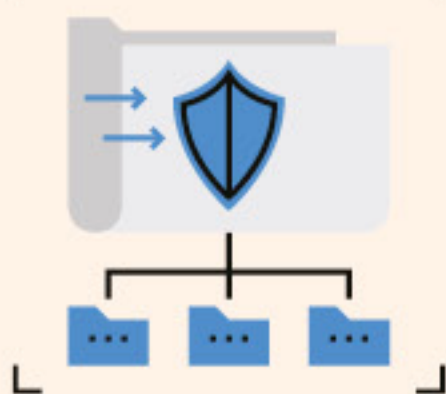
ANTI-APT ПОЛИГОН пройдет 14 февраля с 16:30 до 18:00 в Малом зале в рамках Уральского форума. Приходите для проверки Anti-APT решений в боевых условиях и приносите свои вредоносы для тестирования! До встречи!

**ЗАЩИТА ПОЧТЫ**

На сегодняшний день почта остается основным вектором распространения направленных атак. Мы рекомендуем использовать режим блокировки, так как он препятствует первичному заражению. Практика показывает, что задержка в получении почты на время проверки составляет от трех до пяти минут, что не критично для пользователей.

**ЗАЩИТА WEB-ТРАФИКА**

С точки зрения анализа web-трафика мы рекомендуем использовать режим мониторинга, позволяющий обходиться без задержек в обмене трафиком и исключить воздействие на бизнес-процессы организации. Одновременно решение не видно злоумышленникам, при этом позволяет обнаруживать угрозы на самых ранних стадиях. Блокировку целесообразно осуществлять на уровне рабочих станций, когда скачиваемые файлы перехватываются и проверяются в «песочнице» до их открытия и запуска, или на уровне сетевого оборудования после вынесения соответствующего вердикта для передачи фидов и создания правил блокировки. Наш опыт показал, что использование Anti-APT решения для анализа только HTTP-трафика нецелесообразно. Необходимо расшифровка SSL-трафика и анализ его на скрытые угрозы, ведь его доля составляет уже более 50% в общем объеме трафика.

**ЗАЩИТА ФАЙЛОВЫХ ХРАНИЛИЩ**

Наряду с защитой почты и мониторингом сетевой активности необходимо проверять файловые хранилища на наличие угроз. Самый простой пример того, как могут воспользоваться незащищенностью файловых ресурсов злоумышленники: контрагенты заказчика подгружают документы на ресурсы компании. Атака идет на контрагента, имеющего недостаточный уровень защиты, а затем уже компрометируется инфраструктура жертвы. Для защиты файловых хранилищ мы рекомендуем нашим заказчикам использовать возможности Anti-APT решений: сканирование загружаемых файлов по расписанию и отправку подозрительных файлов в карантин (удалять их без разбора — не лучшее решение).

**ЗАЩИТА РАБОЧИХ СТАНЦИЙ**

Мы рекомендуем внимательнее относиться к защите рабочих станций. В линейке Anti-APT решения есть агентское ПО для противодействия угрозам «нулевого дня» двух типов: «легкие агенты», совместимые с текущим антивирусом заказчика, и полноценные AV-агенты. В последнее время все большую популярность набирают EDR (Endpoint Detection and Response) агенты, которые позволяют выявлять, изолировать и устранять сложные устойчивые угрозы на уровне рабочих станций. Данный класс решений оперативно выявляет отклонения в поведении приложений и объектов с возможностью быстрого восстановления в случае подтверждения инцидента офицером безопасности, а также предлагает расширенные возможности по расследованию атаки.

**ИНТЕГРАЦИЯ С СУЩЕСТВУЮЩИМИ СРЕДСТВАМИ ЗАЩИТЫ**

Внедрение Anti-APT решения подразумевает также интеграцию с текущими средствами защиты компании. Например, с сетевыми системами (прокси, межсетевые экраны, IDS/IPS), с WAF, с SIEM в качестве важных источников данных. Поддержка API позволит реализовать собственный сервис автоматизированной проверки объектов в решениях данного класса с получением обратной связи.

SHADOW IT. ВСЕМ ВЫЙТИ ИЗ ТЕНИ!



Андрей АКИНИН
генеральный директор
компании Web Control

В современной России развитие сегмента облачных технологий опережает общемировой уровень. Согласно отчету IDC, в 2018 году рост облачных технологий ожидается на уровне 11,8%.

Облака все больше привлекают внимание и частных предпринимателей, и крупных холдингов, при этом информационная безопасность и контроль за потоками данных становятся все более актуальными.

Что же конкретно сулит движение бизнеса в «облака» и что с этим делать ИБ-специалистам, рассказал генеральный директор компании Web Control Андрей Акинин.

— Облачные сервисы сегодня: что они собой представляют и какие из них набирают наибольшую популярность?

— Сегодня мы используем облака, даже не замечая этого. Почтовые службы, CRM-системы, офисные приложения все больше внедряют облачные технологии. Сотрудники компаний используют десятки, а то и сотни облачных сервисов. И это естественно. Облачные сервисы — это удобно, они позволяют компаниям избавиться от жесткости физической ИТ-инфраструктуры и привести её в соответствие с изменившимися бизнес-потребностями.

Однако, как это ни парадоксально, сегодня мало кто в полной мере осознает, что такое облачные сервисы. В основном ими считают довольно узкую группу сервисов, объединяющих Google, Amazon, Яндекс и т.п. На самом деле, даже заходя на обычные банковские сайты, можно найти множество скриптов, таких как SDM (Service Data

Management), RuTarget, Google Analytics, Google tag manager и прочих, — а это тоже облака. Соответственно, заходя на многие современные сайты, мы автоматически становимся пользователями облаков и наши данные начинают перемещаться в облака, и гипотетически это является потенциальной угрозой. Современные социальные сети — тоже по сути облачные сервисы, и часто они становятся рабочим инструментом бизнеса. При этом возрастает роль облачных бизнес-систем — CRM, конференций, инструментов совместной работы.

Все они могут стать каналами, и не только утечки информации, но и проникновения вредоносного ПО или целенаправленной атаки.

Важно, что сотрудники компаний используют облака вне зависимости от того, разрешено это корпоративной политикой или нет, и далеко не всегда это вредно для бизнеса!

— В какой момент облачные сервисы становятся проблемой для бизнеса и как избежать этого?

— Если социальными сетями достаточно легко управлять, поскольку они на виду, то облачные бизнес-системы могут представлять значительную угрозу. Например, так называемые Shadow IT, то есть сторонние ИТ-решения, неподконтрольные корпоративному управлению. И это не всегда облака,

это могут быть любые информационные системы, находящиеся вне зоны видимости или контроля.

Информационная безопасность, к счастью, имеет достаточно инструментов для выявления облачной активности. Нужно только уметь ими пользоваться. Гораздо легче это делать не запрещая и блокируя, а регулируя и наблюдая за использованием. Чем жестче борьба, тем быстрее она уйдет в тень, где ее трудно контролировать.

Инфраструктура Shadow IT не всегда зло, часто она возникает из «добрых» побуждений, для оптимизации легитимных бизнес-процессов. Поэтому ее нужно выявлять и анализировать, и только при необходимости предложить альтернативу. Это даст возможность сделать облачную среду контролируемой, удобной и безопасной.

Изначально нужно иметь гибкий подход к облакам. С одной стороны, есть разные сервисы, платформы и инфраструктуры; с другой, все они делятся на глобальные/локальные, безопасные/небезопасные, надежные и не очень, и всегда можно найти оптимальный вариант. Необходимо выявлять потенциально небезопасные или ненадежные сервисы, и искать им надежную и безопасную альтернативу.

— Как возведение периметра отражается на взаимоотношениях меж-

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ,
К СЧАСТЬЮ, ИМЕЕТ ДОСТАТОЧНО
ИНСТРУМЕНТОВ ДЛЯ ВЫЯВЛЕНИЯ
ОБЛАЧНОЙ АКТИВНОСТИ. НУЖНО
ТОЛЬКО УМЕТЬ ИМИ ПОЛЬЗОВАТЬСЯ**

ду бизнес-подразделениями, ИБ и ИТ-структурами?

— Те, кто пытаются сохранить четкий периметр безопасности вокруг корпоративной сети и отстаивают жесткую политику ограничений, по сути возбуждают неприятие среди сотрудников компании. Сегодня добиться гибкости бизнес-процессов и оптимизации затрат можно только при полном взаимодействии ИБ-служб, бизнес-подразделений и пользователей.

Представители ИБ должны осознать, что их задача — обеспечить безопасную деятельность пользователей, выявляя потенциальные аномалии в ИТ-структуре компании, сглаживая и выравнивая их.

Одно из наиболее эффективных решений, способных помочь наладить систему контроля за облачными сервисами, — Cloud Access Security Broker (CASB), о котором, мы и будем говорить на «облачной» сессии X Уральского форума.

CASB-решения в данном контексте делают облачные сервисы контролируемыми и безопасными, поскольку могут быть интегрированы с различными компонентами контроля облачных сервисов.

— Как компания Web Control пришла к идее продвижения решений от Symantec? В чем их отличие от других технологий, представленных на российском рынке?

— За нас выбор сделал рынок. Являясь дистрибьютором Blue Coat Systems, мы активно продвигали идею обеспечения безопасного поведения пользователей в Интернет, однако эти решения обеспечивали в основном сетевую безопасность. Слияние Blue Coat с Symantec дало нам возможность значительно расширить наши возможности реализации этой идеи.

Symantec — один из мировых лидеров в области производства систем ИБ для всего спектра информационных систем от ПК до глобальных облачных сервисов. На мой взгляд, преимущество Symantec заключается в том, что развитие его продуктовой линейки идет от endpoint («пользовательский компьютер»). Периметр безопасности современных ИТ систем сужается до границ endpoint и его защищенность

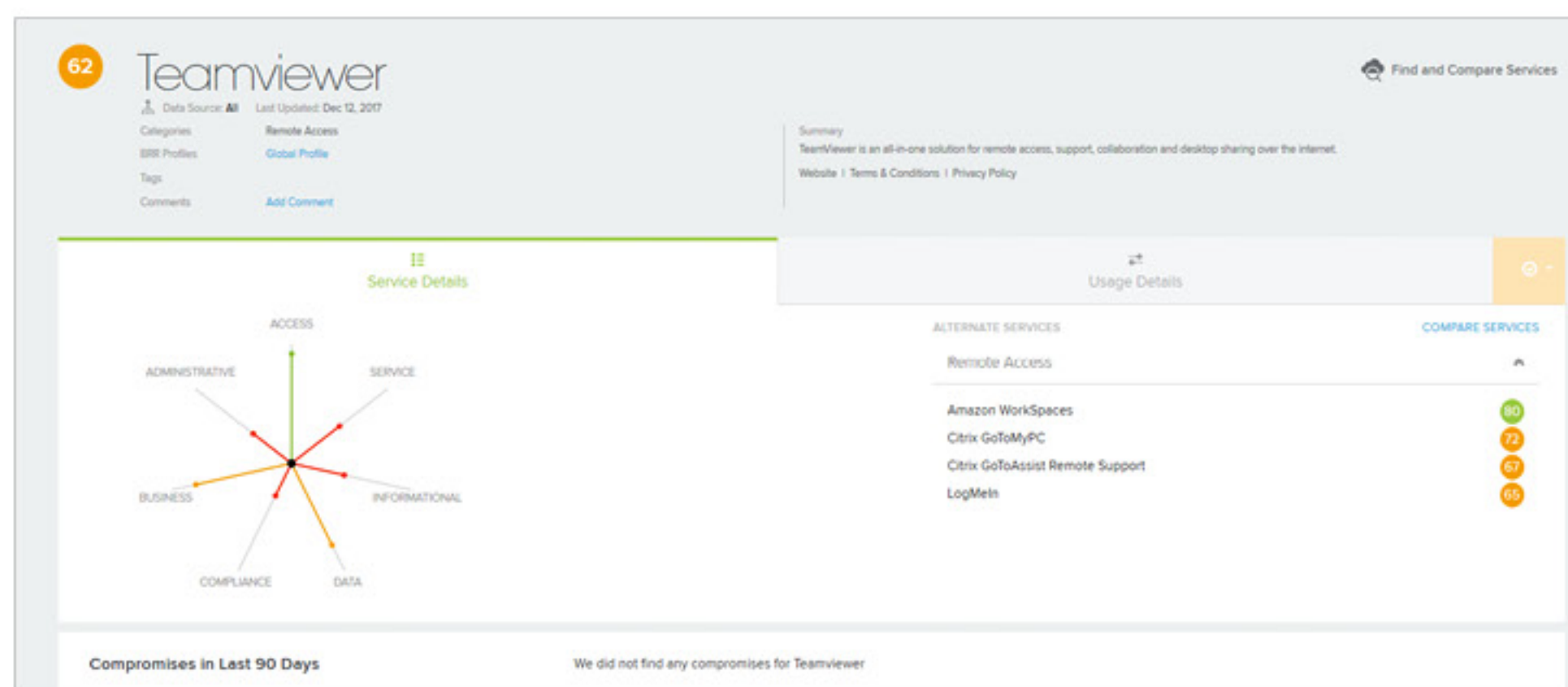


Диаграмма оценки рисков по категориям и технологии ИБ реализованные сервисом

становится фундаментом всей безопасности компании.

Мы традиционно занимаемся вопросами внутренней безопасности корпоративных сетей, то есть вопросами обеспечения правильного/безопасного поведения сотрудников внутри инфраструктуры компании. Как показывает наша практика, а мы работаем в этой сфере более 10 лет, значительная часть проблем сосредоточена внутри периметра, который сейчас все больше сужается до границ endpoint. Поэтому Symantec и получил то естественное преимущество, которое делает его лидером — управление контентом внутри периметра и его полный контроль.

— Как выбрать облачного провайдера и на какие параметры необходимо обращать внимание?

— Мировой рынок все больше уходит от исключительно облачных услуг (SAAS) к все более востребованной корпоративным заказчиком инфраструктуре как сервису (IAAS). Сейчас эти решения активно предлагает Ростелеком, Microsoft Azure, Google и другие компании. При этом возникает вопрос: как обеспечить в них целостность, безопасность и, что самое важное, понимать, что происходит внутри?

Бизнес всегда принимает решения, исходя из коммерческой целесообразности, и старается обойти неудобные для себя решения. Соответственно ИБ- и ИТ-службы должны делать жизнь бизнеса безопасной и эффективной. Для этого, выбирая какие-либо облачные технологии, важно обратить внимание на такие критерии: контроль привилегированного досту-

па (как внешнего, так и внутреннего), надежность и управляемость сервиса, а также информативность отчетности о его использовании. В рамках облачной сессии Уральского форума мы попробуем все вместе более детально ответить на вопрос, на что обращать внимание при выборе облачного провайдера.

— Что дает мониторинг Shadow IT и какие перспективы открывает для будущего?

— Прежде всего, он позволяет увидеть реальную картину использования облачных технологий внутри компании. Облачные сервисы нужно учиться контролировать, а не запрещать, ведь отказаться от них — значит потерять свои конкурентные преимущества в бизнесе. Чем жестче ограничения по безопасности, тем больше вероятность, что их будут обходить. Мониторинг использования облачных сервисов позволит вывести Shadow IT из тени и превратить облачные технологии из угрозы в преимущество бизнеса.

Необходимо формировать безопасную траекторию поведения при использовании сети, что позволит эффективно и безопасно его использовать. Служба ИБ должна заботиться не о том, как запретить что-то, а о том, как сделать это безопасным и удобным для бизнеса. Это сложная задача, требующая понимания всех бизнес-процессов.

Вообще, хватит пугать бизнес, это контрпродуктивно! Давайте искать, как ему помочь, в том числе, выявляя Shadow IT и унифицируя подходы безопасного использования облаков.

Беседовала Анна Воробьева



Владимир ИВАНОВ
директор по развитию
компании «Актив»

БАНК НА ДИВАНЕ

ЗАКОН И БИОМЕТРИЧЕСКАЯ
ИДЕНТИФИКАЦИЯ. НЕ ВСЕ ОЧЕВИДНО

Наверное, самым заметным для банковского сообщества законом из принятых в последнее время стал закон, вносящий поправки в 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем». Эти поправки вызвали большой резонанс как в банковской среде, так и в сообществе специалистов по информационной безопасности. Закон дает возможность использовать удаленную биометрическую идентификацию для получения банковских услуг.

Тема биометрической идентификации давно и сильно будоражит умы банковского сообщества. И представители бизнеса банков не сложно понять. На первый взгляд, этот инструмент открывает потрясающие возможности: в перспективе банк получает доступ сразу ко всем жителям нашей необъятной Родины при сравнительно скромных затратах. Открытие счетов будет проходить удаленно, биометрические данные будут предоставляться в банк из государственной системы, затраты банка уменьшаются, количество клиентов увеличивается. На горизонте виднеется рассвет новой банковской эпохи.

Однако имеется ряд не вполне очевидных последствий принятия этого закона, некоторые из которых мы и рассмотрим в контексте хитросплетения технологий, бизнеса и государственных интересов.

ДЕЛО ТЕХНИКИ

Чем существующие способы идентификации не удовлетворяют регулятора и чем обусловлена необходимость применения биометрической идентификации? В первую очередь тем, что

при удаленной идентификации без использования биометрии невозможно убедиться в том, что идентификацию проходит законный владелец идентификатора. Доступ к материальным носителям идентификационной информации, PIN-кодам и паролям может быть получен злоумышленником законным или незаконным способом.

Ответственность за результат идентификации несет банк. Поэтому необходимо с достаточной степенью уверенности убедиться в том, что идентификаторы предъявляет их законный владелец.

Для проведения удаленной идентификации авторами закона были выбраны те биометрические характеристики, которые проще всего снимать в «домашних условиях» — изображение лица и голос. Почему был сделан такой выбор? Вероятно потому, что у типичного клиента банка имеются в распоряжении довольно примитивные средства снятия биометрических характеристик. Как правило, это довольно средний смартфон с видео/фотокамерой и микрофоном, либо компьютер, оборудованный веб-камерой и микрофоном. Характеристики этого оборудования даже близко не позволяют анализировать радужную оболочку или сетчатку глаза, а другие биометрические данные зачастую крайне неудобно получать при прохождении идентификации в банковском приложении.

Краеугольным камнем биометрической идентификации можно назвать стойкость к ошибкам второго рода, то есть способность распознавать подделки. Идентификация по лицу — это многоступенчатый и сложный с математической точки зрения процесс, завершающим этапом которого является

собственно идентификация субъекта. Но для начала алгоритму распознавания требуется определить, есть ли на полученном с камеры изображении человеческое лицо, насколько пригодно изображение для идентификации, в конце концов насколько это лицо «живое». На любом из этих этапов возможны ошибки и задача злоумышленника состоит в том, чтобы изготовить подделку, которую алгоритм не сможет распознать.

Поскольку технологии распознавания лица еще не применяются массово, у злоумышленников пока еще нет достаточной мотивации. Но с распространением технологии в финансовом секторе такая мотивация появится, и мы увидим подделки такого уровня, что ни один современный алгоритм не сможет их распознать. А для изготовления поддельного «лица» потребуется всего лишь некоторое количество фотоснимков жертвы в достаточном разрешении. Возможно, например, появление технологии динамической генерации 3D-модели лица любой степени реалистичности и «живости». Пока поставщики решений не раскрывают свои алгоритмы, но секретность алгоритмов еще никогда не давала хороших результатов.

Ситуация с распознаванием и синтезом голоса представляется даже более простой с точки зрения изготовления подделок.

Изображение лица и голос — это те биометрические характеристики, контролировать распространение которых человек не в состоянии. Невозможно постоянно ходить молча и с бумажным пакетом на голове. В случае компрометации биометрических данных их обладателя ждет незавидная судьба, поскольку изменить биометрические характеристики пока еще невозможно.



ДОВЕРЯЙ, НО ПРОВЕРЯЙ

Коль скоро дело дошло до принятия закона, регламентирующего применение биометрической идентификации, оценка качества решений, которые будут использоваться для проведения процедур первичной и вторичной идентификации в скором времени станет насущной задачей.

С криптографией все более-менее ясно и привычно: существуют обязательные для применения ГОСТы, классификация СКЗИ, требования к криптографическим средствам различных классов и существует система оценки соответствия конкретных продуктов этим стандартам.

С биометрией в этом смысле ситуация полностью неопределенная и непрозрачная. Если государство берется регулировать эту область, необходимо построить всю систему: разработать классификацию средств биометрической идентификации в зависимости от выполняемых задач и условий применения, сформулировать требования и критерии оценки. Именно на этом и должно базироваться доверие к той или иной технологии или набору технологий, применяемой для целей идентификации в государственных масштабах.

Косвенно эта проблема нашла отражение в реализации Единой Биометрической Системы. Для обеспечения «вендорнезависимости» биометрические

персональные данные будут храниться в виде «сырых» образцов, полученных в процессе первичной идентификации. Такой способ хранения дает потенциальную возможность смены алгоритмов распознавания и предполагает развитие конкуренции на рынке технологий распознавания. Платой за такую возможность станет необходимость обеспечения очень серьезной безопасности хранения биометрических персональных данных.

Авторы закона в пояснительной записке утверждают, что «идентификация с использованием биометрических персональных данных имеет наивысшую степень надежности в цифровом пространстве», однако без проведения масштабных независимых исследований в этой области и публикации результатов утверждение остается спорным.

БИЗНЕС, НИЧЕГО ЛИЧНОГО

Сбором биометрических данных будет заниматься сильно ограниченный круг уполномоченных банков. Организация сбора данных потребует определенных вложений со стороны уполномоченных банков. Отдадут задачу банкам, входящим в рабочую группу по удаленной идентификации с максимально развитой сетью филиалов. Понятно, что государственная федеральная информационная система ЕСИА выбрана как

нейтральная по отношению к кредитным организациям. Это в своем роде защита для мелких игроков рынка банковских услуг. Но пока не прописаны механизмы контроля и обеспечения обязательности внесения полученной биометрической информации в ЕСИА, возможны злоупотребления со стороны уполномоченных банков. Очевидно, что крупные кредитные организации, будучи операторами сбора данных, получают определенное конкурентное преимущество. Они в первую очередь не заинтересованы в том, чтобы доступ к этим данным получали другие банки.

Таким образом, основная конкуренция за клиента скорее всего развернется среди крупных и средних игроков, которые смогут предложить более интересные условия, уровень обслуживания, качественные онлайн-сервисы. Как результат, малые региональные банки могут остаться без возможности выйти на новые рынки.

* * *

Мы сейчас находимся в самом начале пути. Еще многое предстоит сделать и с технической, и с правовой точек зрения. Кто знает, какой результат нас ждет впереди — светлое будущее, где будут удобные сервисы для людей? Но чем придется расплачиваться за удобство?



Евгений ЦАРЕВ
эксперт RTM Group

МНОГОЛИКАЯ ЭКСПЕРТИЗА

ТЕКУЩАЯ ПРАКТИКА СУДЕБНЫХ ДЕЛ ПО
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Окончание. Начало в № 4/2017)

ТРИ ИПОСТАСИ

Если происходит привлечение эксперта в судебный процесс, то есть, когда в судебном порядке стороны не смогли прийти к соглашению и оказались в суде, эксперта можно привлечь в трех различных качествах. Во-первых, в качестве представителя одной из сторон, когда эксперту выдается доверенность, и он уже является даже не экспертом в процессуальном статусе, а именно представителем стороны. Тем не менее, за счет своих специальных знаний он может повлиять на ход процесса, найти новые доказательства, привести их для рассмотрения суда и т.д.

Во-вторых, в качестве специалиста. Это отдельный процессуальный статус. Специалиста в судебное заседание привлекают для дачи пояснений. В зависимости от специализации суда — общей юрисдикции или арбитражный — позиция специалиста и варианты его работы могут отличаться. Но в целом он не готовит экспертное заключение, он именно дает пояснения суду. Когда возникает узкопрофильный специальный вопрос, его могут вызвать, он даст пояснения, напишет расписку об ответственности за дачу ложных показаний, и после этого суду будет проще оценивать доказательства и выносить обоснованное решение.

В-третьих, в качестве эксперта. Тут есть два варианта. Первый называется внесудебная экспертиза. Это — привлечение эксперта для проведения досудебной экспертизы, когда одна из сторон привлекает специалиста для дачи соответствующего заключения. Доверие к такой экспертизе значительно ниже, чем к судебной экспертизе по причине того, что эксперт в данном случае не предупреждается об ответственности

за дачу заведомо ложного заключения по 307 статье Уголовного кодекса. А вот когда суд самостоятельно либо по ходатайству одной из сторон привлекает эксперта для проведения судебной экспертизы — такого рода экспертиза носит в большинстве случаев решающее значение. То есть, оспаривать в дальнейшем выводы эксперта крайне сложно. Если суд назначил эксперта, эксперт подготовил экспертное заключение, у него есть соответствующие выводы, то с высокой долей вероятности суд примет эти выводы просто как данность.

ДОСУДЕБНАЯ И СУДЕБНАЯ

Соответственно, есть различие в привлечении экспертов для проведения досудебной экспертизы, и для проведения судебной экспертизы.

Досудебная экспертиза проводится по инициативе одной из сторон (на основании прямого договора между этой стороной и экспертом). Если в суде будет принято решение о том, что необходима уже судебная экспертиза, то стороны должны представить суду информационные письма из экспертных организаций. В них будет указано экспертное учреждение, которое привлекается, фамилия эксперта, сумма, за которую эксперт готов работать, на какие вопросы он должен ответить, какой срок на экспертизу ему не-

обходим. После этого стороны по делу или сторона, ходатайствующая о проведении экспертизы, вносит деньги на депозит суда. Эти деньги в дальнейшем будут использованы для оплаты работы экспертов, то есть экспертные учреждения или эксперт получают деньги уже непосредственно от суда.

Здесь есть принципиальное отличие от досудебной экспертизы. В данном случае эксперт работает по поручению суда, а не по поручению одной из сторон.

ОЦЕНКА КОМПЕТЕНТНОСТИ

Вариантов оценки компетентности судебного эксперта много, и если обобщить, то его компетентность оценивается судом самостоятельно по собственным внутренним убеждениям. Каким образом, какие документы необходимо предоставлять? Как правило, это сведения об образовании, местах предыдущей работы, службы, различные сертификаты, подтверждающие квалификацию, ссылки на экспертизы, проводившиеся ранее — и в результате суд из нескольких кандидатов выберет того, кого считает наиболее подходящим.

ЭКСПЕРТИЗА ИБ

В России традиционными именно в части ИТ и ИБ являются эксперти-

ВАРИАНТОВ ОЦЕНКИ КОМПЕТЕНТНОСТИ СУДЕБНОГО ЭКСПЕРТА МНОГО, И ЕСЛИ ОБОБЩИТЬ, ТО ЕГО КОМПЕТЕНТНОСТЬ ОЦЕНИВАЕТСЯ СУДОМ САМОСТОЯТЕЛЬНО ПО СОБСТВЕННЫМ ВНУТРЕННИМ УБЕЖДЕНИЯМ

зы компьютерно-технические, когда проводится исследование какого-то материального объекта — компьютера, жесткого диска, сервера, какой-то информационной системы. Но судебная практика показывает, что не всегда этого оказывается достаточно, и в первую очередь — именно в рамках вопросов, связанных с ИБ. Потому что, даже получив выводы технического эксперта, суд не всегда однозначно понимает, какое решение будет наиболее объективным и правильным.

Здесь можно привести пример, связанный с дистанционным банковским обслуживанием. Техническая экспертиза может, например, показать, что компьютер клиента, с которого осуществлялись платежи или перевод денег в банк, был заражен вирусом.

Эксперт может указать тип вируса, описать механизм хищения, но, тем не менее, для суда так же интересно — каковы были договорные отношения между банком и клиентом, не нарушали ли стороны какие-то требования регуляторов в части, например, той же криптографии. В данном случае суду также нужно оценить, были ли выполнены клиентом все требования банка по ИБ, какие меры принял банк для предотвращения хищения и т.п. Как быть, если сам банк не исполнял требования Банка России? Для суда вскрытие таких фактов будет более чем интересно. Таким образом может быть доказано, что банк не проявил должной осмотрительности в проведении платежей, и в результате ответственность за хищение может лечь на банк.

В ТРЕНДЕ НОРМАТИВНАЯ ЭКСПЕРТИЗА

Нормативная экспертиза позволяет суду получить специфичные и ранее неизвестные факты по делу. Такая экспертиза будет отдельным доказательством наравне с другими экспертизами, которые имеются в деле. При этом нормативная экспертиза никоим образом не подменяет компьютерно-техническую экспертизу, а скорее ее дополняет и корректирует.

Досудебная нормативная экспертиза может быть достаточным основанием не назначать другие экспертизы и вынести решение по делу. Бывали случаи,

ВОВРЕМЯ ПОДГОТОВЛЕННАЯ НОРМАТИВНАЯ ЭКСПЕРТИЗА МОЖЕТ ПОВЛИЯТЬ НА РЕШЕНИЕ ОДНОЙ ИЗ СТОРОН ЗАКЛЮЧИТЬ МИРОВОЕ СОГЛАШЕНИЕ

когда проведение досудебной нормативной экспертизы по вопросам информационной безопасности в принципе завершало процесс, то есть суд выносил решение, не назначая соответствующую судебную экспертизу. Выводов эксперта было достаточно для суда. И, как уже говорилось, если проводится судебная экспертиза, оспорить ее выводы чрезвычайно сложно, это основное доказательство.

Почему нормативная экспертиза столь значима в текущей судебной практике? Дело в том, что огромное количество требований РФ по вопросам информационной безопасности носят предписывающий характер со стороны регуляторов, законодательства, и выявление тех или иных нарушений может значительно изменить ход процесса в целом. Вовремя подготовленная нормативная экспертиза может повлиять на решение одной из сторон заключить мировое соглашение. Немало примеров, когда в результате нормативной экспертизы вскрывалось множество нарушений с одной из сторон, после чего стороны приходили к мировому соглашению, дабы не выносить спор в публичное русло.

Вариативность нормативных судебных экспертиз в части ИБ огромная. Вопросы, связанные с хищением через ДБО, в настоящий момент приоритетны, это некий тренд. В то же время и сама судебная практика меняется. Если раньше практика была строго на стороне банков, то сейчас и банк, и клиенты банка находятся в ситуации, когда они могут оказаться виноватыми в том или ином хищении. Соответственно нормативные экспертизы становятся самостоятельным видом судебной экспертизы, необходимым в таких процессах.

ПРИМЕРЫ КЕЙСОВ

Удаленный доступ к ресурсам организации. К внутренним ресурсам орга-

низации был осуществлен доступ со стороны злоумышленников, которые нарушили работу систем. В дальнейшем, в ходе расследования, проведения компьютерно-технических и нормативных экспертиз было выявлено, что удаленный доступ совершили бывшие сотрудники. После чего были подняты договоры с этими сотрудниками, и в дальнейшем они были привлечены к ответственности, в том числе им пришлось полностью возместить ущерб.

Защита охраняемой законом тайны. Нужно сказать, что вариантов тайн в РФ очень много. И если в организации — неважно государственная она или коммерческая — внедрен соответствующий режим, то экспертиза может установить факт наличия такого режима, его корректность или наоборот некорректность. На основании этого уже можно спорить о нарушениях данного режима. Как правило такие споры ведутся между организацией и ее сотрудниками, либо между отдельными организациями.

КЕЙС-НОВИНКА

Один из новых трендов, который появился буквально в прошлом году, — это споры, касающиеся крупных сделок с использованием электронной подписи. В настоящий момент разрешено заключать договоры, например, купли-продажи недвижимости с использованием электронной подписи. Электронная подпись организациями и клиентами не всегда хранится и охраняется должным образом. Соответственно имеют место инциденты, когда сделки с использованием ЭП совершаются, и в дальнейшем их пытаются оспорить. Тут практика только формируется, но тем не менее это новый выраженный вектор атак, не требующий крупных затрат со стороны злоумышленников. При этом тот куш, который злоумышленники могут получить и часто получают, чрезвычайно велик.



Ольга ЗИНЕНКО
аналитик информационной
безопасности
Positive Technologies

МИШЕНЬ ДЛЯ ТЕРПЕЛИВЫХ

КАКИЕ НЮАНСЫ УПУСКАЮТ БАНКИ
В БОРЬБЕ С ХАКЕРАМИ

Одну из самых дорогих картин мира — «Крик» Эдварда Мунка — похищали дважды. Во время зимней Олимпиады 1994 года охранники были увлечены спортивной трансляцией и просто не услышали сигнализацию. А через десять лет инцидент повторился: грабители в масках забрались по строительным лесам и на глазах посетителей забрали другую версию «Крика» (и еще одну картину впридачу), вся операция заняла 58 секунд. В результате музей Мунка закрыли почти на год для усиления мер защиты, поставив ударопрочные стекла для картин, видеонаблюдение, рентгеновские сканеры, металлоискатели, ворота безопасности.

Ситуация в банковской сфере немного похожа. В 2017 году мы собрали статистику по 170 компаниям, 23% которых — финансовые организации. Значительная их часть (за исключением тех, которые отличаются высоким уровнем зрелости с точки зрения информационной безопасности, и большей ориентацией на digital), к сожалению, до сих пор практикуют поистине музейный консерватизм по отношению к информационной безопасности, применяя только типичный набор средств и мер защиты. Оценивают уровень своей реальной защищенности и внедряют

новые технологии защиты (например, самообучаемые механизмы выявления атак) далеко не все.

Большинство участников отрасли слышали об атаках Carbanak и Cobalt (а то и вовсе сталкивались с ними). Эти группировки активно использовали фишинговую рассылку, имитируя финансовую корреспонденцию, письма от службы ИБ, подрядчиков и др. Хорошая новость в том, что 100% банков обучают сотрудников основам информационной безопасности: как минимум, выявлять подозрительные письма и ссылки. Плохая — в том, что эффективность такого обучения не проверяется аж в 57% случаев. Все равно что у студентов отменить экзамены, рассчитывая на их сознательность.

БЕЗОТКАЗНЫЕ ОТМЫЧКИ

При этом «на темной стороне» идет активнейшая работа. Мы уже отмечали, что методы проникновения группы Cobalt в сеть банков очень быстро эволюционируют — фишинговые письма отправляются с почтовых адресов взломанных контрагентов, регистрируются схожие домены, используются вредоносные документы MS Word, имитирующие предупреждения Центробанка, Visa и MasterCard, атакуются личные почтовые ящики сотрудников банка. Потенциально опасные вложе-

ния открывают в среднем 20–30% сотрудников. Но в случае с атаками группировки Cobalt, отправляющей письма от лица контрагентов, процент открывших в 2–2,5 раза выше. Поэтому ограничиваться формальным подходом к обучению сотрудников основам ИБ просто опасно.

Защита периметра в банке сегодня бесполезна без одновременной защиты веб-приложений, так как злоумышленник всегда выбирает наиболее легкий путь. По нашим данным, в трех из четырех случаев периметр можно преодолеть при помощи веба. Через веб взламывали даже таких защищенных «монстров», как JPMorgan Chase. Проблема в том, что контролировать (или поддерживать в актуальном состоянии) безопасность веб-приложений достаточно сложно: они регулярно требуют улучшений и доработок. Пытаясь уложиться в сроки, разработчики полностью фокусируются на функциональности, создавая все больше уязвимостей в исходном коде приложения. Кроме того, идеальную картину всегда подпортят сервисы подрядчиков, защищенность которых не всегда возможно контролировать, и legacy-приложения, которые уже не поддерживаются разработчиками. Эту задачу помогают решать межсетевые экраны прикладного уровня (Web Application Firewall), однако в 2017 году в России для защиты веб-приложений их применяют только 70% банков (из топ-10 по ИБ-бюджету) и лишь 13% среди остальных.

По нашим оценкам, в 36% систем сетевой периметр удастся преодолеть из-за недостаточной защиты беспроводных сетей. Во время одного из аудитов безопасности специалисты Positive

**ЗАЩИТА ПЕРИМЕТРА В БАНКЕ СЕГОДНЯ
БЕСПОЛЕЗНА БЕЗ ОДНОВРЕМЕННОЙ
ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ, ТАК
КАК ЗЛОУМЫШЛЕННИК ВСЕГДА
ВЫБИРАЕТ НАИБОЛЕЕ ЛЕГКИЙ ПУТЬ**

Technologies прямо со стоянки возле офиса смогли подключиться к корпоративной сети компании, перехватить учетные записи нескольких сотрудников и получить все возможности для развития атаки внутри сети. Об опасности автоматического подключения мобильных устройств к знакомым сетям специалисты говорят не первый год: злоумышленники могут использовать поддельную точку доступа для перехвата паролей и логинов. В 2016 году с помощью подобных атак специалисты Positive Technologies успешно перехватывали аутентификационные данные в 75% проектов по анализу защищенности. Но почти каждый четвертый опрошенный нами банк уверен в безопасности своих беспроводных сетей и никогда не проводил анализ их защищенности, еще половина делала аудит только после инцидента.

ВРАГ УЖЕ ВНУТРИ

Представим ситуацию, что преступник уже попал в сеть и пытается захватить контроль на критическими рабочими станциями (АРМ КБР, например). Выявить подозрительную активность возможно с помощью грамотно настроенных SIEM-систем. Однако подобные системы установлены лишь у 65% банков.

Но самая любопытная история была связана с атаками шифровальщиков. WannaCry и NotPetya, кажется, научили бизнес своевременно устанавливать обновления безопасности для исключения уязвимостей. Но нет — у 25% банков-респондентов отсутствует контроль установки обновлений ПО, а 8% не отслеживают появление информации о новых уязвимостях (0-day).

Можно предположить, что кредитные организации не осознают потенциальный ущерб. Но у всех перед глазами ситуации с «Металлинвестбанком» или «Глобэкс». В первом случае потери составили 200 миллионов рублей, во втором случае преступникам удалось по разным оценкам забрать из банка 80 млн рублей, причем преступники уже вывели 75 млн долларов, но SWIFT в своих системах заморозил большую часть суммы.

Более половины участников нашего опроса оценили предполагаемые по-

КАЖДЫЙ ВОСЬМОЙ БАНК НЕ ПРОВОДИТ ИНВЕНТАРИЗАЦИЮ СВОИХ РЕСУРСОВ, А КАЖДЫЙ ТРЕТИЙ ДЕЛАЕТ ЭТО ТОЛЬКО ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О РЕСУРСАХ И НЕ ОЦЕНИВАЕТ ИХ ЗАЩИЩЕННОСТЬ

тери от кражи базы данных клиентов конкурентом в сумму более 50 млн руб. Треть оценивают минимальный ущерб от нарушения деятельности в течение одного дня в 50 млн рублей. Эти суммы превышают годовой бюджет на ИБ большинства опрошенных финансовых учреждений, который ограничиваются суммами в 20–40 млн рублей.

Как мы видим, российские банки хорошо понимают возможные потери. Однако только 13% опрошенных организаций финсектора применяют комплексный подход к защите от киберугроз. Иными словами, один банк защищается от веб-атак, но не учит сотрудников выявлять потенциально опасные вложения в письмах, второй анализирует защищенность Wi-Fi-сетей, но никогда не проводит работ по тестированию на проникновение. Поэтому опасность может прийти откуда угодно.

ВЫНУТЬ ГОЛОВУ ИЗ ПЕСКА

Вышеперечисленные проблемы касаются кредитных организаций со средними и небольшими затратами на информационную безопасность. Но и банкам, расходуящим на ИБ выше 100 млн руб. в год, рано почивать на лаврах. Уровень защищенности «слабого звена» определяет, в конечном счете, прочность всей системы, и чем быстрее растет инфраструктура, тем сложнее следить за ней.

Не так давно мы рассказывали, насколько легко найти уязвимые сервисы банков в открытом доступе, в том числе в инфраструктуре топ-25 крупнейших кредитных организаций. Если коротко, то сегодня целенаправленные атаки на банки не требуют особых финансовых затрат: вместо специальных сканеров может быть использован Google, вместо уязвимостей нулевого дня — эксплойт-паки, слитые группой The Shadow Brokers. Согласно нашему

опросу, каждый восьмой банк не проводит инвентаризацию своих ресурсов, а каждый третий делает это только для получения информации о ресурсах и не оценивает их защищенность.

Так что же делать? Основной принцип — не закрывать глаза на проблему, а находить оптимальное ее решение. Если отказ от установки актуальных патчей для печально знаменитого протокола SMBv1 связан с опасениями по поводу корректности работы бизнес-процессов, значит необходимо принимать альтернативные шаги, выделяя такие системы в отдельный сетевой сегмент и блокируя к нему доступ из пользовательской сети.

Любой банк проводит тренировочные учения на случай пожара, но как действовать при блокировке шифровальщиком рабочих станций не всегда знает даже специалист по ИБ. При устройстве в банк нового сотрудника служба безопасности, как правило, неделями проверяет его биографию, однако к инструктажу сотрудников в вопросах ИБ банки подходят не столь внимательно. В итоге специалист вполне может открыть зараженное письмо с очередной счет-фактурой, передавая управление своим ПК неизвестному киберпреступнику.

* * *

Каждая финансовая организация — мишень для терпеливых, скрупулезных целевых атак. В данных случаях традиционный набор средств информационной безопасности оказывается несостоятельным в девяти случаях из десяти. При этом такие атаки не требуют больших инвестиций. И если вы планируете защитить свой банк от групп подобных Cobalt, необходимо учитывать перечисленные особенности.



Лев ПАЛЕЙ
эксперт
по информационной
безопасности

АНАЛИТИКА ОСОБОГО НАЗНАЧЕНИЯ

КАК УЗНАТЬ, КУДА ДВИЖЕТСЯ РЫНОК СРЕДСТВ ЗАЩИТЫ?

Сейчас на слуху UEBA (User and Entity Behavior Analytics, если кратко — пользовательская аналитика) — транскрипция на русском, при плохом произношении, неблагозвучная, но слышно про нее из каждого «утюга» на каждом профильном мероприятии. По аналогии с раскрытой UEBA предлагаю назвать процесс анализа поведения компаний-производителей решений информационной безопасности — Vendor Behavior Analytics (VBA). К чему это?

Одна из сторон деятельности ИБ — выбор подходящего средства защиты, а в случае с распределенными, централизованно управляемыми компаниями ещё и архитектурно-экономическое моделирование будущей комплексной системы обеспечения ИБ. По сути этот процесс анализа можно обозвать анализом рынка, но с учётом геополитической ситуации, критериев становится на порядок больше. Как минимум: функциональность решения, цена, страна-производитель (теперь идет как повышающий приоритет для выбираемого решения, а при решении задач обеспечения соответствия, как определяющий), соответствие задачам (насколько маркетинговый анонс соответствует текущей постановке задачи), надежность решения/качество.

РАЗУМНОСТЬ ВЛОЖЕНИЙ

Выбор можно осуществлять на основе известной управленческой методики под названием «домик качества», но вот «задел на будущее» сложнее.

Как определить, что именно тот вендор, будет развиваться и поставлять нужные компании функции? Простого ответа нет, но согласитесь, полезно понимать куда идёт рынок. Основная идея прозрачна — для того, чтобы определить перспективное решение, необходимо понимать основные угрозы, как актуальные на текущий момент для вашей компании, так и возможные будущие. Один из способов определения будущих угроз — проведение оценки набирающих популярность на мировом рынке направлений, потому как если и учится, то у столпов. И здесь ориентировку на популярность, с учетом базового понимания механизма принятия решений самими компаниями-производителями, коротко можно объяснить разумностью вложений. Схематично получается так:

1. Любая глобальная компания (примеры будут ниже), которая в значительной степени зависит от продажи решений для информационной безопасности ориентируется на потребности своего рынка.

2. От того насколько широко покрытие рынка (в мировом масштабе) продуктами, варьируется количество запросов на потребности от заказчиков, а значит и степень проработки сценариев использования.

3. Сценарии зависят от локальных потребностей, обусловленных законодательством, менталитетом и другими критериями.

4. На основе известных сценариев, данных об их количестве формируются инициативы по расширению, модернизации продуктовой линейки. Инициативы проходят процесс обоснования, прорабатываются и оцениваются с учетом актуальных угроз и перспективной прибыли получаемой компанией-производителем.

ПОЧЕМУ НЕ ИСПОЛЬЗОВАТЬ «AS IS»?

Наличие и объем такой информации дает пищу для последующей аналитики и принятия решения о выборе направлений развития. Почему не использовать уже проведенную другими работу на благо своей компании по

**ДЛЯ ТОГО, ЧТОБЫ ОПРЕДЕЛИТЬ
ПЕРСПЕКТИВНОЕ РЕШЕНИЕ,
НЕОБХОДИМО ПОНИМАТЬ
ОСНОВНЫЕ УГРОЗЫ, КАК
АКТУАЛЬНЫЕ НА ТЕКУЩИЙ
МОМЕНТ ДЛЯ ВАШЕЙ КОМПАНИИ,
ТАК И ВОЗМОЖНЫЕ БУДУЩИЕ**



принципу «как есть»? Во-первых, как говорил известный «сериальный» доктор — «все врут» (или немного приукрашивают). Поэтому прямой звонок в маркетингово-продажный отдел не приведёт к успеху. Во-вторых, для приземления чужого опыта нужно понять, в чем разница между исходными данными. И вот тут уже «полный VBA» — нужно просеять известные действия, отделить свидетельства здоровья компании от активностей, направленных на создание/адаптацию решений для предотвращения новых угроз, попробовать понять логику принятия решений.

БАЗОВЫЕ ПРИМЕРЫ

Попробую выделить основные направления развития компаний-производителей и подкрепить их известной информацией:

1. **Разделение бизнеса ИТ и ИБ.** Яркий пример — продажа 21.06.2016 компанией Dell инвестиционной фирме Francisco Partners и хедж-фондом Elliott Management Corporation своего подразделения Dell Software Group,

которое занималось и информационной безопасностью, в частности, развивая решения ранее приобретенных Qwest и SonicWALL. Более показательные и известные примеры: 7.09.2017 Intel продала компанию McAfee инвестиционному фонду TPG Capital за сумму меньшую, чем компания была приобретена ранее. НРЭ в свою очередь 1-го сентября объявила о слиянии с британской компанией Micro Focus своего подразделения по разработке ПО (как и в случае Dell внутри подразделения прорабатывались решения по ИБ). Что характерно для обоих случаев, ИБ-ориентированный бизнес был приобретён в конце 2000-х годов, произведены попытки интеграции новых подразделений в существующую организационную структуру компаний. Во всех случаях в результате попытки унификации операционных процессов привели к закрытию ряда продуктовых направлений, в частности Intel сделала шаг в сторону от устоявшейся стратегии McAfee по развитию собственной продуктовой экосистемы, за-

крыв направления, не представленные в Gartner (McAfee Email Gateway и Vulnerability Management).

2. **Западный тренд «все в облако».** Ещё раз упомяну McAfee, которая в ноябре 2017 закрыла сделку по приобретению одного из лидеров решений класса CASB, компании SkyHigh. Компания Landesk в 2016-м году прикупила ещё одного облачного игрока — Appsense. Вкупе с движением Microsoft в сторону предоставления облачных сервисов и уходом изрядной части функциональности решений по выявлению уязвимостей известных производителей (Quails, Nexus и пр.) в облако, одноименный тренд становится очевидным.

3. **Поведенческая аналитика, искусственный интеллект, наращивание сервисной составляющей и карты интеграций.** На первый взгляд пункт смешивает все мыслимое и несвязанное. Но эти понятия всегда означают системную проработку вопросов реагирования на инциденты ИБ и говорят либо о разработке SOC-связанного продукта, либо о подготовке к оказа-

нию «SOChных» услуг. К примеру, Juniper в августе приобрела Cyphort, ещё одного производителя решений класса «Sandbox» (или по-простому — песочниц), став таким образом в один ряд с Fortinet (который в июне 2016-го года приобрёл AccelOps), уже обладавшим таким решением в своей линейке продуктов, и Palo Alto (купившей LightCyber, специализирующейся на поведенческой аналитике в марте 2017-го). Помня про IBM, которая продвигает идею искусственного интеллекта (в том числе и в информационной безопасности) на базе IBM Watson, нельзя забыть про приобретение этой же компанией в 2016-м году Resilient System известной своей платформой управления инцидентами и предоставляемыми сервисами. Ещё один гигант, смотрящий в сторону искусственного интеллекта, ориентированного на информационную безопасность, — Microsoft, в июне 2017-го поглотившая стартап Hexadite.

ПАРА АНАЛОГИЙ

И это только самые известные примеры. Из выделенных направлений уже можно делать выводы, которые, конечно могут быть субъективными и частично спорными. И чтобы логическая цепочка была более полной, предлагаю рассмотреть ещё один общий тренд (более технический) — абстрагирование от аппаратного уровня при создании ряда решений обеспечения ИБ. Как пример можно привести набирающую популярность аббревиатуру SDN (Software Defined Networking), которая напрямую не относится к защите информации, но зачастую упоминается в связке с процессами автоматизации применения политик безопасности при создании управляемых сетей (особенно активно этим понятием пользуется VMware при продвижении своего решения NSX). Здесь самой близкой ИБ аналогией являются устройства класса NGFW, которые изначально позиционировались как комбайны предоставляющие из коробки разные сервисы (IPS, FW, Web-filter), включаемые «под заказ» потребителя, после оплаты определенной расширяющей лицензии. Первыми компаниями, предлагающими такие комбайны, стали уже упомянутые Palo Alto Networks и Check Point, а сей-

час классических устройств почти не осталось — даже адепт надежного подхода компания Cisco отказалась от развития линейки ASA в принятой ранее модели и уходит на аналогичную модульную платформу Firepower (разработанную по итогам слияния с Sourcefire). Чем похожи SDN и NGFW? Уходом от восприятия «устройство-задача», переносом модульности на программный уровень и ослаблением привязки к аппаратной составляющей.

НИША ДЛЯ СПЕЦАНАЛИТИКИ

И если здесь вспомнить про тренд отделения софтверных бизнесов от аппаратных (п.1), прослеживается связь и сходство. П.2 говорит об устойчивом перемещении аналитической части ИБ в облако, а также популяризации сервисов обеспечения защиты облачных приложений. П.3 говорит о рождении пока не настолько понятной, но усиленно развивающейся ниши искусственноинтеллектуальной-поведенческой аналитики, практически всегда сопровождающейся развитой экосистемой взаимноинтегрированных продуктов (IBM, Microfocus/HPE, McAfee, Fortinet), либо имеющих в основе платформы обработки больших данных (SIEM), либо ориентированных на интеграцию с широким спектром систем такого класса.

ЛОГИЧЕСКАЯ ЦЕПОЧКА

Прослеживается интересная цепочка, в которой постепенное движение от аппаратной составляющей и программного обеспечения к полному абстрагированию от решений, платформ и функций выглядит следующим образом:

1. Под каждую задачу самостоятельная аппаратная и программная платформа, отсутствие интеграции;
2. Интеграция смежных решений, создание собственных экосистем компаниями;
3. Активное использование и продвижение открытых стандартов, API — обязательный компонент, открытость для внешних экосистем;
4. Работа с большими данными, управление компонентами систем защиты других производителей, разделение на нишевых и глобальных игроков,

абстрагирование от парадигмы развития одна-задача-одна-коробка;

5. Ориентировка на автоматизацию первичной аналитики, отделение программных платформ от аппаратных составляющих, «fly-to-the-sky», рождение искусственного интеллекта.

ПОЛЕЗНА ЛИ VBA?

Можно представить следующий пункт в таком виде: сервис, предоставляемый искусственным интеллектом на базе облачной платформы. Если не считать такую аналитику просто развлечением и футуристическими фантазиями, учитывая все вышеописанное, чем может быть полезна VBA компании? Предлагаю посмотреть с нескольких точек зрения:

♦ В разрезе архитектурной составляющей и планирования расходов: не имеет смысла закупать или расширять продуктовую линейку, снятую или готовящуюся к снятию с продаж. Стоит синхронизировать планы с общими направлениями развития.

♦ Если вы интегратор или ИТ-ориентированная компания: многое из перечисленного выше — ваш хлеб, а значит, громкое внедрение или инновационный продукт, учитывающий общие тенденции развития, могут повысить вашу капитализацию.

♦ Если у вашей компании высокая зрелость процессов ИТ и ИБ, вы задумываетесь о выполнении KPI, оптимизации затрат и трудоресурсов в долгосрочной перспективе.

Как бы ни была надумана сама аббревиатура, основание под ней крепкое — с помощью даже такой базовой аналитики можно получить представление как о направлениях развития гигантов индустрии, так и об актуальных угрозах, на нейтрализацию которых ориентирована основная часть заказчиков таких решений

Простые выводы, которые можно сделать по опубликованным данным, приводят к мыслям о реальной динамике применения изменений, ведь то, что находится на вершине айсберга, не позволяет представить ни объем, ни основные составляющие двигателей прогресса.



Олег ИВАНОВ
генеральный директор
ООО «ЦИБИТ»



Василий ОКУЛЕССКИЙ
руководитель Департамента ООО «ЦИБИТ»,
кандидат технических наук

КАК УСПЕТЬ ЗА РЕГУЛЯТОРОМ?

ОСОБЕННОСТИ COMPLIANCE В УСЛОВИЯХ
ИЗМЕНЯЮЩИХСЯ ТРЕБОВАНИЙ НОРМАТИВНЫХ
ДОКУМЕНТОВ БАНКА РОССИИ

Усиливающийся тренд современности — непрерывное повышение уровня защищенности развивающихся информационных технологий.

Что реально стоит за этими словами? Можно ли спать спокойно в «умном» доме? Можно ли не беспокоиться за свои деньги в on-line мире? Как вообще спокойно жить в эпоху всеобщей «виртуализации»?

Однозначного ответа на эти и сотни похожих вопросов не существует. Тем не менее, есть некоторое количество способов снизить общий уровень нервозности и беспокойства в беспокойный век.

Можно просто на все наплевать, и жить как живется, чему быть — того не миновать. Можно отказаться от интернета и всего, что с ним связано, в том числе и от мобильного телефона, а деньги хранить под матрасом или в банковской ячейке (хотя и здесь есть возможность все потерять).

Можно ... — много всего, но для разумных людей всегда есть классический способ обеспечить доверие к окружающему миру, в том числе и к денежному, и это принятие соглашений о «правилах игры» и выполнение этих правил. И здесь всегда важен статус того, кто выполняет роль «судьи». Для «движения вверх» в такой игре всегда важно, чтобы правила были «правильные», выполни-

мые, контролируемые, понятен порядок их проверки, требования к компетенции проверяющих (им как бы делегированы права и обязанности «судьи» в этой сфере). Тогда, когда есть свидетельство этого проверяющего, что у партнера всё соответствует установленным правилам, можно доверять этому партнеру.

Собственно, эта конструкция и называется «compliance», где в банковской среде самым главным «судьей» выступает Банк России, который устанавливает «правила игры» своими нормативными требованиями, а проверяющими могут стать только те организации, которые имеют необходимые подтверждения своей квалификации от других «судей», и тогда заключение от проверяющих о соответствии проверяемой организации требованиям Банка России теоретически должно давать ощущение спокойствия.

Все хорошо?

Только на первый взгляд. При такой конструкции принципиально все требования делятся на три категории — уже устаревшие (и хорошо, если они только не мешают), вполне себе актуальные (как правило, таких большинство), и те, которых еще нет, но должны бы быть. И состав каждой группы меняется ежедневно, и нет такого состояния, когда все хорошо.

Попробуем посмотреть, как это выглядит на практике.

Банк России предлагает для банков примерно такую конструкцию обязательных нормативных документов, без учета требований стандартов Банка России (рис. 1).

Эти обязательные документы содержат примерно 130 категорий требований (около 700 проверяемых показателей). А еще есть стандарты (условно обязательные) Банка России по обеспечению информационной безопасности:

ВСЕ ТРЕБОВАНИЯ ДЕЛЯТСЯ НА ТРИ КАТЕГОРИИ — УЖЕ УСТАРЕВШИЕ, ВПОЛНЕ СЕБЕ АКТУАЛЬНЫЕ (КАК ПРАВИЛО, ТАКИХ БОЛЬШИНСТВО), И ТЕ, КОТОРЫХ ЕЩЕ НЕТ, НО ДОЛЖНЫ БЫ БЫТЬ. И СОСТАВ КАЖДОЙ ГРУППЫ МЕНЯЕТСЯ ЕЖЕДНЕВНО

♦ СТО БР ИББС-1.0–2014. «Общие положения (5 редакция)»;

♦ СТО БР ИББС-1.1–2007. «Аудит информационной безопасности»;

♦ СТО БР ИББС-1.2–2014. «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2014 (4 редакция)»;

♦ РС БР ИББС-2.0–2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0»;

♦ РС БР ИББС-2.1–2007. «Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0»;

♦ РС БР ИББС-2.2–2009. «Методика оценки рисков нарушения информационной безопасности»;

♦ РС БР ИББС-2.5–2014. «Менеджмент инцидентов информационной безопасности» и т.д.

Перечисленные нормативные документы содержат около 400 различных

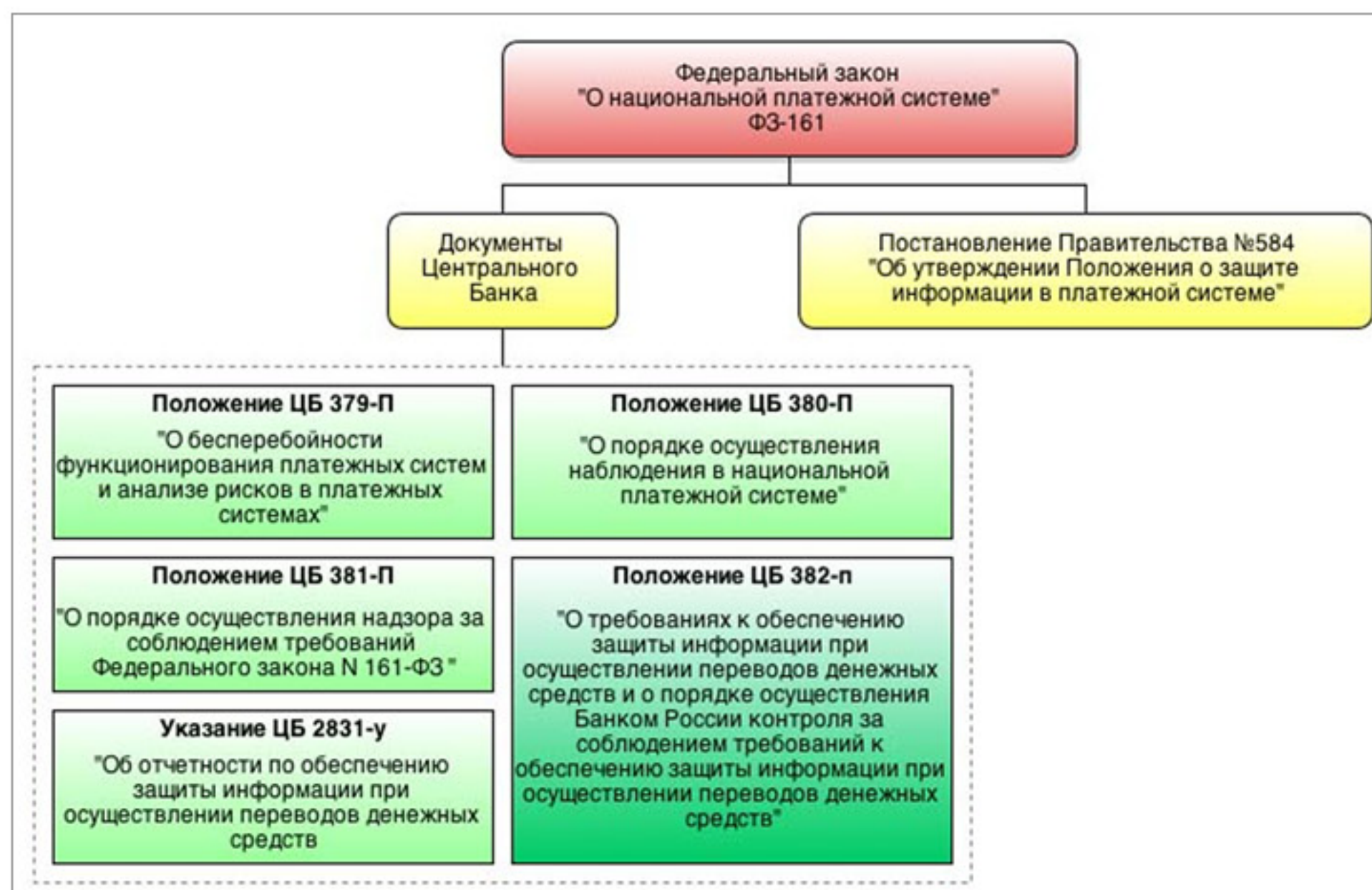


Рисунок 1. Обязательные нормативные документы Банка России

требований, а еще PCI DSS — примерно 240 основных типов требований и 300 других требований различных ответвлений этой группы стандартов, осталось вспомнить требования иных регуляторов (ФСТЭК, ФСБ и Роскомнадзор) — в совокупности более 1000

(одних требований ФСТЭК по обеспечению доверия приближается к 300). Очень грубая арифметика дает оценку в не менее чем 2000 различных требований. Понятно, что все эти требования очень разные, как по типу, уровню, среде применения и т.д., часть тре-



Рисунок 2. Структура примитивов ИБ



Рисунок 3. Модель системы менеджмента примитивов ИБ

бований просто повторяются, часть поглощаются, часть уточняют другие, часть требований противоречат другим требованиям, особенно в запрете/возможности применения тех или иных технических или программных средств.

Могут ли 1–2–3 специалиста по ИБ в небольшом банке (а таких банков не менее 200) сами организовать выполнение всех требований (т.е. обеспечить «compliance»)? Вероятно, где-то есть чудо-специалисты, но они недолго проработают в банке, уйдут на повышение, а как быть тем, у кого нет таких героев?

Выход есть — позвать на **первый раз** организацию, которая имеет необходимые подтверждения своей квалификации от других «судей» и имеющую соответствующий опыт и компетенции и вместе с ней провести комплекс работ по подготовке к первой процедуре оценки.

Сначала потребуется разобрать на элементарные кирпичики объекты защиты ИБ (сформировать своеобразные «примитивы ИБ»), понять для конкретного «примитива», какие требования на него распространяются и задокументировать этот шаг.

Как правило, все нормативные документы, в конце концов, при своей пошаговой декомпозиции имеют дело именно с требованиями по обеспечению «примитива ИБ». Для такого шага

полезно обратиться к стандартам серии ISO 27000 (рис. 2).

Имея описание «примитивов» и схему взаимодействия между собой, можно попробовать затем оценить каждый кирпичик с точки зрения нарушения основных свойств информационной безопасности и рассмотреть возможность его использования злоумышленниками, оценить реальность (актуальность) такой угрозы, если есть актуальная угроза этому кирпичику «примитиву», разработать механизм контроля параметров, отклонения которых будут свидетельствовать о наличии угрозы. Если к этому предусмотреть способы и механизмы реагирования на выявленные признаки угроз, то может получиться вот такая картинка (рис. 3).

Если аккуратно и системно выполнять эти шаги, то вы можете гарантировать, что практически не упустили ничего, чем бы мог заинтересоваться злоумышленник.

В сухом остатке от этой проделанной работы должна остаться уверенность, что вы знаете, где вас могут обидеть, и вы знаете, что вы при этом будете делать.

Есть еще один элемент для творчества — все, что было проделано, основано на наших знаниях об уже «бывших угрозах». В эту модель управления необходимо добавить заботу об «угрозах нулевого дня» и тогда картина будет полной.

Вот теперь можно приступать к следующему шагу — обеспечить уверенность в выполнении вами требований по ИБ самых разных регуляторов. Имея хорошо описанные именно ваши модели рисунков 2 и 3, любой профессиональный аудитор может дать вам заключение, которое сможет убедить ваших клиентов (ибо они вам помогают получать зарплату) и регуляторов (которые тоже заботятся о вас). Эти модели имеют еще и «вишенку на торте». Теперь, когда придут очередные изменения нормативных документов и требований регуляторов, у вас будет описание всего, на что эти изменения могут влиять именно у вас, и что именно вам потребуется доделать/переделать/создать заново, и как это будет влиять на ваши остальные объекты защиты.

* * *

После такой проделанной работы вместе с вашим партнером-консультантом, которым для вас уже с момента прочтения этой статьи становится «Центр исследования безопасности информационных технологий» («ЦИБИТ»), вы сможете самостоятельно поддерживать всю систему менеджмента информационной безопасности и регулярно давать аудиторам возможность положительно вас оценить.

Для этого:

- ♦ Эксперты «ЦИБИТ» проведут квалифицированный аудит на соответствие требованиям регуляторов;
- ♦ Специалисты «ЦИБИТ» подготовят организацию к получению всех необходимых лицензий в области информационной безопасности и помогут их получить;
- ♦ Учебный центр «ЦИБИТ» обучит вас премудростям информационной безопасности и выдаст документ о дополнительном образовании установленного образца (диплом, удостоверение, сертификат);
- ♦ Кадровое агентство «ЦИБИТ» поможет подобрать квалифицированные кадры.

Мы поможем вам соответствовать требованиям, а вы получите уверенность в собственных силах.



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

ТРИ РЕГЛАМЕНТА

ТРЕНДЫ ИБ В СФЕРЕ СТАНДАРТОВ
И НОРМАТИВНЫХ ТРЕБОВАНИЙ

2018 год богат на международные стандарты и обновления требований регламентов по безопасности, которые вступают в силу и ожидаемо серьезно осложняют жизнь организациям. Как показывает практика, многие организации даже не подозревают, что они, в силу своей деятельности, попадают под действие регламентов. Есть три, касающихся европейского законодательства и финансовых организаций: PCI DSS 3.2, GDPR и eIDAS. Они вступают в силу в феврале, мае и сентябре 2018 года соответственно.

Примечательно, что первые два регламента предполагают существенные штрафы за их несоблюдение. Так размер штрафа за несоблюдение GDPR может составлять 2 миллиона евро, либо доходить до 4% годового оборота компании, в зависимости от того, какая сумма больше... Уверен, что до конца этого календарного года мир увидит реальные примеры применения наказаний за несоблюдение регламентов по безопасности для европейских и сотрудничающих с ними компаний, расположенных в разных частях мира.

В PCI DSS 3.2, раздел 8.3, наиболее значительным изменением явилось требование многофакторной аутентификации для администраторов внутри защищенной инфраструктуры организации, имеющей дело с данными платежных карт. Это очень существенное и порой трудновыполнимое требование отражает понимание рисков, связанных с одной стороны с инсайдерами, а с другой — с привилегированными пользователями. Важно отметить, что

в требованиях появилось явное описание понятия многофакторной аутентификации (то, что вы знаете — пароль, то, что вы имеете — токен, или то, что вам присуще — отпечаток пальца) и неприменимость многократного использования однофакторных, хотя и сложных, и отличающихся паролей. Также изменения коснулись всех сотрудников, имеющих доступ к данным держателей карт — пункты 8.3.1 и 8.3.2. Теперь, независимо от их работы в защищенной сети или удаленно, они должны применять многофакторную аутентификацию.

Другим важным изменением стали требования к сервис-провайдерам. Они коснулись как компаний в целом, так и напрямую отдельных руководителей этих компаний. Теперь сервис-провайдеры должны иметь описание полной криптографической архитектуры, что должно нивелировать риски утечек при участии третьих вовлеченных сторон. Также добавлено требование регулярных тестов инфраструктуры на проникновение и создание процессов защиты, отражения, документирования и информирования об атаках, которые могут привести к потере данных.

Несмотря на сужение периметра вокруг данных и минимизацию хранимой информации, требования к физической безопасности становятся не менее актуальными и выражаются в комбинированных требованиях контроля доступа в помещения (RFID) с аутентификаторами PKI (смарт-картами) инфраструктуры открытых ключей. При этом все более приветствуются возможности визуального контроля смарт-карт в решениях корпоративных бэджей (физический и цифровой идентификатор сотрудника) и методов контекстной аутентификации, когда в зависимости от местонахождения сотрудника и используемого им устройства предъявляются разные по степени сложности и защищенности методы аутентификации (рис. 1).

Если требования PCI DSS к использованию шифрования и хранения ключей шифрования отдельно, в железе, уже не является чем-то удивительным, то возможность не разглашать публично взлом данных, которые были зашифрованы (регламент GDPR) — это важный фактор. На текущий момент только 4% компаний шифруют данные, что открывает большую перспективу по

**УВЕРЕН, ЧТО ДО КОНЦА ЭТОГО
КАЛЕНДАРНОГО ГОДА МИР УВИДИТ
РЕАЛЬНЫЕ ПРИМЕРЫ ПРИМЕНЕНИЯ
НАКАЗАНИЙ ЗА НЕСОБЛЮЖДЕНИЕ
РЕГЛАМЕНТОВ ПО БЕЗОПАСНОСТИ ДЛЯ
ЕВРОПЕЙСКИХ И СОТРУДНИЧАЮЩИХ
С НИМИ КОМПАНИЙ, РАСПОЛОЖЕННЫХ
В РАЗНЫХ ЧАСТЯХ МИРА**

	8.1.1	8.1.2	8.1.3–8.1.8	8.2	8.2.3	8.3	9
Context-based	+	+	+	+	+	+	
OTP Push	+	+	+	+	+	+	
PKI (cert-based)	+	+	+	+	+	+	
PKI with PAC	+	+	+	+	+	+	+
OOB	+	+	+	+	+	+	
OTP HW	+	+	+	+	+	+	

Рисунок 1. Рекомендации по решениям аутентификации для соответствия определенным разделам требований PCI DSS

применению методов шифрования данных и управлению ключами шифрования в финансовых организациях и корпоративном секторе, особенно, если подходить к этой задаче системно и защищать данные в состоянии покоя, во время транзита, в виртуальных средах, облаках и т.д.

В свете всё большего использования моделей аутсорсинга, облачных и виртуальных технологий, что благотворно

влияет на сокращение издержек и расходов, открытым остается вопрос ответственности организации за персональные данные и данные платежных карт. Кому вы доверяете? Кто будет нести ответственность, если ваши данные будут скомпрометированы в облаке или арендованном ЦОДе? Ответ — никому. Организации должны ответственно подходить к вопросам защиты информации, и первые шаги, которые помо-

гут решить эти вопросы, начинаются с контроля доступа с помощью автоматизированных систем аутентификации, шифрования данных и управления жизненным циклом ключей шифрования. В совокупности использование этих подходов позволит закрыть львиную долю требований регламентов по безопасности и оградить ваши организации от материальной ответственности и штрафов.



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ПРОФИ

18+

**ПРОФЕССИОНАЛЬНАЯ
КОНФЕРЕНЦИЯ**

ПО УПРАВЛЕНИЮ
**ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТЬЮ**

**1-4
марта
2018**

МОСКВА

msk.codeib.ru

2 дня учебы + 2 дня приключений



Анна ВОРОБЬЕВА
корреспондент
BIS Journal

SOC-ФОРУМ 2017

КАК ОТЕЧЕСТВЕННЫЕ СОС'И ДЕРЖАТ
ЦИФРОВУЮ ОБОРОНУ

Что помогло российским кредитно-финансовым организациям устоять против мощнейших кибератак? Будет ли введено лицензирование центров ГосСОПКА? В чем причина низкой эффективности современных SOC? Взаимодействие с госструктурами: что нас ждет? Эти и многие другие вопросы обсуждались на SOC-Форуме 2017 «Практика противодействия кибератакам и построения центров мониторинга ИБ», проходившем в ноябре в Москве.

«КИБЕРБЕЗОПАСНОСТЬ — ПРОДУКТ ВЗАИМОДЕЙСТВИЯ»

На фоне прочих конференций, связанных с ИБ, коих в России ежегодно происходит не один десяток, SOC-Форум 2017 выделяется качественным контентом и представительностью. Среди участников — представители регуляторов и главы служб кибербезопасности крупных кредитно-финансовых организаций, а именно: заместитель начальника Центра ФСБ России Игорь Качалин, заместитель директора ФСТЭК России Василий Лютиков, заместитель начальника ГУБиЗИ Банка России Артем Сычев, руководитель службы кибербезопасности Сбербанка Сергей Лебедь, заместитель генерального директора компании «Информзащита» Максим Темнов и др.

Особого внимания заслуживает пленарная часть, охватившая наиболее острые вопросы SOC-сферы. Ход дискуссии направляли и задавали неудобные вопросы генеральный директор



Среди участников — представители регуляторов и главы служб кибербезопасности крупных кредитно-финансовых организаций

Solar Security Игорь Ляпунов и главный редактор BISA Олег Седов.

На неловкие паузы и молчание времени не было. Участники рассказали о построении качественных SOC, обсудили массовые вирусы-шифровальщики, от которых пострадали как государственные, так и коммерческие структуры. Говорилось и о том, что череда массовых атак позволила выявить реальную готовность информационных систем банков, телеком-операторов и самих регуляторов к критическим ситуациям.

По мнению выступавших, основная проблема, которая может поставить под удар безопасность любой организации — это, прежде всего, «человеческий фактор». При этом речь

идет не только о сотрудниках, открывающих подозрительные файлы, но и о ИБ-специалистах, которые, к примеру, вовремя не обновили систему. Кроме того, таким же «фактором» может стать и руководство организации, не уделяющее соответствующего внимания системам киберзащиты. Тем не менее все согласились, что в этом году ситуация значительно меняется к лучшему. И немаловажную роль тут играет само государство. В частности, по словам Игоря Качалина, позитивные перемены сулит ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации», который был принят в июле 2017 года. При этом представитель ФСБ России заверил, что уже в ближайшее время будут приняты дополнительные законы, развивающие ИБ в более динамичном ритме.

Неоднократно отмечалось, что и с технической, и с организационной стороны есть все, чтобы обеспечить современный уровень киберзащиты и свести ущерб к минимуму или вообще исключить его. Артем Сычев рассказал о взаимодействии Банка России и ГосСОПКА, благодаря чему достигнута высокая скорость реагирования на угрозы: «В Центре мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) скорость обработки каждой угрозы в среднем составляет от 40 до 90 минут». Также

ФАКТЫ О SOC-ФОРУМЕ

- ◆ За 3 года количество участников выросло в 4 раза
- ◆ SOC-Форум — единственная в России конференция, полностью посвященная вопросам создания и эксплуатации центров мониторинга и реагирования на инциденты информационной безопасности
- ◆ SOC-Форум 2017 — самая масштабная конференция такого формата: 38 докладов, 9 сессионных заседаний, 23 выставочных стенда ведущих российских и мировых организаций по противодействию кибератакам
- ◆ Государственные регуляторы выступили с узконаправленными докладами и представили собственные стенды
- ◆ Среди участников — ИТ-компании, кредитно-финансовые организации, промышленные и образовательные структуры, операторы связи
- ◆ На Форуме присутствовали свыше 50 СМИ



В SOC-Форуме 2017 приняло участие более 1700 специалистов

представитель регулятора отметил, что сегодня SOCI являются реальным инструментом, способным помочь в борьбе с киберинцидентами.

По словам Сергея Лебеда, специалисты Сбербанка «стали видеть все атаки в реальном времени, своевременно принимать решения. В качестве показателя эффективности могу сказать, что от компьютерных атак простой банка в этом году были ноль минут... Мы видели попытки атак на какие-то элементы нашей инфраструктуры, но не центральной».

Конечно же, остается много вопросов, поскольку пока SOC все еще на-

ходится в стадии становления. «На сегодняшний день приходит только понимание того, что мы закладываем в SOC. Ещё не существует открытых процессов, подобных ITSM, ITIL в области ИБ и операционного управления безопасностью, поскольку мы пока не готовы. Пока мы пытаемся понять, как управлять этим, что такое операционная безопасность, что такое управление на стратегическом уровне. Современный SOC, с точки зрения технологий, это набор информационных систем (SIEM, Threat Intelligence-платформы), системы мониторинга и средства защиты. Однако пока они не связаны между

собой, и главный вопрос состоит в том, как объединить все эти компоненты», — продолжил руководитель службы кибербезопасности Сбербанка.

Конечно, пленарная дискуссия только разбудила аппетит к теме, хотелось копнуть еще глубже во время пресс-брифинга. Но, не знаю, к счастью или сожалению, эта часть мероприятия оставила больше вопросов, чем ответов. Наверное, поэтому все ожидания переориентировались на тематические сессии.

SOC В РОССИИ: ОТ ТЕОРИИ К ПРАКТИКЕ

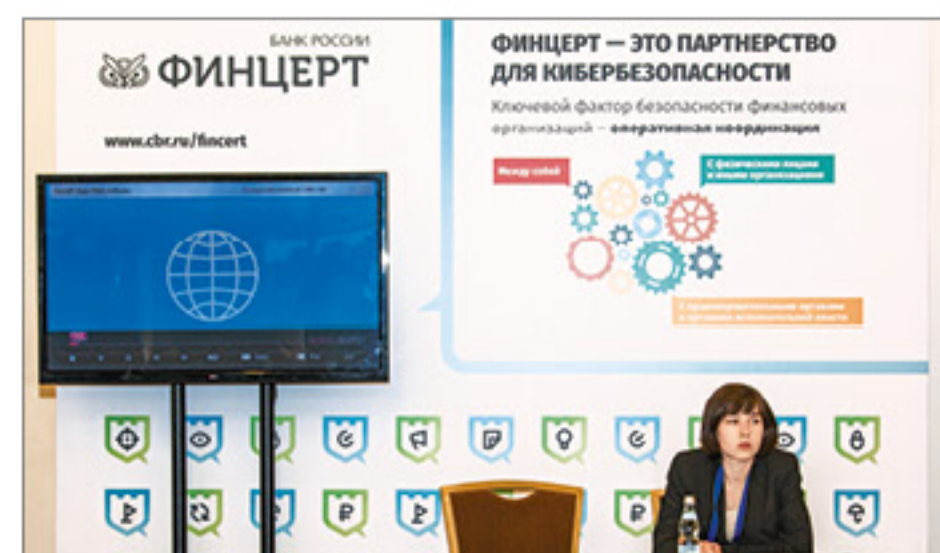
Тематическое меню сессий порадовало и даже поставило в тупик, уж очень сложно было выбирать между тремя параллельными потоками. В итоге, во всех залах не осталось ни одного свободного места.

Рассказать все, о чем удалось узнать, в коротком репортаже невозможно, поэтому остановлюсь на том, что особенно запомнилось. Сегодня SOC — это часть общего процесса управления кибербезопасностью наравне с управлением рисками, контролем утечек информации и управлением доступом. Большинство российских компаний, занимающихся построением SOC-центров, развивают эти процессы в рамках единой стратегии обеспечения информационной безопасности.

Большинство выступавших рассказывали о всевозможных вариантах решения текущих и будущих проблем ИБ и демонстрировали свои технологии и предложения, позволяющие повысить эффективность SOCa. Свой выход предложили в Solar Security. К примеру, интегратор проводит с заказчиком краткое исследование-инвентаризацию в формате бизнес-интервью, чтобы понять, как выглядит инфраструктура, что реально «болит», где хранится самое важное, где возможны проблемы. Данный подход позволяет не только понять систему работы организации, но и определить какие еще нужны подсистемы, кроме базовых. Параллельно подключаются стандартные подсистемы и накладывается карта сети, а также сценарии для получения статистики. Какой результат? Уже через месяц SOC начинает видеть только то, что хочет выявлять.



В демозоне были представлены 22 стенда лидеров отрасли ИБ, в том числе государственных структур: ГосСОПКА, БДУ ФСТЭК, ФинЦЕРТ



Много выступлений были посвящены опыту эксплуатации центров мониторинга. Даже дилетанты в области SOC смогли уйти отсюда с приличным багажом полезной информации. К примеру, заместитель начальника управления безопасности и защиты информации РосФинМониторинг Николай Белобров отметил, что соблюдение основных условий успешного внедрения SOC (компетенция, коммуникация, ответственность) позволит создать прозрачную и контролируемую систему, способную реагировать на атомарные инциденты безопасности.

Неоднократно обсуждался вопрос: строить собственный SOC или подключаться к внешней структуре? Так, в первом случае, заказчику всегда необходим быстрый старт, а интегратор готов выполнить проект за 3–5 лет. В итоге — в проигрыше все: «у нас нет SOC ни своего, ни внешнего».

Бывает и по-другому — внешний SOC запускает огромное количество ненужных сценариев. С чем это связано? Интегратор не видит цели, «лупит из пушки по воробьям», потому что сам заказчик не компетентен в том, что выбирает, не уверен в своих решениях.

Выступления ИБ-экспертов свидетельствуют: темпы развития киберзащиты в России связаны не только с новыми нормативными актами и законами, но и с общим осознанием того, что информационной безопасностью нужно заниматься серьезно, системно

выстраивая процессы. Иначе есть риск не только потерять инфраструктурные элементы, но и понести реальные финансовые убытки.

Из выступлений представителей госструктур стало понятно, что государство тоже думает и продвигает не только меры по борьбе с киберугрозами, но разрабатывает механизмы, позволяющие укреплять сферу ИБ, совершенствовать и строить что-то новое. Так, о деятельности центров ГосСОПКА и регулировании работы центров мониторинга киберинцидентов рассказал представитель ФСБ России Андрей Раевский. В рамках его доклада были четко обрисованы все практические шаги по построению центров ГосСОПКА, охарактеризованы ближайшие нововведения, необходимые для реализации Ф3-187.

Конечно, насколько полезными и практичными стали озвученные предложения и инициативы, мы сможем судить спустя время, и скорее всего, об этом мы поговорим на SOC-Форуме 2019.

СТЕНДЫ, СТЕНДЫ, СТЕНДЫ...

Пристальным вниманием присутствующих пользовались демонстрационные стенды. Впервые свои инициативы по информационной безопасности презентовали государственные структуры: ГосСОПКА, ФСТЭК, ФинЦЕРТ Банк России. Приятно, что здесь можно было подробно пообщаться по интересующим вопросам, получить полезные материалы. К примеру, на стенде ФСБ

России выдавали диски с методическими рекомендациями по ГосСОПКА, которых, кстати, в свободном доступе нет.

Positive Technologies и Solar Security презентовали совместное решение — систему управления инцидентами и взаимодействия с главным центром ГосСОПКА, а также программно-аппаратный комплекс, позволяющий создавать данные центры в минимальные сроки. Группа экспертов «Информзащиты» представила обновленный функционал SOC.

В общем, демонстрационная зона была не менее интересна, чем экспертные дискуссии: представленные ИБ-решения и услуги привлекли даже самых продвинутых и требовательных посетителей.

Если говорить в целом, то форум в очередной раз продемонстрировал серьезное отношение к вопросам информационной безопасности в стране и понимание, в том числе и государством, того, какие проблемы необходимо решать прямо сейчас. И хотя методы работы регуляторов порой вызывают определённые опасения как среди специалистов, так и у рядовых пользователей, готовность быстро реагировать на угрозы и обсуждать свои действия на подобных мероприятиях следует воспринимать скорее в положительном ключе.

RAIF 2017

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПЕРСПЕКТИВЫ И ДЕНЬ СЕГОДНЯШНИЙ

Российский Форум по системам искусственного интеллекта (RAIF) заслуживает внимания по многим причинам. Актуальная тема, достойный состав участников, известные компании, высокий уровень проведения... Приятно, как деликатный организатор, не выпячивая лишь собственные компетенции, предоставил гостям возможность напрямую пообщаться с теми, кто уже практикует технологии artificial intelligence, AI.

ВОСПОМИНАНИЯ О БУДУЩЕМ

Тональность Форуму задал Майк Вирт, IBM, который в своем выступлении настроил аудиторию на пару-тройку десятилетий упорной работы по развитию аппаратных, методологических и «софтверных» основ AI до того момента, когда эта технология в полной мере станет зрелой и превратится в действительно AI. Но докладчик убедительно доказал, что оно того стоит. Уже сегодня состоявшийся полёт изящной бабочки-робота в замкнутом пространстве явил пример той грандиозности чувств и, несомненно, пользы, которые AI обеспечит человечеству. Но это произойдет не скоро — после того, как суперкомпьютеры снизят мегаватты потребляемой им мощности до долей ватта, расходуемых, как полагают исследователи, живым мозгом при решении аналогичных задач.

Сочетание трезвого взгляда на AI с убежденностью в том, что дорогу осилит идущий, было присуще всем докладчикам. Сравнение ситуации в России с внедрением AI с аналогичными показателями в мире оказалось вполне ожидаемо не в пользу нашей страны. Однако состояние дел отнюдь не катастрофическое, методически отечественные исследователи и практики вполне себе на мировом уровне. Что касается практических, как часто гово-

рят, «кейсов», то тут дело в нынешних социально-экономических перекосах, не имеющих отношения к AI и даже к интеллекту вообще.

При этом случилось так, что наряду с первыми двумя обзорными выступлениями (докладчики — уже упомянутый г-н Вирт, IBM, и Владимир Молодых, «Инфосистемы Джет»), два доклада были сделаны «властью», заместителем председателя комитета Госдумы по информационной политике, информационным технологиям и связи Александром Ющенко, и «индустрией», представителем Yandex Data Factory Константином Горбачём.

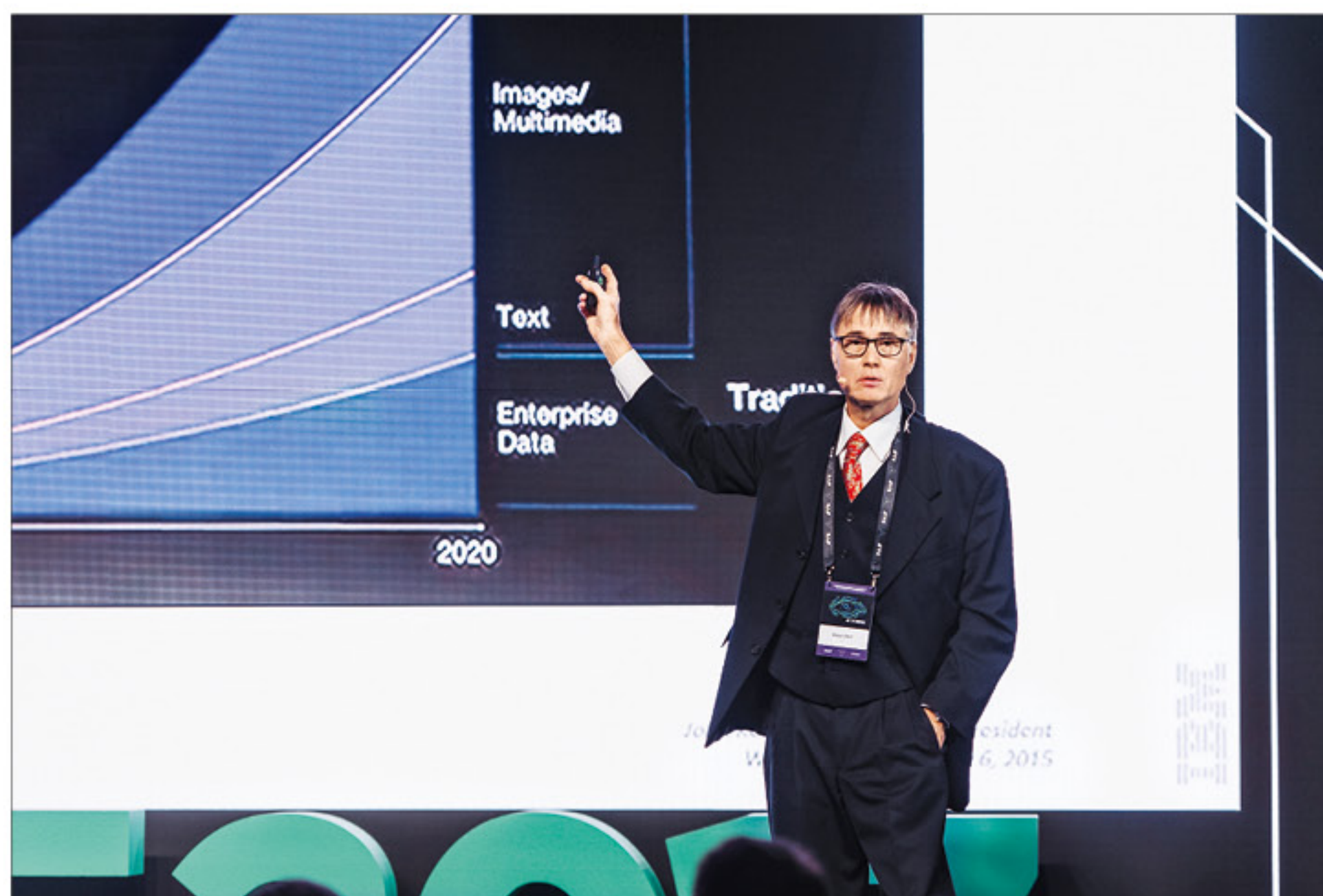
Yandex Data Factory представила доклад о промышленном внедрении элементов AI на металлургическом комбинате, предприятии золотодобычи и предприятии, относящемся к пищевой промышленности, а сообщение об успехах в производственном секторе отечественной экономики приятно во всех отношениях, тем более, когда речь идет об успехах интеллекта на производстве.

Приятное впечатление произвело и выступление представителя Госдумы. В нём прозвучала и искренняя заинтересованность в успехах по направлению AI в России, а также конкретные предложения в адрес организаторов форума по части представления резолюции по итогам форума с предложениями по поддержке работ в области AI.

БЫЛОЕ И ДУМЫ

Дискуссионная площадка форума собрала представителей компаний — лидеров по части внедрения AI в его нынешнем виде. Это розничная торговля, банковское дело, страхование, инвестиционный бизнес, кибербезопасность. При этом очевидно, что кибербезопасность сегодня — это головная боль всех.

В связи с дискуссией по теме «Machine Learning: технологический пузырь или насущная необходимость для бизнеса» уместно заметить, что её участники сочли необходимым отметить многообразие нынешних представлений о том, что является «внедрением AI» се-



годня. Спектр действительно широк: от машинной реализации алгоритмов регрессионного анализа и до технологий комплексной биометрической идентификации (по голосу, лицу, походке...), а также того, что сегодня называют технологиями Machine Learning (ML) и Big Data. Ну а наиболее радикальный пример «AI» привёл Рустэм Хайретдинов из InfoWatch, обратив внимание на работу сливного бачка.

Кстати, в каждой шутке, как известно, лишь доля шутки. «Умные» унитазы уже существуют, и в 2013 и 2016 годах в таких изделиях японской промышленности были обнаружены уязвимости, способные заинтересовать киберзлоумышленников. Последствия для пользователей могли весьма дурно пахнуть.

Представляя в более развёрнутом и серьёзном виде свои соображения о насущной необходимости AI, Рустэм Хайретдинов выразил надежду, что опасные производства благоразумно останутся под управлением интеллекта, подобного тому, что управляет биметаллическим предохранителем в электрической цепи.

А вот в области информационной безопасности технологии Machine Learning весьма актуальны. Обнаруженный здесь и сейчас код вредоноса может больше и не встретиться, но всё чаще он используется в модифицированном виде в последующих атаках, атаки изменяются, что называется, «на лету». В результате одним из аспектов ИБ становится борьба интеллектов злоумышленника и защиты в режиме реального времени. В связи с этим использование AI «реального времени» в кибербезопасности наиболее естественно и желаемо, тогда как в банках, страховых и инвестиционных компаниях с «задачами нулевого дня» пока могут справляться подходы к реализации интеллектуального машинного анализа в режиме off-line. Хотя и здесь не всё так однозначно.

Среди перечисленных руководителем департамента «Цифровой Банкинг» Банка УРАЛСИБ задач, которые его подчинённые хотели бы отдать на откуп AI, был и анализ в режиме «реального времени» настроения клиента по голосу, чтобы на запросы недовольных реагировать быстрее. В таком свете уместно



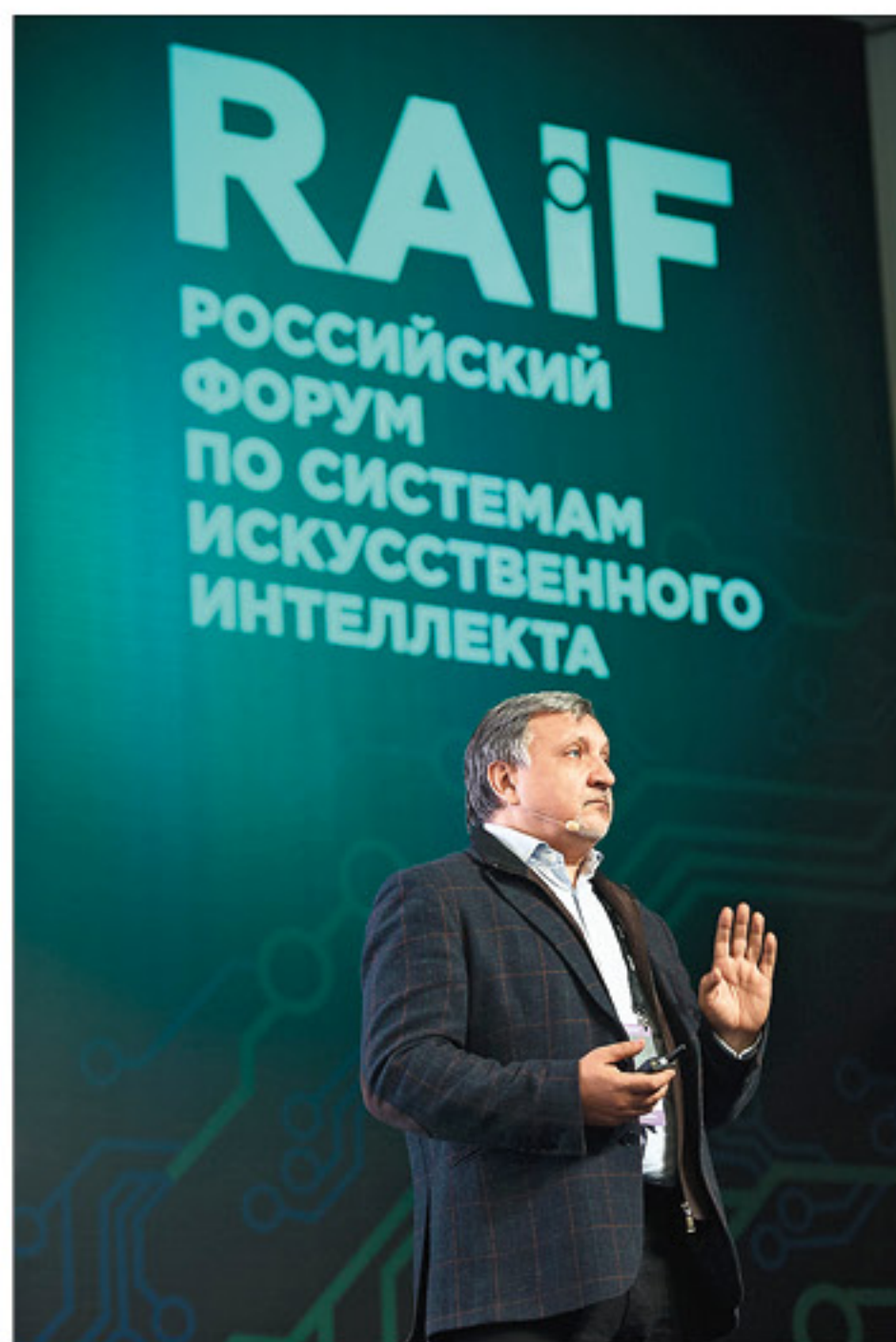
САМАЯ УСПЕШНАЯ РАЗРАБОТКА В ОБЛАСТИ AI НЕ СТАНЕТ УСПЕШНЫМ ВНЕДРЕНИЕМ БЕЗ ПОНИМАНИЯ, ЗА КЕМ — ЧЕЛОВЕКОМ ИЛИ МАШИНОЙ — ОСТАНЕТСЯ ПРАВО ОКОНЧАТЕЛЬНОГО ВЫБОРА

заметить, что самая успешная разработка в области AI не станет успешным внедрением без понимания, за кем — человеком или машиной — останется право окончательного выбора, особенно в режиме работы в реальном времени. Этот режим работы является штатным для специалистов по информационной безопасности. Таким же штатным, как работа отделов ИБ в режиме нехватки кадров. Нехватки, обусловленной не только общеотраслевыми проблемами кадрового «голода», но и проблемами подхода к определению численности персонала ИБ, исходя из оценки «среднего уровня» ожидаемых угроз. В момент атаки нагрузка на персонал службы ИБ вполне естественно превосходит оценочный средний уровень. В этой ситуации искусственный интеллект системы кибербезопасности организации способен подставить «плечо» живым людям. Этот аспект актуальности внедрения AI в технологии ИБ был обсуждён в докладе «Заменит ли ML офицера информационной безопасности?» на секции «AI в банках».

AI И МИР

Участники RAiF 2017 затронули не только технические и методологические проблемы построения систем AI и выгоды, которые они сулят, а их прототипы — приносят. Обсуждались и социальные эффекты от появления систем AI. Доклад «Заменит ли ML офицера информационной безопасности?» на секции «AI в банках» — это лишь звоночек о малой толике проблем, с которыми столкнётся общество, использующее системы AI.

На пленарной части были озвучены, представлены на экране в письменном виде и, полагаю, остались в памяти участников три высказывания. Одно из них — Илона Маска — прямое указание на угрозу обществу со стороны AI. Второе — пояснение Марка Цукербергера о причинах приостановки одного из проектов по AI в его компании. Эта причина связана с тем, что «искусственный интеллект» пошёл своим путём, который пока остается непонятым родителями, и озадаченные родители предпочли взять таймаут.



Ну а третья цитата уже перестала быть таковой и превратилась в крылатую фразу, широко используемую политическим истеблишментом в части утверждения, что первый, кто покорит вершину AI, станет властелином мира.

В связи с этим вспоминается гонка атомных проектов, в результате которых никто не стал властелином мира, а МАГАТЭ, как реактивный отклик на понимание этого обстоятельства, не смогло ни остановить распространение ядерного оружия, ни правильно оценить плюсы и минусы ядерной энергетики.

Минусы AI ещё только предстоит оценить.

Но уже сейчас в качестве сухой оценки речь идёт о перспективах безработицы около 2 млрд человек во всём мире. Внутренняя кухня этих расчётов не была раскрыта на Форуме, но ужасает уже то, что результат выгод от AI оценивается в количестве безработных, а не в часах сокращения рабочего дня,

увеличении отпусков, освобождении замужних женщин от работы с предоставлением социальных гарантий.

Другой потенциально опасный аспект AI — это использование его в кибероружии. В этом случае подлётное время Першингов, Искандеров и Курьеров отойдёт на третий план в той группе угроз, что способны развязать войну на взаимное уничтожение.

Поэтому в свете вялотекущей агонии МАГАТЭ, ЮНЕСКО и ООН одной из текущих задач, решаемых разработчиками AI, должны стать и проекты по оценке социальных последствий таких разработок.

ВМЕСТО ЭПИЛОГА

Что показал Форум? Во-первых, способность российской компании собрать пул заинтересованных партнёров и провести на высоком методическом уровне научно-техническую конференцию по актуальной проблематике. При этом, наряду с вдумчивым подбором тем, докладчиков

и участников, организаторы создали и весьма лаконичную, но выразительную зрительную атмосферу площадки hi-tech Форума.

Во-вторых, RAiF убедил, что в перспективе станет центром кристаллизации экосистемы разработчиков и пользователей AI, широко взаимодействующим с отечественной властью и зарубежным сообществом своих коллег.

Тем более, что заместитель председателя комитета Госдумы по информационной политике, информационным технологиям и связи Александр Ющенко, подчеркнув необходимость развития технологий AI как для бизнеса, так и для государства в целом, отметил: «Государство сегодня заинтересовано в развитии ИТ, в поддержке перспективных молодых специалистов, стартапов и, конечно, российских ИТ-компаний и интеграторов. Мы должны сегодня создать все условия, чтобы наши специалисты приносили максимальный результат. Им в поддержку мы разрабатываем законодательные акты в области новых перспективных технологий. Однако совершенствование данного направления возможно лишь при объединении усилий государства и бизнеса».

МИНУСЫ AI ЕЩЁ ТОЛЬКО ПРЕДСТОИТ ОЦЕНИТЬ. НО УЖЕ СЕЙЧАС В КАЧЕСТВЕ СУХОЙ ОЦЕНКИ РЕЧЬ ИДЁТ О ПЕРСПЕКТИВАХ БЕЗРАБОТИЦЫ ОКОЛО 2 МЛРД ЧЕЛОВЕК ВО ВСЁМ МИРЕ

ZERONIGHTS 2017

ЧУЖИЕ ЗДЕСЬ НЕ ХОДЯТ

У пруго надвигающийся с экрана на зал киборг с бейсбольной битой на плече и тяжёлый рок в живом исполнении стали первыми предвестниками того, что на конференции ZeroNights 2017 будет круто.

Последние сомнения по этому поводу развеял открывший конференцию один из её основателей, обозначивший вехи взросления мероприятия. По его словам, эти вехи включали и «изгнание бейсбольными битами» со сцены ныне признанного гуру отечественного рынка ИБ, и быстрое обретение морального превосходства над «бумажными» ИБэшниками. Также было заявлено, что сегодня кибербезопасностью должны заниматься лишь те, кто сам пишет код, а остальные могут идти лесом. «Идти лесом» — не прямая цитата, а скорее выражение настроения выступавшего. В общем, в качестве зачина было заявлено, что «Ночь Разрешения Проблем Нулевого Дня» (возможно именно так допустимо перевести название мероприятия) — это круто, международно и для практиков.

ДЛЯ ПРАКТИКОВ

То, что ZeroNights 2017 для практиков, стало понятно сразу после ознакомления с программой. Упоминание в тезисах докладов рисков и проблем, которыми пестрят сегодняшние заго-

ловки ИТ- и деловых изданий в разделах, посвященных кибербезопасности, и упоминание современных технологий и продуктов, эти риски и проблемы генерирующих, с очевидностью указывало на полезность мероприятия.

Ещё одним признаком практичности был внешний вид некоторых демонстрационных стендов, на которых к современным компьютерам с помощью нескольких проводов, двух-трёх скруток и пары плевочков были подключены столь же современные платы, а ребята, кучкующиеся рядом, с помощью компактных ноутов, пристроенных на колёсиках, всё это исследовали и «ломали» в режиме реального времени.

Более того, пользу смогли почерпнуть не только практики в области кибер-, но и практики по просто безопасности просто некоторых физических объектов, а именно дверных замков и автомобилей. Про автомобили было прямо заявлено в тезисах конференции, а что касается замков, то в руках посетителей демонстрационных стендов не раз мелькали обычные замки и инструменты, представленные на Youtube в роликах типа «вскрыть за минуту».

МЕЖДУНАРОДНО

То, что ZeroNights 2017 — это международно, было понятно и по фамилиям спикеров, и по тому, как свобод-

но перемежались доклады на русском и английском языках без сопровождения переводом. А в кулуарах при знакомстве немало молодых людей честно признавалось, что не говорят по-русски.

Ложку дёгтя в международность пролила программа пленарки, которую по большей части отдали иностранным спикерам, так что иной раз казалось, будто ты в Лондоне или Лас-Вегасе, а не в Москве. Иногда спикеры забывали о золотых правилах, сформулированных для подобных конференций ещё более полувека тому назад (например, «Не забывайте о слушателях, работайте над культурой публичных выступлений!» или «Уровень выступления рассчитывайте на среднего слушателя, а то многие молодые специалисты выступают так, будто объясняют что-то Оппенгеймеру, Зейтцу или Милликену...»).

АКТУАЛЬНО

Собственно научно-техническая часть конференции открылась докладом о том, что сегодня называют искусственным интеллектом (ИИ), и как это применяют в сфере ИБ. Доклад был и научным, и техническим, и практичным. Томас Даллиен не только раскрыл тему исторически, заострив внимание слушателей на научной основе проблемы, но ещё и дал критический обзор современных возможностей ИИ.





Основания для скепсиса по отношению к последним кроются в недостатке вычислительных мощностей (ну, не хватает их, чтобы ИИ сравнялся с человеческим мозгом), и, что важнее, в слишком прямолинейных приёмах технологий машинного обучения (Machine Learning, ML). В результате логика нынешнего ИИ — это логика шаблонно мыслящего «троечника», тогда как компьютеры атакуют нестандартно мыслящие мотивированные личности.

Менее экзотичны, чем ИИ, и уже получили широкое распространение технологии виртуализации, используемые, в том числе, и для обеспечения ИБ киберсистем. Тем не менее, и эта технология, как и некоторые другие, созданные во благо, имеют свою обратную сторону, открывая при некоторых обстоятельствах злоумышленникам дорогу к конфиденциальным данным. На конференции были затронуты актуальные вопросы о подводных камнях технологии виртуализации в контексте возможной компрометации конфиденциальных данных. Проблематика, безусловно, актуальна, а рекомендации — полезны, особенно в связи с развитием предложений облачных сервисов. Будучи осведомлёнными о рисках для пользователей, создатели «облаков» смогут предложить пути их устранения, а потенциальные клиенты облачных сервисов — трезво оценить допустимые сферы их применения в публичном и частном вариантах.

Существенной рамочной проблемой является и использование поставщиками (исключительно в интересах бизнеса!) урезанных вариантов базовых ИТ-технологий, когда «обрезанию» подвергаются элементы, ответственные за кибербезопасность конечного оборудования. Эта тема была затронута одним из отцов-основателей ZeroNights Алексом Матросовым в конкретном практическом приложении к проблеме безопасности прошивок UEFI.

Алекс также рассказал о том, насколько полезно для ИБ не забывать об аппаратных возможностях «железа». Эту тему впоследствии докладчики затрагивали не раз.

Подтверждением того, что ZeroNights идёт в ногу со временем, стали доклады и практические занятия, посвященные безопасности мобильных Android-устройств, оборудованию на основе плат для встраиваемых систем, возможностям процессоров с архитектурой ARM, киберзащите в Web-пространстве и многому другому.

А О НАБОЛЕВШЕМ?

В целом ZeroNights 2017 действительно представила практический взгляд на актуальные проблемы ИБ киберсистем, от компьютеров, серверов и Web-приложений компаний до автомобилей и дверных замков частных лиц. Обескураживает лишь то, что количество вопросов в данной сфере столь велико, что их «с верхом» хватило на два дня мероприятия. И нет сомнений, что да-

леко не все киберриски нашли на нем своё отражение.

В связи с этим позволю провести аналогию. Сегодня кибербезопасники-практики, «умеющие писать код», напоминают бригаду ремонтников-коммунальщиков, обслуживающих дом, построенный без проекта. Нулевой цикл — фундамент — заложен «на глазок», стены также возведены на основе «визуальной координации», инженерные коммуникации смонтированы бессистемно...

Все это, естественно, приводит к перманентным ремонтам, подгонкам, сварке «по месту» в условиях, когда дом уже сдан в эксплуатацию и частично заселён. В таких условиях безработица практикам ИБ, конечно, не грозит. Однако зарубежные коллеги уже ведут работы по «геоподоснове» и научному проектированию новой комфортной и безопасной ИТ-среды для пользователей. В ней «угроз нулевого дня» будет гораздо меньше.

Было бы интересно узнать о планах ZeroNights-комьюнити принять участие в подобных работах или, возможно, о намерении провести собственное проектирование.

Если организаторам конференции есть что сказать по этому поводу, может, стоит зарыть топор войны с «бумажниками» и на будущих «Ночах Разрешения Проблем Нулевого Дня» поговорить об этом?

Я уверен.

Решения С-Терра надежно защищают
сеть моего банка.



Преимущества сетевой защиты С-Терра:

- Защита всех участков сети: от банкомата до ЦОД
- Использование мировых стандартов IKE/IPsec
- Соответствие ГОСТ и СТО БР ИББС
- Сертификация ФСБ России и ФСТЭК России
- Отсутствие зависимости от поставщика оборудования
- Защита подключения к СМЭВ
- Высокая экономическая эффективность продуктов
- Качественная, оперативная служба техподдержки



TERADATA ФОРУМ 2017

КТО СОСТАВИТ КОНКУРЕНЦИЮ БАНКАМ?

Кто составит конкуренцию банкам в ближайшее время? Этот вопрос, заданный в ходе пленарной дискуссии на TERADATA Форум 2017, привёл зал в лёгкое замешательство. Ведь очевидно, что лучше гор могут быть только горы, а конкурировать с банками могут только банки.

КОНКУРЕНТЫ ЕСТЬ

Ричард Лиу, вице-президент банка Wells Fargo, посетовал в своем выступлении, что ныне принадлежность к сообществу банковских сотрудников уже не является эффективным инструментом завоевания девушек и их родителей. Ныне «королевским» активом банка становятся уже не деньги, а данные, а принципы банковского обслуживания теперь «клиентоцентрические», тогда как ранее они были «операционно-центрическими». В общем, полный Банкинг 4.0 на базе Big Data и максимальное «облизывание» уже завоёванных клиентов. При этом KPI сотрудников кредитной организации больше не привязан к количеству операций или счетов клиентов.

И, тем не менее, вопрос о возможном существовании конкурентов у банков, заставил Ричарда Лиу взгрустнуть, после чего он признался, что уже есть претенденты на самых «сливочных» клиентов его организации, и претензии этих злодеев подкреплены как раз обладанием множеством данных о таких клиентах.



После этого микрофоном завладел Стивен Бробст, главный технический директор корпорации TERADATA, который сообщил слушателям, что одна из социальных сетей уже получила лицензию на финансовую деятельность, и её успех на этом поприще весьма вероятен. И опять же вследствие того, что сеть обладает исчерпывающей информацией о членах своего сообщества на основе технологий Big Data.

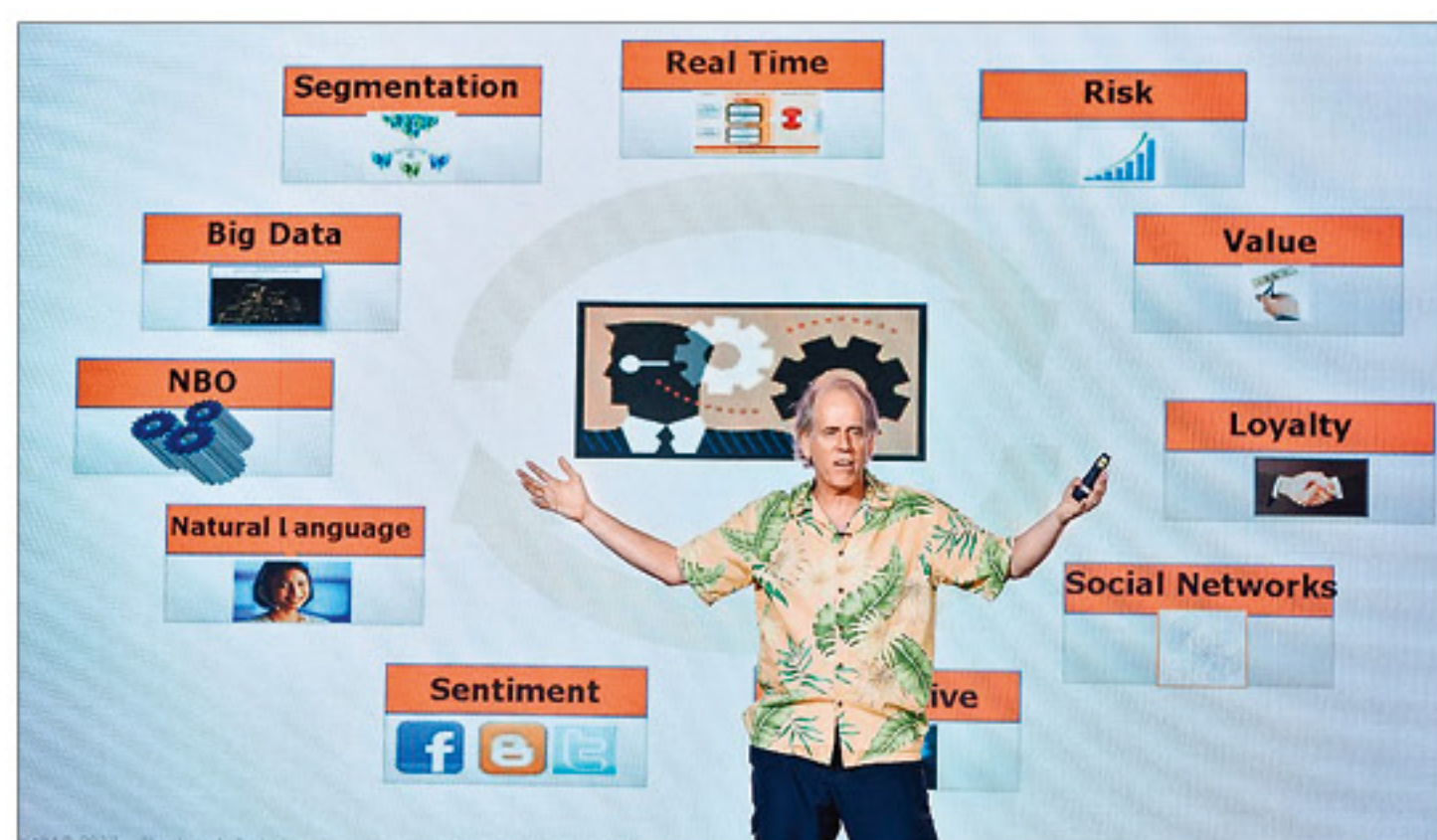
БОЛЬШИЕ ДАННЫЕ В ФОКУСЕ

Банки традиционно стали первопроходцами в освоении технологий Больших Данных, поэтому не удивительно, что клиентская аналитика (в BNP

Paribas, VISA и других организациях) была ядром секционных заседаний конференции.

Однако впервые представленная секция Индустрия 4.0 и модная нынче Цифровая Экономика также предъявили интересные практические примеры применения Больших Данных. Например, для повышения собираемости налогов, обеспечения безопасности на транспорте, эффективности логистики и перевозок.

Уместно заметить, что достаточно чёткий хронометраж выступлений и обсуждений позволял участникам составить интересную программу посещения докладов на разных секциях





и получить объёмную картину практической полезности Больших Данных.

Взвешенное сочетание в докладах прогнозов и положительной практики по части использования Больших Данных позволяют утверждать, что принятый ныне набор метрик данных в виде конфиденциальности, целостности, доступности следует дополнить такими характеристиками, как полнота и степень использования. Требования к полноте должны определяться экспертами, а степень использования — зрелостью систем аналитики и поддержки принятия решений.

Интересной проблемой становится обеспечение конфиденциальности данных. Теперь ей угрожают не только злоумышленники внешние и внутренние. С ростом числа социальных сетей и повышением уровня их оснащённости системами сбора данных и аналитики понижается общий уровень приватности частной жизни. Причём фактически с помощью самих же участников социальных сетей, сообщающих сведения не только о ФИО, месте рождения, образовании и т.д., но и в реальном времени — о своём социальном окружении, интересах, географии отпускных перемещений и прочем. Эти данные, подкреплённые сведениями те-

леком-компаний и обработанные аналитическими системами, позволяют получить полезнейшую информацию для финансовых организаций, ритейла. О Большом Брате упоминать не будем, отдавая это на откуп конспирологии.

Описанная ситуация хорошо ложится на ту, что описал в своём докладе главный технический директор корпорации TERADATA, когда рано или поздно маржинальность телекома за счёт бизнеса предоставления услуг связи обратится в нуль, и единственной ценностью компаний станут данные о клиентах. Г-н Бробст деликатно обошёл вопрос о моральных аспектах монетизации этого актива, но нам следует задуматься и об этом.

КОМУ ОНИ ПРИНАДЛЕЖАТ?

Впрочем, в отличие от Стивена Бробста зал был менее деликатен. Ещё в ходе дискуссии после первой части пленарного заседания (доклады главы TERADATA в России Андрея Алексеенко и профессора бизнес-школы Said Оксфордского университета Эндрю Стивена) был задан вопрос о судьбе приватности личной жизни.

Интерес вполне закономерный после рассказа г-на Стивена о том, как всем известная косметическая компа-

ния через своё приложение для смартфонов частой гребёнкой вычёсывает данные о внешнем облике и косметических предпочтениях заказчиц. Включая и тех, кто выбирает товары бюджетного ценового диапазона.

В связи с этим Андрей Алексеенко предположил, что в недалёком будущем на эту тему будет разработано что-то вроде договора между обществом и компаниями.

А вот в промышленности вопрос о принадлежности данных уже, похоже, решён. Рассказав о решении Siemens RAILIGENT для управления железнодорожными активами (подвижным составом, железнодорожными путями, контактной сетью), докладчик упомянул, что все собранные данные являются собственностью заказчика, и он может их получить. Однако модели и алгоритмы обработки этих данных и их анализа — это ценное ноу-хау Siemens.

Благодаря инициативе корпорации TERADATA около 500 гостей форума (руководители крупных компаний, эксперты в области бизнес-аналитики, ИТ-специалисты и специалисты в области Data Science) смогли обозреть с разных сторон проблемы обладания Большими Данными, получить консультации у людей, отчасти решивших эти проблемы и трансформировавших Big Data в ценный актив. Можно сказать, что 14 ноября 2017 года человечество сделало ещё один шаг к освоению технологий Big Data.

**НЫНЕ «КОРОЛЕВСКИМ» АКТИВОМ
БАНКА СТАНОВЯТСЯ УЖЕ НЕ
ДЕНЬГИ, А ДАННЫЕ, А ПРИНЦИПЫ
БАНКОВСКОГО ОБСЛУЖИВАНИЯ
ТЕПЕРЬ «КЛИЕНТОЦЕНТРИЧЕСКИЕ»**

ANTIFRAUD RUSSIA 2017

ИНТЕЛЛИГЕНТНЫЕ ДИСКУССИИ О РАЗБОРКАХ ПО ПОНЯТИЯМ

Русско- и англоязычное названия мероприятия — VIII Международный форум по борьбе с мошенничеством в сфере высоких технологий AntiFraud Russia — не следует трактовать слишком уж буквально ни на одном из упомянутых языков. На конференции не сказали ни слова о мошенничестве, например, в нанотехнологиях или, скажем, в ядерной медицине. Однако и термин «fraud» слишком узок для того, чтобы в полной мере охарактеризовать круг тем, затронутых на мероприятии.

ЩИТ И МЕЧ

Эксперты и гости форума обсудили не только мошенничество в финансовой сфере и способы борьбы с ним, но гораздо более широкий круг тем, касающихся кибербезопасности, от прорех в законодательстве до блокчейна и искусственного интеллекта.

Широта спектра обсуждений связана с тем, что в нынешнем киберпространстве обитают не только мошенники, но и киберфорточники, взломщики банкоматов и грабители секретных файлов. Их технологическое оснащение перестало быть уделом ремесленников, а превратилось в одну из областей высокотехнологичного и пока, похоже, безнаказанного бизнеса. Возможно, именно эти обстоятельства заставили организаторов форума сформулировать тему панельной дискуссии («Эволюция «щита» и «меча»: что меняется быстрее?») в том ключе, что киберпреступники обладают разящим «мечом», а в руках противостоящих им имеется лишь «щит» — пассивный инструмент защиты.

НАШЛЕПКА ИЛИ ИММУНИТЕТ?

На ущербность такого подхода сразу обратили внимание и ведущий панельной дискуссии Борис Мирошников и эксперт Василий Окулесский. Они аргу-

ментировано обосновали, что пришло время киберинфраструктуры, имеющей «природный иммунитет», а не прикрытой от злоумышленников внешними накладками.

Позже на одном из круглых столов, посвящённом технологии блокчейн, дискуссия на эту тему была продолжена. Уместно отметить, что обсуждение блокчейна на форуме резко контрастировало с тем хайпом, который, как выразился эксперт «Лаборатории Касперского» Алексей Маланов, доносится сегодня «из каждого утюга». Был проведён дотошный SWOT-анализ технологии и критически проанализированы возможности ее применения вне сферы генерации электронных денег.

А ИНОГДА НЕ РАБОТАЮТ ЗАКОНЫ...

Из обсуждения практики правоохранительных органов следует, что рост киберпреступности и рост ответных реактивных действий идут «ноздря в ноздю» в процентном исчислении. Однако процентные успехи правоохранительных органов — это следствие низкой начальной базы этих успехов, а вот выявленные преступления — это лишь верхушка айсберга, масштабы подводной части которого не поддаются точной оценке.

Иногда преступники аккуратно зачищают после себя «поляну». Иногда жертвы не спешат «выносить сор из избы». Иногда образованные киберпреступники не переступают «красные флажки» Уголовного кодекса. А иногда не работают законы...

В ходе дискуссии был поднят вопрос о реакции на противоправные действия, которые были выявлены и пресечены службой ИБ банка. По таким инцидентам у несостоявшейся жертвы может иметься информация, способная пролить свет на личность киберпреступника. Но будут ли правоохранительные органы заниматься расследованием в такой ситуации?

Откровением показалось заявление о том, что преодоление несовершенства законодательства позволило бы предотвращать последствия кибератак по принципу Рикки-Тикки-Тави, а именно — давить гадов в зародыше. Руководитель Департамента по управлению фродом ОАО «Мегафон» сообщил, что у операторов телекома есть возможность оперативно отключать управляющие сервера киберпреступников и блокировать их СМС-рассылки. Но закон запрещает операторам самостоятельно отключать Интернет-ресурсы... И так же закон стоит на страже тайны переписки.

КВАЛИФИКАЦИЯ ПЕРСОНАЛА ИБ

Была озвучена ещё одна не техническая проблема борьбы с киберпреступностью — несовершенство внутренних регламентов по ИБ и недостаток квалификации сотрудников.

В ходе диалога между руководителем Службы ИБ Сбербанка и начальником ФинЦЕРТа Банка России была озвучена ситуация, в которой Сбербанк своевременно выявил киберугрозу, а ФинЦЕРТ сразу разослал соответствующее уведомление о ней. И, тем не менее, несколько банков понесли многомиллионные потери... из-за неосторожности или служебного несоответствия сотрудников ИБ, не среагировавших на уведомление.

Нельзя утверждать, что вопросы квалификации персонала не находят понимания. На форуме этой теме были посвящены как минимум два мероприятия. Но проблемы с количественным составом служб ИБ и организационной дисциплиной остаются. Один из подходов к их решению — использовать то, что «лирики» называют искусственным интеллектом, а «физики» — автоматизацией и машинным обучением. Приятно удивило, что эти технологии обсуждались в том объёме, который соответствует их реальному уровню развития.



ГЛАВНЫЙ ИСТОЧНИК РИСКОВ

Был озвучен и бессмертный тезис о том, что главный источник рисков для ИБ — человек.

Обычно после ритуального произнесения слов о человеческом факторе и социальной инженерии начинаются пространные рассуждения о безрассудствах клиентов, играющих на руку киберпреступникам. Реже «под раздачу» попадают сотрудники организаций, ставшие жертвами той же социальной инженерии. И совсем редко говорят о топ-менеджерах, которые сэкономили на инфраструктуре и персонале, а утвердив своим росчерком высосанные из пальца KPI, фактически вынудили подчинённых совершать вредные для безопасности бизнеса действия.

ПОРА ПРИЗНАТЬ!

Однако пришла пора открыто признать, что человеческий фактор как источник киберугроз — это совокупные и неосознанно системные действия сразу нескольких групп людей. В том числе и отличающихся пониженной социальной ответственностью разработчиков «кривых» приложений, а не только потребителей этого дешёвого или «бесплатного» киберширпотреба.

Причём одни потребители с энтузиазмом, достойным лучшего применения, скачивают что ни попадя в XYZ-Stores, оттачивая до автоматизма навыки клика на кнопках «ОК» и «Принимаю», а другие используют «сырые» разработки для окучивания клиентов.

В кулуарах форума услышал рассказ, как сотрудник известного банка,

оформляя пенсионную карту клиенту, установил на его смартфон приложение, которое банк считает необходимым предлагать в составе своей пенсионной услуги. В результате была фатально нарушена работа другого банковского приложения — действительно необходимого.

Этот инцидент ставился в вину сотруднику банка, дисциплинированно работавшему на свой KPI. Тогда как первопричина зла в этой ситуации — синергия некачественной разработки навязанного приложения и экономии банком на этапе его испытаний.

По уму лидер банковского рынка должен был проверить совместимость навязываемого им ПО с разными смартфонами и сформулировать требования к их допустимым конфигурациям. Понятно, что задача эта затратная, и банк попросту сэкономил.

Приведённый пример призван проиллюстрировать утверждение, что подброшенные флэшки с .exe-файлами и электронные письма с обязывающими к действиям темами — это лишь «надводная часть» зловерной для кибербезопасности социальной инженерии, истоки которой находятся в том числе и в пониженной социальной ответственности разработчиков казалось бы «рутинных» клиентских продуктов и сервисов.

В результате круг виноватых и потерпевших замыкается, и далее киберпреступники заваливают эту «связанную одной цепью» толпу своими инфицированными SMSками, электронными письмами и программами из интер-

нет-магазинов приложений, и зараза распространяется «воздушно-капельным путём»: по сетям и при прямых контактах инфицированных флэшек с USB-разъёмами здоровых ПК.

Впечатления от AntiFraud Russia 2017 (вкупе с другими последними ИБ-мероприятиями) позволяет утверждать, что отечественная экосистема трудовых ресурсов в области ИБ — это взболтанный, но пока ещё недостаточно смешанный коктейль из странствующих рыцарей с заплечными мешками с парой ноутбуков, готовых по первому зову «заштопать» любую «дыру» в системе безопасности ИТ-инфраструктуры, и тех специалистов, которые понимают, что «чисто не там, где убирают, а там, где не мусорят».

Энтузиазм «рыцарей» ИБ заслуживает уважения, но иногда складывается впечатление, что их сообщество скатывается в ИТ-троцкизм, для которого «движение всё, конечная цель — ничто». Тогда как системный подход к повышению культуры проведения ИТ-разработок и их внедрения способен в зародыше подавить многие предпосылки к киберинцидентам. И сыграть решающую роль в формировании такого системного подхода призвана собравшаяся на конференция AntiFraud 2017 интеллигенция ИБ, чей аккуратизм способен переломить эпидемиологическую ситуацию в ИТ-сфере в лучшую сторону.

КАК ПОВЫСИТЬ?

ГЛАВА 3. ПОВЫШЕНИЕ ОСВЕДОМЛЁННОСТИ ПЕРСОНАЛА В ОБЛАСТИ ИБ СВОИМИ СИЛАМИ

(Продолжение. Начало
в № 3,4/2017)

«**О**сведомлённость повышать надо, кто ж спорит... Но «кем» это делать?» — мало что может скрасить безрадостные раздумья ИБ-руководителя над этим вопросом. В его ИБ-подразделении 2,5 человека, одновременно и непрерывно занимающиеся всем спектром ИБ-вопросов. А сунься к руководству с предложением закупить необходимые услуги «на стороне» — тут надо быть очень готовым к встречному вопросу «а ты на что?».

Предмет этой главы — можно ли повысить осведомлённость персонала в области информационной безопасности «собственными руками»? Или надо непременно звать платных консультантов, которые уверяют, что всё сделают лучше и за вас?

Не будем ходить вокруг да около: осведомлять персонал своими силами, разумеется, можно и, более того, нужно. А в некоторых организациях, где понимающий полезность повышения «безопасник» не находит должной поддержки, это вообще единственный путь хоть как-то минимизировать «человеческий фактор» при обеспечении ИБ.

ТРУДНОСТИ

Однако, если вы задумали действительно решать задачу повышения культуры обеспечения информационной безопасности персоналом (не для «галочки» или прохождения ближайшей проверки), надо быть готовым к тому, что дело это непростое. Потому что надо будет:

♦ Самому хорошо понимать что и как делать, знать методологию выполнения проектов по повышению осведомлённости и чужой опыт их реализации. Не только потому, что многое вам придётся делать самому, но ещё и потому, что в данном случае вам

очень пригодится «тактика быстрых побед» — пока вам дают что-то делать, нужно быстро показать, что вы делаете это эффективно и позитивный результат налицо. В противном случае вполне возможно, что первая ошибка станет последней: ваше самоотвлечение от «стандартных» активностей «безопасника» будет быстро признано нецелесообразным.

♦ Быть хорошим «маркетологом» проекта по повышению осведомлённости персонала. Проекты по повышению — это проекты масштаба всей организации, вам не сделать их в одиночку, а потому будут нужны авторитетные коллеги-руководители, с пониманием относящиеся к вашим усилиям, и если не помогающие, то хотя бы не мешающие.

♦ Быть ещё и хорошим руководителем проекта: иметь достаточный для реализации проекта объём ресурсов и правильно спланировать работы для достижения нужных результатов. В данном случае вам придётся не только руководить, но и многое делать самому. При этом ответственность за результат остаётся на вас. Поэтому, с одной стороны, важно, чтобы ваших ресурсов (рук, времени, средств) хватило для реализации комплекса мер по повышению, а по итогам реализации проекта получился значимый с точки зрения бизнеса результат (как мы помним по предыдущим статьям, повышение должно быть многоканальным, поголовным и адаптированным под условия проведения; если вы сде-

лаете презентацию с наспех сформулированными тезисами и надёрганными из интернета картинками и выложите её на интранет-портал с просьбой «всем прочитать» — эффективность такого повышения будет нулевой). Не исключено, что вам придётся доказывать руководству, что вы не зря потратили время и силы (причём, и сотрудников других подразделений), и ваши аргументы должны быть убедительными.

ВЫГОДЫ

Самостоятельно реализовывать меры по повышению осведомлённости в некоторых аспектах даже более выгодно и продуктивно, нежели в сотрудничестве с подрядчиком:

♦ Не придётся тратить силы и время на объяснение подрядчику текущих условий реализации проекта, специфики функционирования вашей организации, идей и требований к результатам проекта. Далеко не каждый подрядчик способен делать не так, как ему удобнее, а так, как нужно именно в ваших конкретных условиях.

♦ Вы не так «зажаты» проектными рамками и можете реализовывать меры по повышению практически в удобных вам манере и темпе. Однако, здесь есть опасность настолько растянуть повышение осведомлённости во времени, что его эффект будет близок к нулю.

С другой стороны, как известно, некоторые вещи лучше делать чужими руками. Проекты повышения осведомлённости имеют выраженную органи-

ВАМ ОЧЕНЬ ПРИГОДИТСЯ «ТАКТИКА БЫСТРЫХ ПОБЕД» — ПОКА ВАМ ДАЮТ ЧТО-ТО ДЕЛАТЬ, НУЖНО БЫСТРО ПОКАЗАТЬ, ЧТО ВЫ ДЕЛАЕТЕ ЭТО ЭФФЕКТИВНО



зационную составляющую — если вы не обладаете в организации достаточным политическим весом, не уверены в успехе и не готовы отстаивать проект и его результаты перед руководством и иными подразделениями, возможно, будет проще поручить реализацию проекта методологически «подкованному» подрядчику с профильным опытом.

И ДЕШЕВЛЕ?

Здесь мы умышленно не относим к выгодам «дешевле», ибо считаем, что дешевизна повышения собственными силами по сравнению с привлечением подрядчика:

- ♦ Во-первых, неочевидна, учитывая совокупные прямые и косвенные затраты организации: внутренние ресурсы не являются бесплатными, а их отвлечение на повышение в ущерб другим, подчас не менее приоритетным задачам, может повлечь потери, многократно превышающие затраты на проект повышения и эффект от него;

- ♦ Во-вторых, для проектов по повышению осведомлённости работает правило «дёшево не значит хорошо (эффективно)»: эффективное повышение осведомлённости предполагает создание комплексной программы, включа-

ДЛЯ ПРОЕКТОВ ПО ПОВЫШЕНИЮ ОСВЕДОМЛЁННОСТИ РАБОТАЕТ ПРАВИЛО «ДЁШЕВО НЕ ЗНАЧИТ ХОРОШО (ЭФФЕКТИВНО)»

ющей организационно-методологическую (ОРД и методики), техническую (учебные материалы сразу по нескольким актуальным темам в различных форматах, что требует приличного количества ресурсов) и человеческую (собственно работа с персоналом) составляющие, в достаточно сжатые сроки (в среднем 3–6 месяцев). Это может быть затратно, но только в этом случае эффект будет максимальным. Повышая осведомлённость только лишь своими силами, вам вряд ли удастся сконцентрировать за короткое время много ресурсов, и проект может выродиться в вялотекущую активность с относительно низкой эффективностью. Правда, подчеркнём, и это лучше, чем ничего.

Резюмируя, повышение осведомлённости персонала в области инфор-

мационной безопасности своими силами — вполне жизнеспособный вариант, если вы хорошо представляете его плюсы и минусы и готовы к интенсивной работе с некоторыми трудностями. Особенно учитывая перманентную ограниченность бюджета и сложности выбора подходящего подрядчика — рынок профессиональных консультационных услуг по повышению осведомлённости персонала в области информационной безопасности в России пока сложно назвать зрелым. Потому крайне трудно найти партнёра, который может не просто «на заказ рисовать картинки», а способен методологически правильно реализовать комплексный и законченный проект, адаптировав его результаты под специфику заказчика и в итоге измеримо изменив к лучшему ситуацию с обеспечением безопасности персоналом.



Марина БРОДСКАЯ
обозреватель BIS Journal



НОВЫЕ ПРОФСТАНДАРТЫ

СТУПЕНЬ РОСТА ОТРАСЛИ ИБ ИЛИ НАСОС
ПО ПЕРЕКАЧИВАНИЮ БЮДЖЕТНЫХ СРЕДСТВ?



ОТКАЗ ИЛИ НЕСВОЕВРЕМЕННОЕ ВНЕДРЕНИЕ ПРОФСТАНДАРТОВ В ОРГАНИЗАЦИИ КАРАЕТСЯ ШТРАФАМИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ КОДЕКСА ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ РФ

учреждениях и организациях. Полный переход к профстандартам должен произойти до 2020 г.

Отраслевые профстандарты в области информационной безопасности были разработаны ЗАО «Ассоциация специалистов информационных систем» (г. Санкт-Петербург) при участии Ассоциации защиты информации, ФГКОУ ВО «Академия Федеральной службы безопасности РФ», ФГУП «НТЦ «Атлас», ФУМО «Информационная безопасность». В соответствии с требованиями ФЗ-122 в ноябре 2016 г. Приказами Министерства труда и социальной защиты РФ профстандарты в сфере ИБ были приняты и утверждены Минюстом России.

БЮРОКРАТИЯ В ОСНОВЕ ВСЕГО

Для успешного внедрения профессиональных стандартов в организации, попадающие под требования закона, нужно соблюдение всех бюрократических процедур: создание комиссии, назначение ответственных, издание приказов и прочая бумажная волокита, которая закончится только после полного приведения документации организации в соответствие с требованиями профстандарта. Это касается и штатного расписания, и бухгалтерской документации, и должностных инструкций, и дополнительной подготовки кадров в соответствии с новыми требованиями стандартов, и аттестации сотрудников. При этом все спорные моменты, возникшие на предприятии при внедрении профстандартов, могут быть уточнены в территориальном отделении Минтруда. А вот отказ или несвоевременное внедрение профстандартов в организации карается штрафами в соответствии с требованиями Кодекса об административных правонарушениях РФ.

Казалось бы, с внедрением в жизнь профессиональных стандартов, в т.ч. в области среднего профессионального и высшего профессионального образования, и аттестации всех сотрудников учреждений и организаций государственной и муниципальной форм собственности на соответствие требованиям профстандартов, вопрос нехватки кадров должен уйти в прошлое.

Разработкой квалификационных требований к специалистам в области кибербезопасности сегодня занимаются Банк России, Минобрнауки, ФСТЭК и Минтруд. Отраслевые профстандарты требуют от «безопасника» базовых знаний в области ИТ. Помимо этого специалист должен знать (и уметь применять на практике с учетом специфики отрасли) типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях, базовые конфигурации средств защиты информации (СЗИ), знать особенности применения программных и программно-аппаратных СЗИ, типовые средства, методы и протоколы идентификации, аутентификации и авторизации, нормативные правовые акты в области защиты информации и организационные меры по защите информации.

Кто сегодня имеет право проводить сертификацию в области ИБ? Основными системами сертификации для большей части ПО являются системы сертификации ФСБ и ФСТЭК. Учебные программы по всем направлениям ИБ, на основании которых происходит обучение специалистов в области кибербезопасности по стандартам ВПО и СПО, утверждаются Федеральным учебно-методическим объединением «Информационная безопасность» (ФУМО) при участии межрегиональной общественной организации «Ассоциация защиты информации» и Академии ФСБ. В будущем к ним присоединится сеть ре-

В 2014 г. на государственном уровне начали обсуждать профессиональные стандарты. 2 мая 2015 г. Президент РФ подписал ФЗ-122 «О внесении изменений в Трудовой кодекс Российской Федерации» и изменение в статьи 11 и 73 ФЗ «Об образовании в Российской Федерации». С 1 июля 2016 г. началось поэтапное внедрение профессиональных стандартов в государственных

гиональных Центров оценки квалификации (ЦОК), которые будут работать с уже опытными безопасниками. Сеть только создается и кто и каким образом будет оценивать уровень подготовки специалистов, неизвестно.

Неясно также, как сертификат Центра оценки квалификации будет котироваться на рынке ИБ наряду с известными международными сертификатами Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA) или Certified Information Security Manager (CISM) в Information Systems Audit and Control Association (ISACA) или сертификатами центра анализа инцидентов (Global Incident Analysis Center, GIAC), созданного при институте SANS (System Administration, Networking and Security Institute). Есть вопросы и по тому, будут ли засчитываться квалификационные экзамены на получение международных сертификатов при прохождении испытаний в отечественном ЦОКе.

НАРК-КОНТРОЛЬ

За развитие системы подготовки и переподготовки кадров в России отвечает АНО «Национальное агентство развития квалификаций» (НАРК), его учредители — Российская Федерация, интересы которой представляют Минтруд и Минобрнауки, РСПП и ФНПР. Координирует работу АНО «Национальный совет при Президенте РФ по профессиональным квалификациям», который был создан в соответствии с Указом Президента России от 16 апреля 2014 г. № 249. Председателем Национального совета является глава РСПП А. Н. Шохин. Именно на Совет возложено решение об утверждении профессиональных стандартов.

Национальный совет создает советы по профессиональным квалификациям (СПК), которые являются постоянно действующими органами национальной системы профессиональных квалификаций, создаваемыми с целью формирования и развития систем профквалификаций по определенным видам профессиональной деятельности. И на эти советы возложена работа по выявлению новых специальностей, создание отраслевых профстандартов и проведение независимой оценки квалификации.

НЕЯСНО ТАКЖЕ, КАК СЕРТИФИКАТ ЦЕНТРА ОЦЕНКИ КВАЛИФИКАЦИИ БУДЕТ КОТИРОВАТЬСЯ НА РЫНКЕ ИБ НАРЯДУ С ИЗВЕСТНЫМИ МЕЖДУНАРОДНЫМИ СЕРТИФИКАТАМИ

Например, СПК в области информационных технологий разрабатывает профстандарты для специальностей в области ИТ и ИБ. Под его юрисдикцию попадают направления «Обеспечение безопасности информации в АС», «Проектирование, разработка и интеграция информационных ресурсов в локальной сети и информационно-телекоммуникационной сети «Интернет», «Автоматизация информационно-аналитической деятельности (АИАД) в государственных органах, обеспечивающих национальную безопасность», «Защита информации в компьютерных системах и сетях», «Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним», «Техническая защита информации».

СПК-ИТ возникла на базе «Ассоциации предприятий компьютерных и информационных технологий» (АП КИТ, создана в 2001 г.), в нее входят представители министерств, университетов и компаний, специализирующихся в области разработки программных продуктов и поддержки ИТ-инфраструктуры. В Комиссию по ИБ в рамках АП КИТ входят представители регуляторов, спецслужб, министерств и госструктур, университетов и компаний, занимающихся вопросами информационной безопасности. Найти информацию о том, каким образом АП КИТ связана с Центрами оценки квалификации, на сайте организации не удалось.

ЦОК

С 1 января 2017 г. вступил в силу Федеральный закон «О независимой оценке квалификации» № 238-ФЗ от 03.07.2016 г. Он стал дополнением одобренных осенью 2016 г. отраслевых профстандартов. В соответствие с этим ФЗ работодатели могут отправлять со-

трудников на независимую оценку квалификации в Центры оценки квалификации (ЦОК); или специалисты в области ИБ могут самостоятельно пройти этот квалификационный экзамен. НАРК будет вести реестры специалистов, подтвердивших свою квалификацию в соответствии с требованиями отечественных регуляторов. В настоящее время идет создание региональных ЦОК, которые работают на основании ФЗ № 238-ФЗ.

Для оценки квалификации создан «Программно-методический комплекс «Оценка квалификаций». На сайте НАРК о нем говорится так: это — «функциональная интернет-платформа, включающая совокупность инструментальных средств автоматизации подготовки и проведения профессионального экзамена с использованием содержащейся в ней электронной базы регулярно обновляемых комплектов оценочных средств (КОС) по профессиональным квалификациям». Он призван автоматизировать «процессы разработки, экспертизы и применения оценочных средств для оценки профессиональных квалификаций».

О том, кто и как будет проводить сертификацию, на сайте НАРК есть размытая информация. Идет подготовительная работа по отбору региональных методических центров и подготовке кадров, которые будут проводить работу по оценке квалификации госслужащих.

ФУМО

Главная структура, которая сегодня занимается подготовкой профстандартов в области образования и аккредитацией вузов — Федеральное учебно-методическое объединение (ФУМО) в сфере высшего образования по УГСН 10.00.00 «Информационная безопасность». По программам ФУМО по направлению ИБ работают

BIS-КОММЕНТАРИЙ

Наступил 2018 год, до введения обязательной сертификации в области информационной безопасности остается все меньше времени, а вопросы по этой проблематике только множатся. До сих пор активно обсуждается вопрос предметной области ИБ, кто такие специалисты ИБ и где проходит водораздел между ИБ и ИТ? До сих пор из уст многих начальников звучат слова, что безопасность им не нужна, ИТшники и так все сделают. А есть ли, вообще, такая отрасль знаний, как ИБ? Может её просто кто-то придумал, а на самом деле это просто раздел ИТ?

Те, кто хорошо знают кухню ИБ, уже точно осознали, что информационная безопасность — это нечто самостоятельное, со своими правилами игры, требованиями, условиями, этикой, наконец. И появление стандартов специальностей и стандартов образования — свидетельство уровня зрелости предметной области ИБ.

Знакомство с этими документами оставляет сложное чувство.

С одной стороны, необходимость в таких документах созрела и их появление — это здорово. Теперь при формировании штатного расписания я могу четко сказать, сколько и каких специалистов мне нужно, а если есть пересечение специальностей и требований, то это хорошее основание поговорить с руководством о повышении компенсаций и вознаграждений за профессиональные навыки. Отпали вопросы у кадровиков, какие специальности ставить в штатном расписании, появилась официальная возможность строить социальные лифты, в зависимости от сложности навыков. Появление стандартов образования дает какое-то понимание, что специалистов будут специально готовить, программы вузов (как минимум двух) по этим стандартам дают уверенность, что это будут именно специалисты.

Приходит, наконец, время, когда домохозяйке лучше заниматься домашним хозяйством, а защиту информации оставить специалистам. Это большой шаг вперед. Рывок.

И, тем не менее, остается горьковатый привкус от более пристального знакомства и со стандартами, программами и молодыми специалистами.

По своему предназначению и в силу специфики реальный специалист ИБ должен быть «широким» и вращаться в среде более «узких» специалистов ИТ, иначе невозможно преодолеть традиционно сложившийся системный дискомфорт «превосходства» ИТ над ИБ. Стандарт образования этот момент просто не видит и не учитывает. Специалист ИБ должен знать особенности ИТ, как минимум, не хуже ИТшников, иначе его не услышат и не поверят. Он должен видеть «сверху» взаимосвязи «узких» направлений, их влияние друг на друга, т.е. в обоих стандартах необходимо усилить изучение/знание информационных технологий как системного явления, а не как простой совокупности информационных объектов.

Очень слабо рассмотрены аспекты управления системой информационной безопасности, ведь по сути, СУИБ является частью системы управления всей организации, влияющей буквально на все процессы в организации, т.е. ИБ — не обособленный субъект, а необходимая существенная часть единого организма.

Очень слабо рассмотрены вопросы управления рисками, что недопустимо. Сегодня, в условиях сильной неопределенности направлений угроз, применение тех или иных защитных мер строится на оценке потери/стоимости защиты, и это является фундаментальным понятием ИБ, мерилom эффективности, метрикой ИБ, если хотите.

Картина мира с приходом бабушки из 38 попугаев поменялась: «Теперь мы будем гулять по правилам...»

Подведем итоги. Благодаря стандарту специальности мы знаем, кто мы есть. Благодаря стандарту образования мы знаем, как нас надо готовить. Благодаря обоим стандартам у нас есть, куда развиваться.

Василий Окулесский, кандидат технических наук

138 университетов. В вузах с государственной аккредитацией учатся 25,5 тыс. человек. Из них 5 тыс. человек — по программам магистратуры. За счет бюджетных средств учатся 77,6% студентов. Средний балл для поступления на специальности по направлениям 10.00.00 «Информационная безопасность» — 71,7, средний конкурс на поступление — 10,9 человек на место (данные по состоянию на март 2017 г.).

По версии Минобрнауки, в десятку лучших университетов, обучающихся студентов по направлениям ИБ входят: МГТУ «МИРЭА», МГТУ им. Н.Э. Баумана, НИУ ИТМО, НИЯУ «МИФИ» НИУ «МЭИ», СКФУ, СПбПУ Петра Великого, ТУСУР, СГАУ, УГАТУ.

Можно предположить, что вопрос подготовки и переподготовки специалистов в области защиты информации будет решаться, в первую очередь,

именно силами университетов, имеющих аккредитацию на работу по направлениям ИБ, и на базе их учебных центров как соответствующих всем требованиям ФГОС и имеющим соответствующую лицензию на обучение слушателей.

Если учесть, что средняя стоимость года учебы на коммерческой основе в государственном университете составляет порядка 100–120 тыс. руб., то

BIS-ОПРОС

На вопросы BIS Journal ответил Валерий Богдашов, руководитель Центра экспертизы компании R-Vision.

— Нужны ли отечественные профессиональные стандарты ИБ, как в области образования, так и для дальнейшей профессиональной квалификации госслужащих?

— Думаю, что на данном этапе развития отрасли, — скорее не нужны. Рынок очень узкий, готовых специалистов крайне мало, приходится «вращивать» из смежных областей. Специалист по информационной безопасности — довольно редкий персонаж, и найти подходящего не просто. Профстандарты введут дополнительные требования и еще сильнее уменьшат выборку. А реальной пользы от них практически не будет, поскольку технологии и требования очень динамичны, стандарты не успеют за изменениями.

— Повысится ли качество подготовленных кадров в области ИБ после введения профстандартов и начала работы Центров оценки квалификации?

— Однозначно нет. Проблема в качестве кадров тянется именно от проблем с высшим образованием. Если смотреть правде в глаза, сегодня молодой специалист в сфере ИБ выпускается из вуза с очень низким уровнем образования. По многим дисциплинам его знания давно устарели и нерелевантны к современной действительности. Это больше вопрос не профстандартов для выпускников, а уровня квалификации преподавателей и релевантности образовательных программ.

— Будет ли отвечать на запрос времени программа подготовки или переподготовки кадров в соответствии с требованиями профстандартов?

— Как я уже сказал, реальная квалификация будет низкой. Профстандарты не могут успеть за технологиями, и программы подготовки кадров, ориентированные на такие стандарты, будут еще больше отставать от реальных потребностей индустрии.

— Вопрос для учебных центров как самостоятельных компаний и вендоров. Будете ли вы участвовать в конкурсах, чтобы получить аккредитацию и сертификат регионального ЦОК? Как введение новой структуры отразится на вашей работе?

— Пока не планируем, поэтому нововведения никак не отразятся на нашей работе.

— Есть люди, которые рассматривают программы по профстандартам в области ВПО как стартовую площадку для подготовки хакеров. Не станет ли это привлекательным моментом для сертифицированных госслужащих с невысокими окладами?

— Нет. Общий уровень отрасли для такой задачи слаб.

цены на переподготовку кадров и регулярное повышение квалификации, как того требуют профстандарты, будут не ниже. А повышение квалификации будет осуществляться за счет бюджета госпредприятия, отправившего сотрудника на учебу, или за счет самого частного лица. Как кому повезет.

УЧЕБНЫЕ ЦЕНТРЫ

Многие из тех компаний, кто не может позволить себе ждать прихода специа-

листов, аттестованных по всем требованиям профстандартов, давно готовят квалифицированные кадры сами. Кто-то закупает курсы по подготовке кадров в области ИБ у крупных иностранных университетов, кто-то разрабатывает свои.

Учебный центр «Информзащита» специализируется на заказной разработке курсов и дальнейшем обучении по программам повышения квалификации, содержащим сведения, составляющие

гостайну. Центр имеет государственную аккредитацию, часть программ обучения согласованы с ФСТЭК России и ФСБ России. Среди клиентов — сотрудники Банка России, Сбербанка, Федерального казначейства, ФТС России, ГАС «Выборы», крупных компаний и промышленных предприятий.

Курс «Профессиональная переподготовка по направлению «Информационная безопасность» согласован с ФСБ, ФСТЭК России и ФУМО ИБ в соответствии с Приказом Минобрнауки от 5 декабря 2013 г. № 1310 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности». Программа вошла в соответствующий реестр учебных программ. Она отражает требования ФГОС ВПО по направлению «Информационная безопасность», а также требования профстандартов и квалификационные требования, обозначенные в Общероссийском классификаторе специальностей. Продолжительность программы — 512 академических часов аудиторных занятий. Программа построена по модульному принципу, что позволяет слушателям проходить обучение короткими циклами, не выпадая надолго из производственного процесса, отмечается на сайте Центра. Стоимость обучения — 120 тыс. руб.

По аналогичной программе работает не только «Информзащита», но и другие центры. «Академия информационных систем» также имеет лицензию на право ведения образовательной деятельности в области ИТ, ИБ, менеджмента и финансов. Академия является авторизованным центром тестирования ведущих сертифицирующих организаций Pearson VUE, тут можно сдать тесты на получение международных сертификатов ИТ-специалистов.

Учебный центр компании «ИнфоТеКС» также осуществляет профессиональную подготовку специалистов в сфере ИБ и имеет курсы повышения квалификации. Курс переподготовки по ИБ, согласованный с ФСТЭК, продолжительностью более 500 часов стоит 120 тыс. руб. Краткосрочные курсы повышения квалификации, утвержден-

ные регулятором, обойдутся слушателю чуть дешевле.

Курсы по подготовке специалистов по ИБ есть у Сетевой академии «Ланит», Центра компьютерного обучения «Специалист» при МГТУ им. Н.Э. Баумана (совместно с компаниями, специализирующимися на СЗИ, например, Group-IB и «Лаборатория Касперского») и т.д. Как отмечают представители компаний, заинтересованные в высококвалифицированных специалистах по ИБ, обучение одного сотрудника стоит 100–300 тыс. руб. Нельзя не упомянуть об учебном центре ЦИБИТ — одном из востребованных в системе подготовки кадров ИБ.

В ОЖИДАНИИ СВЕТОГО БУДУЩЕГО

Однако уже сейчас многие эксперты в области ИБ относят принятые отраслевые профстандарты к популярной у чиновников «бумажной безопасности» и говорят о том, что многие положения стандартов быстро устаревают. Особенно это касается отраслевых профстандартов в области образования — жизнь намного разнообразней, чем кажется чиновникам Минобрнауки и ректорам университетов, получивших лицензии на обучение по ИБ направлениям. Появляются новые понятия и термины, современные технологии развиваются быстрее, чем проходит обновление стандартов с учетом всех бюрократических процедур по согласованию изменений и дополнений.

Что получит профессиональное сообщество после того, как обученные по профстандартам в области высшего и среднего специального образования придут в государственные и муниципальные компании, имея на руках сертификаты соответствия занимаемой должности, полученные в ЦОКах? Пройдет ли кадровый голод?

Как показала дискуссия на тему нехватки квалифицированных кадров, случившаяся на прошедшем в Москве СОС-Форуме, профстандартами проблема кадров не решается. Об этом с один голос заявили представители регуляторов, крупных банков и компаний, работающих в области защиты информации. И аргументы представителей университетов, что специальности

МНОГИЕ ЭКСПЕРТЫ В ОБЛАСТИ ИБ ОТНОСЯТ ПРИНЯТЫЕ ОТРАСЛЕВЫЕ ПРОФСТАНДАРТЫ К ПОПУЛЯРНОЙ У ЧИНОВНИКОВ «БУМАЖНОЙ БЕЗОПАСНОСТИ»

в области ИБ востребованы абитуриентами как в сфере СПО, так и ВПО, что конкурс на место превышает все ожидания и растет с каждым годом, утонули в потоке претензий.

Среди них назывались и слабая базовая подготовка инженерных кадров, и необходимость переподготовки только что выпущенного из стен университета молодого специалиста. Сергей Лебедь, руководитель службы кибербезопасности Сбербанка, заметил, что банк предпочитает приглашать на работу уже состоявшихся опытных специалистов из других компаний (что вызывает недовольство коллег), а не вкладывать средства в дорогостоящую переподготовку выпускников вузов. Вакансии ведущих специалистов по информационной безопасности в Сбербанке закрываются через 6–9 месяцев, при этом первое собеседование проходят не более 10% претендентов на место.

Отдают предпочтение специалистам с непрофильным образованием, но опытом практической работы в ИБ, и представители государственных и коммерческих компаний, которым требуются специалисты по кибербезопасности. На нехватку кадров, разбирающихся в ИБ и IT, юриспруденции, финансах и психологии, жалуются и руководители антивирусных компаний. Они готовы приглашать выпускников гуманитарных специальностей, которые смогут решать задачи в области социальной инженерии.

Как в очередной раз отметил Артем Сычев, заместитель начальника Главного управления безопасности и защиты информации Банка России, выпускники университетов по направлениям ИБ слабо подготовлены в смежных областях: IT, финансовой сфере, юриспруденции, психологии. Поэтому Центробанк совместно с заинтересованными ведомствами продолжает работу над

профстандартом в области информационной безопасности банков.

Кому выгодно ломать сложившуюся в стране систему сертификации в сфере ИБ? Можно предположить, что регуляторы и спецслужбы вряд ли допустят сторонние организации к вопросам кибербезопасности, касающимся гостайны. Многие специалисты сдают тесты на копирующие в отрасли международные сертификаты и не горят желанием проходить испытания на еще один, национальный. Тем более, что он предполагает подготовку специалиста слишком широкого профиля, чем требуется в узкоспециализированных областях госструктур и коммерческих организаций. Помимо финансовых затрат на подготовку такого сотрудника (возможность самообразования никак не отражена в профстандартах, требуется диплом учебного заведения), возникает вопрос: будет ли в последствие оценена его квалификация по достоинству, поскольку уровень зарплат на госпредприятии и частном секторе отличается на несколько порядков? Это подтверждается и запросами работодателей на рекрутерских сайтах. И уже сегодня есть мнение, что профстандарты обязательны к исполнению только для государственных структур и госкомпаний, и потому сотрудникам частных компаний можно обойтись и без национального сертификата.

* * *

Есть вопрос и с другой стороны. Имеют ли смысл затраты госуниверситетов и частных учебных центров на получение лицензий региональных Центров оценки квалификации? Заработает ли вся система сертификации или останется нереализованным проектом — насосом по перекачиванию бюджетных средств в разные карманы под предлогом подготовки столь нужных стране кадров?



Дмитрий ЛАРИН
историк криптографии,
кандидат технических наук

ПЕТР I И КРИПТОГРАФИЯ

«СИЯ ЦИФИРЬ ЗЕЛО К РАЗОБРАНИЮ ЛЕГКА»

В 2017 году исполнилось 345 лет со дня рождения первого российского императора Петра Великого (30.05 (09.06 нов. стиль). 1672 — 28.01 (08.02 нов. стиль). 1725).

Петр I вошел в историю как великий реформатор. Главным итогом его преобразований стало преодоление отставания России от европейских держав в военной, экономической и политической областях. Он коренным образом изменил структуру государственного управления, создал боеспособную армию и флот, при нем произошел прорыв в экономике страны, было создано множество предприятий, мануфактур, оружейных заводов, металлургических и горнодобывающих предприятий, верфей и т.д. Серьезный импульс к развитию получила внутренняя и международная торговля. По его инициативе была учреждена Академия наук, открывались учебные заведения, сотни молодых людей отправлялись учиться за границу. С другой стороны, в Россию во множестве приглашались иностранные специалисты.

Разумеется, эффективное государственное управление, военные победы и дипломатические успехи были бы невозможны без активной криптографической деятельности. Петр это отлично осознавал и уделял криптографии как надежному средству сохранения государственных секретов большое внимание.

ЗАЩИТА ИНФОРМАЦИИ НА ГОСУДАРСТВЕННОМ УРОВНЕ

В петровскую эпоху в России шифрование стало основным средством за-

щиты информации, хотя продолжали использоваться и другие методы: стеганография, физическая защита, условная сигнализация и т.п. При этом, если в прежние времена практически вся шифрпереписка была посвящена дипломатическим вопросам, то при Петре активно шифровалась и военная и внутриполитическая информация.

Для организации связи были созданы ряд учреждений — Кабинет его императорского величества, Посольская канцелярия, Коллегия иностранных дел и т.д. — со строгим разделением функций. Деятельность этих учреждений регламентировалась законодательно. Широко практиковались организационно-административные методы защиты информации, такие как особый подбор кадров для осуществления криптографической деятельности и строгий контроль за их работой, организация пропускного режима в помещения, где производилось шифрование и расшифрование или хранились шифры, обеспечение охраны гонцов и курьеров и т.д. Из новшеств в области связи отметим, что для обеспечения управления флотом и прибрежными районами страны в качестве средства связи стали широко использоваться суда.

К концу XVII века Россия становится самой крупной европейской державой, раскинувшейся от Днепра до Тихого океана. Для управления этой огромной территорией в первую очередь была необходима быстрая, надежная и конфиденциальная связь. Основным средством передачи сообщений в то время являлась почта. Наиболее распростра-

ненным методом защиты информации была физическая защита. Ямщики отвечали за сохранность почты и целостность печатей.

С созданием регулярной армии возникла настоятельная потребность в совершенствовании управления войсками. Уже во время азовских походов против турок в 1695–1696 годах Петр I организовал работу первой российской военно-полевой почты, возглавлял ее первый русский почтмейстер А.А. Виниус. Отправления по линии этой почты назывались чрезвычайными.

Шифры использовались во время Азовских походов и Великого Посольства. Однако наибольшая надобность в криптографии возникла в начале XVIII века, когда за рубежом появились дипломатические представительства России. Также в 1700 году началась Северная война со Швецией, что потребовало эффективного управления войсками на значительном театре военных действий. И, наконец, управление огромной внутренней территорией тоже требовало обеспечения секретности переписки.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н
Ч	2	8	2	Х	н	Ш	3	9	6	5	Д	
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	
+	7	8	2	0	У	В	У	8	Л	Л	У	
	Ъ	Н	Ъ	Ъ	Е	8	Я	Ъ	А			
	У	8	9	8	А	8	У	8				

Рисунок 1. Ключ к шифру простой замены



Рисунок 2. Шифртекст письма Петра I (слева) и его расшифровка (справа)



Петр I (художник Поль Деларош, 1838 год)

«ПУСТЫШКИ», НОМЕНКЛАТОРЫ, «СУПЛЕМЕНТЫ»...

Теперь рассмотрим шифрсистемы, которые применялись в эпоху Петра I. Как и в прежние годы, основным шифром на Руси была простая замена, то есть знаки открытого текста заменялись на буквы (при этом буквы могли принадлежать как алфавиту открытого текста, так и другой азбуки), цифры или специально придуманные знаки. При этом следует отметить, что в шифрах Петровской эпохи употреблялись только привычные нам арабские цифры, так как в начале XVIII века Петром была выведена из употребления архаичная буквенная кириллическая нумерация, заимствованная у греков. В качестве знаков шифрованного текста употреблялись и буквенные сочетания.

Тексты, которые надо было зашифровать, могли быть написаны на русском, французском, немецком, а иногда даже греческом языках. Как известно Петр прекрасно владел несколькими европейскими языками, в то же время на государственной службе состояло много иностранцев, именно в переписке с ними в основном использовались немецкий и французский. При этом следует отметить, что с точки зрения стойкости предпочиталось использовать русский язык. За границей было

очень мало людей, владевших русским, а знание лингвистических особенностей языка может существенно помочь криптоаналитику в дешифровании.

Новым для российских шифров петровского времени стало наличие во многих из них «пустышек» — знаков шифрованного текста, которым не соответствует никакой знак открытого текста, то есть они не несли никакого смысла. Как правило, пустышек было немного, обычно 5–8 знаков. Пустышки увеличивает стойкость шифра, так как они дают криптоаналитику неверную информацию о количестве знаков в алфавите открытого текста, разбивают структурные лингвистические связи открытого текста и изменяют статистические закономерности, то есть именно те свойства текста, которые используют при дешифровании шифра простой замены.

Кроме того, пустышки увеличивают длину шифрованного текста по сравнению с открытым, что усложняет их взаимное сопоставление. Кроме того, в некоторых случаях отдельные знаки применялись для зашифрования точек и запятых, для этого также могли использоваться пустышки. Это особо оговаривалось в кратких правилах пользования шифром.

Вскоре к обычному алфавиту простой замены стали добавлять обозначения

для наиболее употребительных слогов, слов и целых фраз, то есть номенклаторы. Петровские номенклаторы были весьма простыми, они содержали небольшой словарь, называвшийся «суплемент» и содержащий некоторое количество слов (имен собственных, географических наименований или каких-то устойчивых словосочетаний, которые могли часто использовать корреспонденты, использовавшие данный шифр).

Шифр Петровской эпохи представлял собой лист бумаги, на котором от руки был написан ключ — таблица замены (обычно под горизонтально расположенными в алфавитной последовательности буквами кириллицы или иного алфавита подписаны соответствующие элементы шифроалфавита), а также суплемент (если это был номенклатор). Ниже могли помещаться пустышки и краткие правила использования шифра.

Еще одной особенностью петровских шифров является то, что шифроалфавит мог составляться из символов разных типов, например, смеси букв разных алфавитов, цифр и т.д.

ОТ ПРОСТОГО К СЛОЖНОМУ

Главным новшеством стало применение более сложных, чем простая замена, шифров. Так в 20-х годах XVIII века

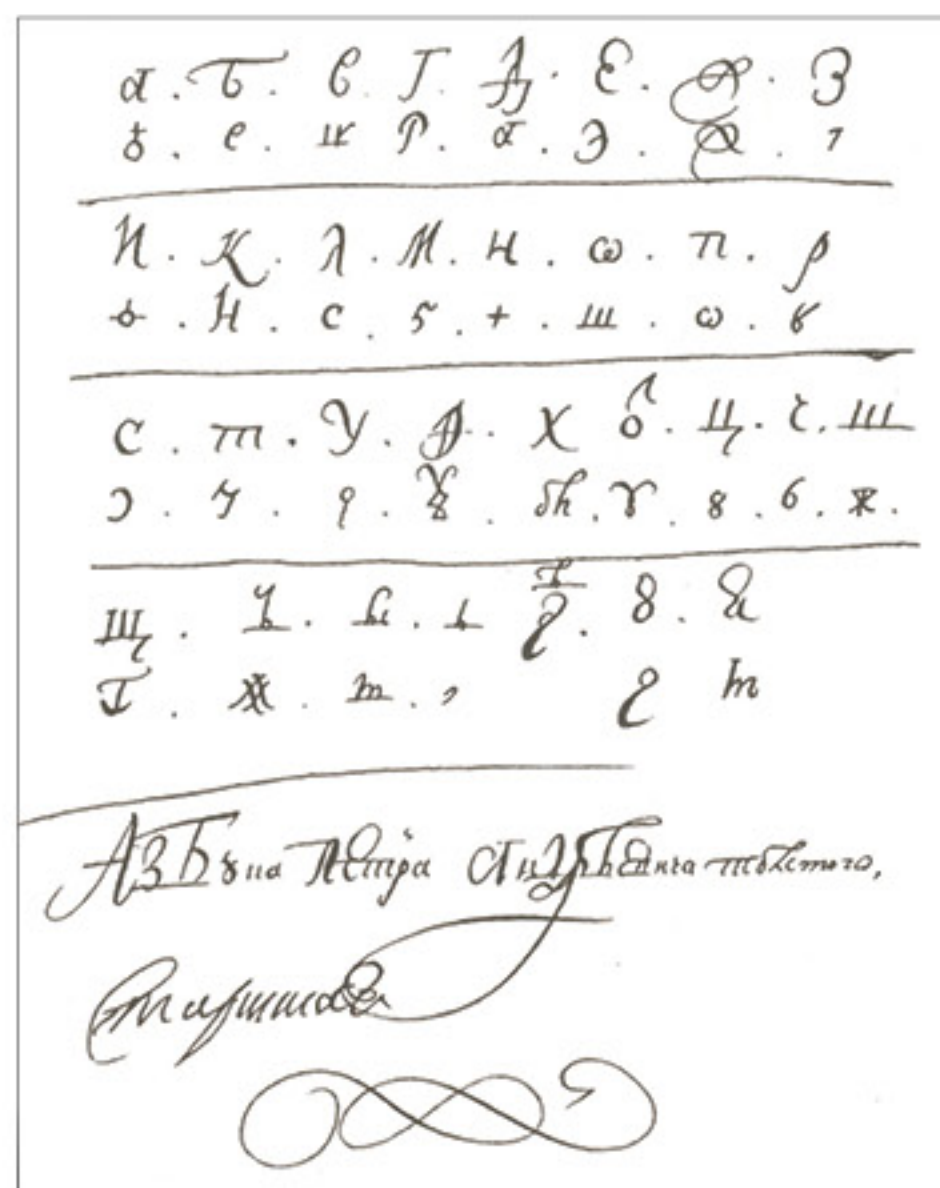


Рисунок 3. Шифр П.А. Толстого

от шифров простой замены переходят к замене пропорциональной, когда наиболее часто встречающимся знакам открытого текста присваиваются несколько шифробозначений, что затрудняет использование «классического способа» криптоанализа — частотного анализа. Еще раньше, примерно с 1708 года, в России начали применять шифры разнозначной замены — когда для замены одного знака открытого текста используется один или два знака шифртекста. Следует отметить, что шифры такого типа, являясь более стойкими, чем «классическая» простая замена, в то же время и более чувствительны к ошибкам при шифровании.

РЕГЛАМЕНТАЦИЯ

В Петровскую эпоху началась нормативно-правовая регламентация криптографической деятельности. Так в 1716 году был принят «Устав воинский» — первый в истории России документ такого рода. В соответствии с Уставом учреждены должности «адъютантов, ординарцев, курьеров для передачи и доставки секретных донесений», а также отредактированы «Правила действия военно-полевой почты».

Военная полевая почта, стала активно использоваться для быстрого обмена конфиденциальной корреспонденцией между крупными воинскими соединениями и вновь создаваемыми центральными органами управления армией и флотом — Военной коллегией и Ад-

миралтейств-коллегией. Для доставки особо важной и срочной корреспонденции в адрес императора или президентов оборонных коллегий при главнокомандующих армиями были учреждены должности военно-полевых курьеров.

Следует отметить, что собственно вручную отредактированные Петром I «Правила действия военно-полевой почты» являются, по сути, первым дошедшим до нас документом, в котором было четко и определенно сформулировано назначение военно-курьерской связи.

Преобразование системы государственного управления страной, осуществляемые Петром, касаются и повышения эффективности системы связи. В 1720 году вводится Генеральный регламент, определяющий процесс функционирования системы управления России. В этом документе впервые четко устанавливался и порядок работы с правительственной корреспонденцией:

«В соответствии с регламентом, вся правительственная корреспонденция в зависимости от степени ее важности и срочности была разделена на определенные группы. Так, особо важные правительственные документы, например, именные указы императора с его личными распоряжениями, всеподданнейшие донесения и доклады на его имя, реляции, манифесты направлялись по каналам «необыкновенной», «чрезвычайной» почты через правительственных гонцов и нарочных курьеров. Особо важную корреспонденцию из личной канцелярии императора доставляли кабинет-курьеры, входившие в штат Кабинета его императорского величества и имевшие воинские звания обер-офицерского состава. Когда же небольшая группа

кабинет-курьеров (по штату 6 человек) не справлялась с доставкой всей исходящей из Кабинета особо важной корреспонденции, для выполнения обязанностей правительственных курьеров широко привлекались военные чины от капрала до полковника, в зависимости от важности даваемого им поручения. А по делам особо важным, как, например, доставка писем императора главам иностранных государств, привлекались генералы (в петровское время преимущественно П. И. Ягужинский и Л. К. Нарышкин). Сенат также имел в своем распоряжении прикомандированных армейских офицеров, которых использовал в качестве курьеров для доставки адресатам своей исходящей корреспонденции».

ВЫСОЧАЙШИЙ КРИПТОАНАЛИЗ

Именно в Петровскую эпоху свои первые шаги сделал российский криптоанализ, стали развиваться методы тайного перехвата информации, осуществлялась агентурная добыча криптографических секретов противника. При этом важно отметить, что занимался оценкой стойкости российских шифров не кто-нибудь, а сам царь!

Приведем две цитаты. Петр писал фельдмаршалу Огильви по поводу одного шифра (цифири, как их тогда называли): «А которую вы перво прислали, и та не годна, понеже так, как простое письмо, честь можно». И еще одна нелестная оценка царя: «Сия цифирь зело к разобранию легка».

ИСКУССТВО ПЕРЕХВАТА

Стали проявлять в России интерес и к шифрам иностранных государств. О регулярном дешифровании иностранной переписки речь пока не шла,

**РУССКИМ ДИПЛОМАТАМ,
РАЗВЕДЧИКАМ И ДРУГИМ
ПРЕДСТАВИТЕЛЯМ ЗА ГРАНИЦЕЙ
ПРЕДПИСЫВАЛОСЬ ДОБЫВАТЬ ЛЮБУЮ
ИНФОРМАЦИЮ, КАСАЮЩУЮСЯ
ШИФРОВ, ОРГАНИЗАЦИИ
СВЯЗИ, ОТКРЫТЫХ ТЕКСТОВ**

однако заинтересованность в получении информации таким методом уже была. Русским дипломатам, разведчикам и другим представителям за границей предписывалось добывать любую информацию, касающуюся шифров, организации связи, открытых текстов (против атаки «открытый текст — шифрованный текст» подавляющее большинство шифров того времени было не устойчиво). На этих лиц и их зарубежную агентуру также возлагалась задача организации перехвата иностранных сообщений за границами России.

В это время пришло понимание важности такого источника информации, как шифрованная переписка иностранных государств. Полученная информация могла быть весьма полезна российскому руководству, дипломатам, военным. Велся перехват сообщений и внутри России, совершенствовались методы перлюстрации, осуществлялась цензура, вводились ограничения на почтовое сообщение.

«ЧУЖИЕ» ШИФРЫ

И тут российские власти столкнулись с «чужими» шифрами (дело царевича Алексея). Таким образом, была зафиксирована негосударственная криптография. Заметим, что Петр I считал шифры монополией царя российского. Он строго наказывал своих подданных за использование «негосударственных» цифирей. Однако частные лица все же пользовались собственными шифрами. Среди них можно указать царевну Софью Алексеевну, которая использовала шифр в переписке со своим фаворитом князем В. В. Голицыным.

В целом отметим, что Петр Великий был первым из российских правителей, кто предельно ясно осознал важность криптографической деятельности для обеспечения безопасности государства. Во время его правления впервые в истории отечественной криптографии к осуществлению криптографической деятельности (в том числе к составлению шифров) привлекалось все высшее руководство России, включая царя.

ЛИТЕРАТУРА

- [Астрахан, 1996] Астрахан В. И., Гусев В. В., Павлов В. В., Чернявский Б. Г. Становление и развитие правительственной связи в России, Орел: ВИПС, 1996.
- [Бабаш, 2002] Бабаш А. В., Шанкин Г. П. История криптографии. Часть I. М.: Гелиос, 2002.
- [Буганов, 1989] Буганов В. И. Пётр Великий и его время. М.: Наука, 1989.
- [Бутырский, 2007–1] Бутырский Л. С., Гольев Ю. И., Ларин Д. А., Никонов Н. В., Шанкин Г. П. Криптографическая деятельность в Швеции. От викингов до Хагелина // Защита информации. INSIDE. № 3, 2007, с. 88–96.
- [Бутырский, 2007–2] Бутырский Л. С., Гольев Ю. И., Ларин Д. А., Никонов Н. В., Шанкин Г. П. Криптографическая деятельность в Швеции в первой половине XX века // Защита информации. INSIDE. № 4, 2007, с. 88–96.
- [Бутырский, 2007–3] Бутырский Л. С., Гольев Ю. И., Ларин Д. А., Никонов Н. В., Шанкин Г. П. Криптографическая деятельность в Швеции. Послевоенный период. // Защита информации. INSIDE. № 5, 2007, с. 82–90.
- [Бутырский, 2007–4] Бутырский Л. С., Гольев Ю. И., Ларин Д. А., Никонов Н. В., Шанкин Г. П. Криптографическая деятельность в Швеции. От прошлого века к настоящему. // Защита информации. INSIDE. № 6, 2007, с. 76–85.
- [Вигилев, 1977] Вигилев А. История отечественной почты. М., 1977.
- [Гладыш, 2005] Гладыш М. Псы войны // Независимое военное обозрение № 19, 2005, с. 8.
- [Голиков, 1789] Голиков И. И. Деяния Петра Великого, мудрого преобразователя России, собранные из достоверных источников и расположенные по годам. М., 1789.
- [Гольев, 2008] Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008.
- [История, 1984] История военной связи. Под общей редакцией А. И. Белова. М.: Воениздат, 1984.
- [Кан, 2004] Кан Д. Война кодов и шифров. М.: РИПОЛ КЛАССИК, 2004.
- [Князьков, 1914] Князьков С. Очерки из истории Петра Великого и его времени. Издательское объединение «Культура», 1990. Репринтное воспроизведение издания Спб.: Издательство книжного магазина П. В. Луковникова, 1914.
- [Козлов, 2001] Козлов В. П. Первые российские архивисты дипломатических бумаг // Российская дипломатия: История и современность. Материалы Научно-практической конференции, посвященной 450-летию создания Посольского приказа. М.: РОССПЭН, 2001, с. 37–41.
- [Костомаров, 1989] Костомаров И. И. Царевич Алексей Петрович. М., 1989.
- [Кудрявцев, 2002] Кудрявцев Н. А. Государево Око. Тайная дипломатия и разведка на службе России. М., ОЛМА-ПРЕСС, 2002.
- [Лурье, 2006] Лурье Ф. М. Политический сыск в России 1649–1917. М.— Спб., Центрполиграф, МиМ-Дельта, 2006.
- [Матвеев, 2001] Матвеев В. М. О трехсотлетию визита Петра I и Великого посольства в Англию // Российская дипломатия: История и современность. Материалы Научно-практической конференции, посвященной 450-летию создания Посольского приказа. М.: РОССПЭН, 2001, с. 90–92.
- [Материалы, 1914] Материалы для истории Гангутской операции. Вып. I, Ч. I. Пг., 1914.
- [Молчанов, 1984] Молчанов Н. Н. Дипломатия Петра Первого. М., «Международные отношения», 1984.
- [Очерки, 1999] Очерки истории внешней разведки. Том 1, под ред. Е. М. Примакова. М.: «Международные отношения», 1999.
- [Павленко, 1989] Павленко Н. И., Александр Данилович Меншиков М.: «Наука», 1989.
- [Письма] Письма и бумаги императора Петра Великого. Т. 1–12, Спб., 1887–1912, М.; Л., 1946–1977.
- [Подъяпольская, 1959] Подъяпольская Е. П., Шифрованная переписка России в первой четверти XVIII века. Проблемы источниковедения. М., 1959.
- [Полмар, 1999] Полмар Н., Аллен Т. Б. Энциклопедия шпионажа. М.: КРОН-ПРЕСС, 1999.
- [Пушкин] Пушкин А. С. Полтава // Полное собрание сочинений десяти томах, том 3, М., 1956–1962.
- [Сборник, 1873] Сборник Русского исторического общества. Т. XI. Спб., 1873.
- [Словарь, 1984] Советский энциклопедический словарь. М., Советская энциклопедия, 1984.
- [Соболева, 2002] Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.
- [Сперанский, 1929] Сперанский М. И. Тайнопись в юго-славянских и русских памятниках письма. Энциклопедия славянской филологии. Вып. 3–4. Л., 1929.
- [Трифанов, 1994] Трифанов М. А. Фельдъегерская связь России. Исторические очерки. М.: АО «Панас-Аэро», 1994.



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

СТО ЛЕТ НАЗАД

СУДЬБЫ УЧАСТНИКОВ «МАГДЕБУРГСКОЙ» ИСТОРИИ

Завершение столетия Революции 1917 года даёт повод вновь вспомнить героев очерка «Сто лет назад. Триумф и трагедия радиоразведки Балтийского флота» (BIS Journal № 2,3/2017). Их судьбы, ярко отразившие революционные перемены, как представляется, заслуживают более подробного рассказа.

Начнём его с памятных читателям событий утра 26 августа 1914 года. На илл. 1 запечатлено, как моряки с эсминца «Лейтенант Бураков» наблюдают за приближением вельбота с их товарищами к подорванному немецкому

крейсеру «Магдебург». Мы знаем, что на этом вельботе плыл к своей удаче лейтенант М. В. Гамильтон: ему посчастливилось обнаружить на палубе крейсера «Сигнальную книгу германского флота», бесценную находку для российских и британских радиоразведчиков и криптографов.

РЕНГАРТЕН

Но пока расстанемся с М. В. Гамильтоном и обратимся к подробностям жизненного пути Ивана Ивановича Ренгартена. Именно он стал, как мы знаем, инициатором создания Радиостанции

особого назначения (РОН), главного радиоразведывательного и дешифровального центра на Балтике в 1915–1917 годах.

Иван Иванович родился в 1883 году в Новгородской губернии. В январе 1904 года окончил Морской кадетский корпус и избрал назначение в Квантунский флотский экипаж, тогда уже начиналась война с Японией. В 1904–1905 годах участвовал в обороне крепости Порт-Артур, получил тяжёлые ранения, последствия которых весьма затрудняли всю его дальнейшую службу на флоте. После сдачи крепости Порт-Артур попал в плен, за попытку побега приговорен к 5 годам тюрьмы. В январе 1906 года Иван Иванович вернулся из плена на Балтийский флот.

В 1907 году он окончил Офицерский минный класс и его оставили при Учебном минном отряде для специализации в области радиотелеграфирования. В будущем Иван Иванович стал главным реорганизатором флотской радиотелеграфии. Уже в 1909 году, изучив новые образцы радиостанций фирмы «Телефункен», он предложил отказаться от их дорогостоящей закупки, организовав заводскую модернизацию по его собственным чертежам имеющегося на флоте оборудования. Экономия была оценена в 800 тысяч руб. бюджетных средств. Результатом стало производство отечественных радиостанций на новом радиотелеграфном заводе Морского ведомства в Петербурге. Тогда же И. И. Ренгартен начал преподавать радиотелеграфию в Минной школе.

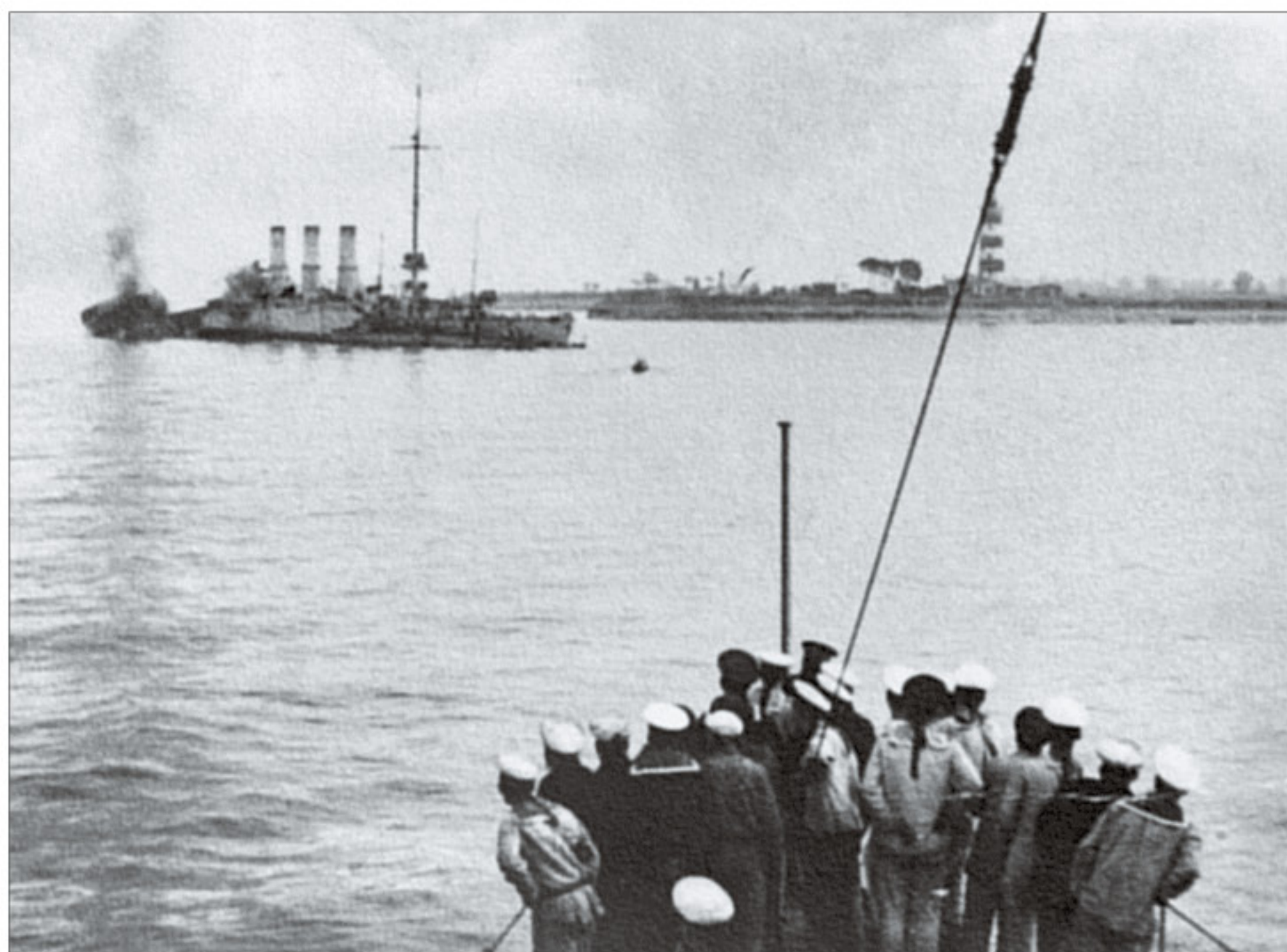


Иллюстрация 1. На вельботе лейтенант М. В. Гамильтон плывёт к своей удаче



Иллюстрация 2. Пленных моряков «Мадебурга» ведут по Петрограду

С 1912 года Иван Иванович служил в штабе Балтийского флота, занимаясь делами радиоразведки. Здесь он проявил себя и как талантливый изобретатель, предложив в сентябре 1914 года первый на флоте радиопеленгатор собственной конструкции, которую постоянно совершенствовал. После проверки его эффективности, пеленгатор стали производить на ведомственном радиотелеграфном заводе, удовлетворяя потребности флотов.

И. И. Ренгартен по своим обязанностям был разработчиком радиокодов и других флотских криптографических документов. В июле 1917 года его произвели в капитаны 1-го ранга. «Здоровье свое он не щадил для службы и несколько раз был принужден из-за слабых легких от последствий ранения и начавшегося туберкулеза лечиться в санаториях, причем отправляли его всегда для лечения в горизонтальном положении, чуть не насильно». Уволен в отставку 30 апреля 1918 года. В 1918–1920 годах И. И. Ренгартен преподавал в Морской академии. Добавим, что в 1917 году его избрали в исполком Совета матросских, солдатских и рабочих депутатов на прежней главной базе флота в Гельсинфорсе (ныне Хельсинки).

Следует заметить еще, что «Иван Иванович обладал большим талантом

в области художественной графики, в которой находил большое удовлетворение после своей разнообразной и плодотворной деятельности. Из его работ в этой области следует указать на помещенные им иллюстрации «Морской транспорт всех времен и народов» в журнале «Балтийский морской транспорт»... Самой капитальной частью его работы в этой области была иллюстрация финской поэмы «Калевала», 9 первых эскизов которой были помещены на выставке дворца искусств в 1919 году» [1]. И. И. Ренгартен умер в Петрограде в январе 1920 года. Его вдова с двумя сыновьями выехала во Францию.

НЕПЕНИН

Обратимся теперь к личности главного организатора успехов радиоразведки Балтийского флота — Адриана Ивановича Непенина. Адриан Иванович родился в Великих Луках в 1871 году. Окончил Морской кадетский корпус в 1892 году. В 1895–1896 годах служил на Черноморском флоте, в 1897 году переведен в Сибирский флотский экипаж и назначен на мореходную канонерскую лодку «Манджур». На илл. 3 можно видеть лейтенанта А. И. Непенина среди офицеров «Манджура», он второй снизу. С началом русско-япон-



Иллюстрация 3. Шутка молодых офицеров «Манджура»: они изображают трап на корабле

ской войны «Манджур», находившийся при российском представительстве в Шанхае, был интернирован.

А. И. Непенин прибыл добровольцем в Порт-Артур. Там, командуя миноносцем «Сторожевой», во время ночной торпедной атаки японцев он прикрыл корпусом своего корабля флагманский броненосец «Севастополь». Приняв японскую торпеду, сумел спасти своё судно, направив его на мелководье. За храбрость награждён орденом св. Георгия 4-й степени.

Вся его дальнейшая служба связана с Балтийским морем. В 1911 году А. И. Непенин произведён «за отличие» в капитаны 1-го ранга. С 1911 года он начальник Службы связи — военно-морской разведки Балтийского флота.

Адриан Иванович обладал способностью замечать чужие дарования и выдвигать их обладателей. Так, он добился назначения главным инженером авиации Балтийского флота для молодого лётчика Игоря Сикорского, много позже всемирно известного, а тогда ещё не имевшего инженерного диплома.

В 1914 и 1915 годах А. И. Непенин совмещал работу в Службе связи с командованием обороной Приморского фронта Морской крепости императора Петра Великого, т.е. обороной входа в Финский залив. С 1 сентября

1914 года — контр-адмирал, а с 28 июня 1916 года — вице-адмирал. С 6 сентября 1916 года он командующий Балтийским флотом.

На доверенных ему постах А. И. Непенин проявил себя и выдающимся организатором криптографической деятельности. Этот факт давно получил признание. По оценке современного германского историка В. Рана, «русский флот весьма искусно вел минную войну... В отличие от немецкого минного наступления в Северном море, русский план был основан на разведывательных данных о действиях немецких военно-морских сил в восточной части Балтийского моря...» [2]. Уместно отметить здесь, что самым минированием надёжно руководил капитан 1-го ранга А. В. Колчак.

Впрочем, качественно новая, с использованием радиоразведки, организация минной войны русским флотом была высоко оценена германскими моряками уже в первом послевоенном исследовании М. Бастиана: «Справедливость в отношении бывшего противника требует открытого признания в том, что германский флот обрел в лице бывшего императорского российского флота своего учителя по части минной войны...».

В подтверждение этих слов укажем на боевой эпизод ноября 1916 года. Тогда германское командование решило пресечь доставку морем подкреплений для русского наступления под Ригой. Подготовку этого наступления выявила немецкая разведка. Из Атлантики к Финскому заливу была направлена флотилия из 11 новейших боевых кораблей — эсминцев постройки 1914–1916 годов под командованием фон Витинга. Но вместо ожидаемых немцами русских военных транспортов их встретили лишь русские мины. Несмотря на меры предосторожности, 7 из 11 эсминцев подорвались на специально для них установленных минах. Случилась беспрецедентная для первой и второй мировых войн потеря боевых кораблей. А ведь их вели опытные моряки, на равных сражавшиеся в Атлантике с британским флотом.

По свидетельствам современников у А. И. Непенина были большие планы на 1917 год, замышлялась десант-

ная операция в Восточную Пруссию. Устроилась и семейная жизнь: в начале 1917 года Адриан Иванович повенчался с вдовой морского офицера. Но Февральская революция сурово изменила ход событий и жизненные планы: 4 (17) марта командующий БФ вице-адмирал А. И. Непенин был убит «революционными матросами» на базе флота в Гельсингфорсе. Убит выстрелом в спину в толпе.

ИЗ ДНЕВНИКОВ И. И. РЕНГАРТЕНА

Чтобы почувствовать обстановку тех дней, приведём краткие выписки из дневниковых записей И. И. Ренгартена [3], скрупулёзно зафиксировавшего развитие событий 1917 года. Разумеется, содержание записей окрашено собственным отношением И. И. Ренгартена к описываемым событиям, ведь он не редко оказывался их непосредственным участником. Все даты в записях указаны по старому стилю.

«30 янв. ... В разговоре комфлот перешёл на личный состав флота и заявил, что с этой стороны он спокоен, ему кажется, что все поутомились, поуспокоились и становятся почти равнодушными... Я горячо возражал; сказал, что сейчас только и разговоров, что о внутренней политике, что офицерство проникнуто негодованием и волнением, что, конечно, оно в целом на эксцессы теперь не пойдёт и их не допустит, но настроение личного состава, в общем, самое оппозиционное!

24 февр. 23–50. Вчера в Петрограде происходили беспорядки на почве недостатка продовольствия. Всё это — результат дезорганизаций нашего управления...

28 февр. 9–00. Ура! Только что узнал потрясающую новость: вчера в Государственной Думе образовалось Временное правительство во главе с Родзянко; все министры в Думе. На утреннем собрании флагманов комфлот был краток и определённо сказал, что ни из ставки, ни от министра определённых указаний не получено, поэтому он сделает то, что сочтёт нужным, а все подчинённые ему лица и места сделают то, что он прикажет. Пояснил свою точку зрения «невмешательства» в революцию. Наши начальники и командиры, в об-

щем, настроены празднично и сочувствуют революции во спасение родины.

1 марта. «Кречет». 9–10. Собрание флагманов и капитанов. Комфлот: «Я прочту вам телеграммы, которые получил, и сообщу вам свои приказания». Следует чтение телеграмм... «Я донёс о своих поступках государю императору. Требую полного повиновения!» (Эти слова сказаны твёрдо, негромко, очень внушительно — Непенин обвёл всех тяжёлым взглядом). «Всё, господа!» Больше ни одного слова не было сказано. Государю императору через ставку и параллельно — министра Непенин прямо и открыто донёс, что считает необходимым пойти навстречу Государственной Думе, ибо, в противном случае, не только немыслимо поддержание боевой готовности, но даже повиновение воинских частей... Ужасны известия из Кронштадта, там разыгралась анархия — убит адмирал Вирен!

2 марта. 16–00. События идут с головокружительной быстротой... Масса разговоров о династии, о присяге. В общем, всё-таки очень тяжело. Радость сменяется тревогой.

3 марта. В 1–10 получена телеграмма, что манифест об отречении от престола подписан.

7–20. Ясное солнечное утро. Было собрание флагманов, причём прочтён манифест — кричали «ура» новому государю. Ночь без сна, но какая великая, радостная, памятная ночь счастливого завершения Великой Российской революции!... Ещё не знаю подробностей, но беспорядки у минной обороны прекращены лично комфлотом и адмиралом Максимовым.

18–35. Нервность растёт, отовсюду слухи о беспорядках... В общем, кажется мы идём к гибели.

19–20. Нас может спасти только чудо! Психоз беспорядка перекинулся — сюда: на «Андрее Первозванном» подняли красные флаги, кричат «ура».

19–43. Непенин пошёл в палубу, сказал речь — всё без утайки. Потом стал говорить всё сильнее, сильнее... Кто-то крикнул: «Адмиралу — ура!», все подхватили... Это было слишком — его качали... Слышна стрельба пулемёта. За что это? Неужели всё погибнет?

20–00. С судов эскадры несутся крики «ура». Стрельбы нет.

20–05. По направлению к «Кречету» идут толпы матросов с кораблей. В ставку и Думу послана телеграмма, что «Балтийский флот как боевая единица более не существует».

20–30. Взбунтовалась минная дивизия: слышна стрельба.

20–35. Команда наша просила разрешения поднять красный огонь... Адмирал разрешил.

21–00. Где-то близко орудейный выстрел.

21–50. Командующий флотом говорил в командной палубе с депутатами с кораблей. Только что увидел, что от 2-й бригады линейных кораблей к 1-й идёт толпа; кажется с требованием арестовать офицеров... Близ «Кречета» в порту — огромная толпа. Митинг.

4 марта. Переговоры Непенина с депутатами были длительны и очень несносны. Жалко было смотреть на Непенина — так он устал, бедняга, и с таким трудом сдерживался... Назавтра адмирал разрешил собрания команд, а позже — депутатов от команд — в столярной мастерской... Адриан Иванович как-то сразу сдал.

5–15. Провокация по радио — смерть тиранам и прочее. Как это! Какое безумие! Развал полный!

8–10. Дал мысль командующему флотом снять царские портреты. Это приказано. Депутаты к Адриану приходили — выслушал. Приказано в столярной мастерской приготовить для депутатов команд чай и хлеб.

11–30. Мне передал Романенко (мой вестовой), будто часть офицеров объявили командующим флотом адмирала Максимова. Что это ещё!?

11–40. Только что прибыл с Львом Муравьевым вице-адмирал Максимов в сопровождении матросов, которые заявили, что избрали Максимова командующим флотом. Непенин ответил, что он согласен, но, до санкции правительства может согласиться лишь на такое решение: сюда приедет Максимов и будет контролировать все поступки Непенина, т.е. без его совета ничего не делается. Максимов иронизирует: «Вчера я был арестован, сегодня возведён в командующие флотом, завтра буду повешен!»... Толпы с красными флагами на улице. Приказано объявить желательность крас-

ных повязок и участия офицеров в манифестациях.

12–00. В общем, царит анархия полная... Романенко мне сообщил, что на собрании команд выбрали штаб, и команда оказала мне доверие, выбрав в штаб.

13–10. Очередная новость: нас всех арестуют.

13–45. Адриан Иванович Непенин убит. Повели почти всех куда-то; здесь остались Черкасский, Сполатбог, я, Комелов — для дел, о чём дал записку делегату.

17–25. В настроении перелом. Комфлот объезжает суда с депутатами. Кричат «ура».

23–00. Я ошибся... Сейчас «Андрей Первозванный» заявил, что он не закроет красного огня, не выпустит офицеров и т.д., пока не будут выполнены его требования...

5 марта. 9–05. Красные флаги спущены, организован Исполнительный Комитет Совета Солдатских, Матросских и Рабочих Депутатов, власть в руках: 1. Исполнительный Комитет, 2. Комфлот. На судах спокойно. Нервность всюду ужасная. Провокация страшнейшая. Только что узнал, что по городу распространяется «Манифест Николая II с призывом к восстанию в пользу престола»... Враги родины видимо работают во всю и сеют новую смуту. Это грозная опасность. Министр Финляндии Родичев, по соглашению с комфлотом, просит Совет Министров восстановить финляндское войско.

10–25. Только что невдалеке раздалось несколько ружейных выстрелов — оказалось, что убит командир порта генерал Протопопов.

13–20. Говорил с матросскими депутатами из Петрограда, товарищем Ско-

белевым и Львом Муравьевым — решено устроить собрание офицерских депутатов».

ГАМИЛЬТОН

Завершая очерк, вернёмся вновь к самому молодому из главных героев «магдебургской» истории. Михаил Васильевич Гамильтон родился в Твери в 1890 году. После окончания Морского кадетского корпуса в 1910 году служил на Балтике. Закончил войну флаг-капитаном штаба БФ, т.е. старшим офицером штаба. После заключения Брестского мира М. В. Гамильтон был уволен с флота. Летом 1918 года примкнул к Белому движению на севере России. После поражения белых в 1920 году он эвакуировался из Архангельска в Норвегию, затем во Францию. Поселился в Париже, долгое время выполнял обязанности адъютанта бывшего руководителя Белого движения на русском Севере генерала Миллера, пока того не похитили агенты НКВД в 1937 году. Умер Михаил Владимирович во Франции в 1975 году.

* * *

Таков глубокий и печальный след, оставленный Революцией в судьбах главных героев «магдебургской» истории, достойно потрудившихся во славу России. Отрадно, что память об их делах на благо Отечества постепенно возрождается. Свидетельством тому публикации в интернете и выставки, приуроченные к 100-летию гибели адмирала А. И. Непенина, книги и статьи, посвящённые балтийским радиоразведчикам.

ЛИТЕРАТУРА

1. Карпов Д. И. И. Ренгартен. Некролог. // Морской сборник. 1920. № 1–3.
2. Кикнадзе В. Г. Развитие сил и средств радиоразведки отечественного военно-морского флота в первой половине XX века: исторический опыт и уроки: дис. д-ра ист. наук. Военная академия ГШ ВС РФ, 2014.
3. Февральская революция в Балтийском флоте (Из дневника И. И. Ренгартена) // Красный архив. 1929. Т. 32.



Александр БОДРИК
заместитель генерального
директора ANGARA
Professional Assistance

КИБЕРБЕЗОПАСНОСТЬ ПО АДИЗЕСУ

ЗАМЕТКИ БЕЗОПАСНИКА

Многие специалисты по кибербезопасности сталкиваются с «необъяснимым» — организации внутри отрасли, находясь в примерно одинаковых финансовых условиях и внешней среде, ведут себя совершенно по-разному. Можно было бы списать все на пресловутый «человеческий фактор», но в мире бизнеса уже был найден более общий ответ — методология «жизненного цикла организаций» от бизнес-тренера Ицхака Кальдерона Адизеса.

«ЖИЗНЕННЫЙ ЦИКЛ ОРГАНИЗАЦИЙ»

Методология описывает развитие организаций (в первую очередь бизнес-организаций) по аналогии с живым организмом и выделяет 10 этапов развития:

- ◆ Ухаживание (рост) — проработка идеи бизнеса.
- ◆ Младенчество (рост) — запуск бизнеса и погоня за денежным потоком.
- ◆ Давай-Давай (рост) — агрессивный рост и погоня за долей рынка.
- ◆ Юность (рост) — реструктуризация и фокусировка бизнеса.
- ◆ Расцвет (рост) — стабильный устойчивый рост.
- ◆ Стабильность (старение) — резкое замедление или отсутствие роста.
- ◆ Аристократия (старение) — начало преобладания формы над сутью бизнеса.

◆ Бюрократия (старение) — преобладание формы над сутью бизнеса.

◆ Охота на ведьм (старение) — начало распада и дезинтеграция бизнеса.

◆ Смерть (старение) — окончательный распад и конец функционирования бизнеса.

ЭТАПЫ РОСТА

На этапах «Ухаживание» и «Младенчество» бизнес обычно не обращает внимания на кибербезопасность — слишком много других более очевидных проблем/рисков. К примеру, нечем платить зарплату, под вопросом востребованность продуктового предложения, тяжело пригласить в штат талантливых сотрудников.

На этапе «Давай-Давай» компании развивают функцию кибербезопасности, если у менеджмента находится на это время. Если время есть, кибербезопасность может быть, хоть и хаотично, но переразвита («Давай-Давай» вообще склонен к перекосам). Что в свою очередь иногда влечет за собой конфликты с общей культурой бизнеса, которая еще ориентирована скорее на принятие, чем на снижение рисков.

Кстати, на всех этапах роста бизнес ориентирован скорее на принятие рисков, а значит, крайне важны механизмы их идентификации и измерения — чтобы понять, когда принятие рисков обойдется себе дороже. Без таких меха-

низмов «Давай-Давай» живет с кибербезопасностью, движимой постоянными инцидентами.

«Юность» знаменуется внутренним конфликтом между духом предпринимательства (устремление в будущее и принятие рисков) и необходимостью уже сейчас выстраивать процессную платформу для последующего устойчивого роста. Кибербезопасность в таких условиях развивается хаотично, как, впрочем, и многие другие функции бизнеса. Этот период нужно проходить взвешенно: развивая функцию в очевидных направлениях, например, в направлениях управления доступом и повышения осведомленности пользователей, и постепенно формируя фокус на внедрение понятных и масштабируемых базовых процессов кибербезопасности. Тем более, что в «Юности» бизнес должен научиться жить без своего владельца, внедрив институты развития предпринимательской инициативы у сотрудников.

На стадии «Расцвет» базовые процессы бизнеса (и кибербезопасности в том числе) так или иначе выстроены, достигнут определенный баланс между принятием и снижением рисков. Бизнес понимает, чего он хочет, и устойчиво развивается, что делает необходимым постепенный переход на сервисную модель кибербезопасности, а также повышение степени де-



Рисунок 1. Схема жизненного цикла организации по Адизесу

централизации — чтобы предоставить бизнес-подразделениям необходимую степень гибкости при принятии решений на рынках.

На этом этапе бизнес охотно инвестирует в проекты, которые имеют понятную финансовую отдачу и безопасность может рассматриваться почти как равноправная бизнес-функция. В этот период бизнес может стремиться достичь state-of-the-art практик, считая себя в силах превзойти и в конечном итоге победить конкурентов. В то же время преобладание коммерческого взгляда на проекты в сочетании с вдумчивым подходом еще не позволяет скатиться в бездумное расходование корпоративных ресурсов.

ЭТАПЫ СТАРЕНИЯ

Этапы «Стабильность» и «Аристократия» для кибербезопасности схожи — бизнес начинает испытывать проблемы с ростом, но пока еще серьезной проблемы в такой ситуации не видит. Снижение рисков начинает превалировать над их принятием, но так как видимых проблем у бизнеса особенно не видно, то говорить о рисках ему

тоже не хочется. Поэтому значимый объем рисков «заматывается под ковер», и ключевым драйвером становится соответствие применимым нормативным требованиям (compliance). Compliance вроде как и не риск, а просто плата за ведение бизнеса в определенной отрасли определенного региона, поэтому обсуждать его ментально проще, и проекты для соответствия требованиям одобряются охотнее.

Этап «Бюрократия» знаменует окончательной победой формы над сутью — процесс становится важнее результата. Риски никого не интересуют, если соблюдены все инструкции, а несоблюдение инструкций или нормативных требований (даже если они относятся к организации постольку-поскольку) становится единственным стимулом для хоть какого-то развития ИБ. Впрочем, «Бюрократия» имеет и свой плюс: существующие достижения и процессы кибербезопасности защищены от посягательств бизнеса — равно как и любые другие ранее согласованные и утвержденные процессы.

Последние этапы функционирования организации («Охота на ведьм»

и «Смерть») отличаются широким использованием кибербезопасности как карающего элемента. Никого уже не интересуют ни риски, ни compliance — лишь возможность свести счеты с политическими конкурентами, продлить свое существование на тонущем корабле. Впрочем, в настоящей кибербезопасности потребности уже и нет — люди и процессы начинают замирать, денег почти нет, и даже киберпреступности этот бизнес становится малоинтересен.

ЭТАПЫ РАЗНЫЕ НУЖНЫ

Организации непрерывно рождаются, растут, процветают и стареют — конкурируя, поглощая и побеждая друг друга. Все этапы развития организации естественны и по-своему нужны, и на каждом этапе кибербезопасность так или иначе помогает бизнесу развиваться (не отвлекаясь на угрозы) или продлить существование. Понимание цикла развития организации и ее текущего статуса помогает управлять системой кибербезопасности более эффективно, а организацию защищать более результативно.



Алексей ПЛЕШКОВ
независимый эксперт
по информационной
безопасности

ЗНАЛ БЫ, ГДЕ УПАДЕШЬ...

ЧТО НА САМОМ ДЕЛЕ ЖДЕТ
ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ
В 2018 ГОДУ?

Перед самым Новым годом увидел свет прогноз, в котором представители известных в мире компаний и признанные профессионалы в сфере киберзащиты определили ТОП-10 наиболее вероятных сценариев поведения рынка ИБ в России и мире.

Если кратко, то основными тенденциями на 2018 год были названы:

1. использование машинного обучения и искусственного интеллекта киберпреступниками;
2. дальнейшее развитие вирусов-вымогателей;
3. эксплуатирование уязвимостей в устройствах класса IoT;
4. взломы СМИ и аккаунтов в социальных сетях для распространения ложной информации;
5. рост атак на промышленные предприятия и атак на цепочки поставок;
6. нашествие безфайловых и облегченных вирусов;
7. атаки на мобильные приложения;
8. атаки на облачную инфраструктуру и хранилища;
9. эксплуатация уязвимостей в мобильных сетях, а также протоколах Wi-Fi и Bluetooth;
10. ренессанс аппаратных атак.

Думается, что данный ТОП — не более чем скрытая реклама товаров и услуг ведущих игроков на рынке ИБ. Как продукт кропотливой работы маркетологов, он содержит описание наиболее интересных и до конца непонятных обывателю современных технологий: «большие данные», «Интернет вещей», всеобщая мобилизация, усложнение «архитектуры облаков»... Доподлинно неизвестно, кто

и как формировал этот ТОП, проводилось ли статистическое исследование и сбор компетентных мнений. И не случайно, видимо, ряд важных с точки зрения развития и обеспечения ИБ направлений в этот ТОП-рейтинг не попали. С целью восстановления равновесия между желаниями маркетологов и фактическим состоянием рынка, автор подготовил альтернативный прогноз, содержащий тенденции, более приближенные к реальности.

КИБЕРАТАКИ ВО ВРЕМЯ ВЫБОРОВ 2018. ОНИ НАС, А МЫ ИХ

Атаки злоумышленников на сотрудников, автоматизированные системы и технические решения, задействованные при проведении президентских выборов. Весь 2016 и часть 2017 года прошли под лозунгом иностранных СМИ о том, что якобы российские хакеры и российские спецслужбы сыграли не последнюю роль в выборах президента США. Ответственные чиновники и лица, приближенные на тот момент к кандидатам в президенты, наперебой сообщали о взломах, компрометациях и утечках конфиденциальной информации. Споры не утихают до сих пор.

Немудрено предположить, что те же киберпреступники, которые стояли за атаками на команды кандидатов в президенты США, будут заинтересованы в повторении своего успеха на выборах президента России. Таким образом, с января по март 2018 года следует ожидать наряду с официальными утечками и разоблачениями, попадание в общий доступ неофици-

альной информации и компромата, неработоспособность ключевых ресурсов и повышение всеобщего интереса к вопросам информационной безопасности.

«НЕ ЛОМИМСЯ В ДВЕРЬ— ВОЙДЕМ ЧЕРЕЗ ДЫМОХОД»

Кибератаки злоумышленников на сервисные и аффилированные с крупными игроками компании в России. В 2016 году известные своими социально-инженерными экспериментами группы злоумышленников обновили инструменты и методики, восполнили за счет «новой крови» кадры, значительно прореженные правоохранительными органами, потренировались «на кошечках» и совершили несколько резонансных кибератак на довольно крупные сервисные компании. Используя похищенные базы данных адресов клиентов, проектной документации, почтовой переписки и т.д., злоумышленники спланировали и поэтапно реализовали в третьем и четвертом кварталах 2017 года ряд громких преступлений.

Если предположить, что те же злоумышленники завладели и персональными данными доверенных клиентских менеджеров, и информацией о партнерских схемах работы, то ущерб от планируемых к реализации в начале 2018 года атак окажется колоссальным.

«НЕВАЖНО, КАК БЕЖИТ САМАЯ БЫСТРАЯ ЛАНЬ, ЛЕВ СЪЕСТ САМУЮ МЕДЛЕННУЮ»

Целевые атаки на финансовые организации и компрометация платежных и операционных платформ. В 2017 году по миру прокатилась се-

рия громких атак, направленных на вывод денег со счетов с использованием инструментов по переводам, реализованных на традиционных для банковской сферы платформах. Международные платежные системы, платежная система SWIFT и некоторые другие были использованы в качестве транспорта для вывода и обналичивания украденных со счетов денежных средств.

2018 год продолжит эту молодую пока традицию. Конечно, многие банки перестраховались и выстроили эшелонированную защиту, серьезно вложившись в обновление инфраструктуры ИБ, но в России таких банков единицы. У нас по-прежнему действует принцип «Пока гром не грянет, мужик не перекрестится» — большинство банков продолжают минимизировать затраты на защиту и демонстрировать в МСФО-отчетности стабильно высокий финансовый результат. АО «КБ «Глобэкс», «Севастопольский морской банк»... кто следующий? 2018 год покажет.

«НА ДУРАКА НЕ НУЖЕН НОЖ: ЕМУ С ТРИ КОРОБА НАВРЕШЬ — И ДЕЛАЙ С НИМ ЧТО ХОШЬ!»

Активное развитие фишинговых технологий и социальной инженерии как методов подготовки и проведения комплексных киберпреступлений. Как бы сложно и комплексно ни защищали специалисты по ИБ введенный им информационный актив, самым слабым звеном в цепи по-прежнему остается человек. В 2017 году воздействию на подсознание с помощью заведомо ложной, но любопытной, важной, пугающей, настоявающей и прочей информации подвергался, по разным данным, каждый первый пользователь сети Интернет. Пенсионерка, получающая по электронной почте фотографии внуков или уведомления от социальной службы, экскурсовод в музее, обменивающийся в перерывах между группами мгновенными сообщениями с родственниками, моряк, ждущий в плавании вестей из дома, и многие другие — все они вне зависимости от социального статуса находятся в группе риска.

У НАС ПО-ПРЕЖНЕМУ ДЕЙСТВУЕТ ПРИНЦИП «ПОКА ГРОМ НЕ ГРЯНЕТ, МУЖИК НЕ ПЕРЕКРЕСТИТСЯ» — БОЛЬШИНСТВО БАНКОВ ПРОДОЛЖАЮТ МИНИМИЗИРОВАТЬ ЗАТРАТЫ НА ЗАЩИТУ И ДЕМОНИСТРИРОВАТЬ В МСФО-ОТЧЕТНОСТИ СТАБИЛЬНО ВЫСОКИЙ ФИНАНСОВЫЙ РЕЗУЛЬТАТ

Злоумышленникам неинтересно, кого и как они взломали. Этот математический «+1» к количеству скомпрометированных и подконтрольных терминалов шаг за шагом в будущем выльется в «+1000» к построенной бот-сети, к организации целевой атаки или проведению показательной политической акции. На современном витке хакерской эволюции для определенных групп киберпреступников главным результатом является сам факт компрометации, а кто именно и насколько подвержен этой компрометации — вопрос второстепенный.

В 2018 году активное заражение продолжится пропорционально, или даже опережая, любимую и ожидаемую многими экспертами массовую диджитализацию.

«НАШЕЙ ОРГАНИЗАЦИИ ТРЕБУЕТСЯ ОБНОВЛЕНИЕ И ОМОЛОЖЕНИЕ ПЕРСОНАЛА»

Активное вовлечение по всему миру новых специалистов в ряды хакерских и олоухакерских группировок.

Сегодня нестабильная экономическая ситуация подвигает молодых людей разных стран задумываться о своем будущем раньше, чем это было в девяностые-нулевые годы. Технически грамотные ребята активно ищут применение своим навыкам: кто-то идет в науку, кто-то в коммерческие проекты, а кто-то в сферу киберпреступности. Целевые атаки и политические акции так же требуют рабочих рук. Не все студенты и выпускники вузов смогли в 2017 году найти работу по профилю, с наступлением 2018 года спрос на специалистов в виртуальном мире как минимум не уменьшится...

ЗНАЛ БЫ, ГДЕ УПАДЕШЬ...

Сложно делать прогнозы в такой скачками развивающейся сфере, как ИБ. Еще вчера руководитель компании не мог и представить возможности ущерба от отсутствия на своих рабочих станциях актуальных обновлений по ИБ. А сегодня, после захвата «ушастым» вирусом-шифровальщиком каталогов с отчетной и клиентской информацией, он считает убытки и подумывает о продаже бизнеса. Совсем недавно мы с благожелательным интересом следили за развитием одного из иностранных производителей мобильных телефонов. Ровно до того момента, пока не получили подтверждения фактов технической слежки за пользователями этих мобильных телефонов.

В советское некомпьютеризированное время лозунг «Храните деньги в сберегательной кассе!» звучал как гарантия сохранности денег. Сегодня физические и юридические лица, периодически подвергаясь атакам злоумышленников, теряют уверенность в сохранности чего-либо где-либо, и от безысходности апеллируют только к правоохранительным органам в надежде хотя бы на частичный возврат похищенного.

* * *

Тем не менее, чтобы не допустить рецидивов кибератак и мошенничества, целесообразно держать руку на пульсе современных тенденций, отделять маркетинговые угрозы от реальных и разбираться в инструментарию по минимизации рисков. Недаром говорят: «Знал бы, где упадешь, соломки бы подстелил!»

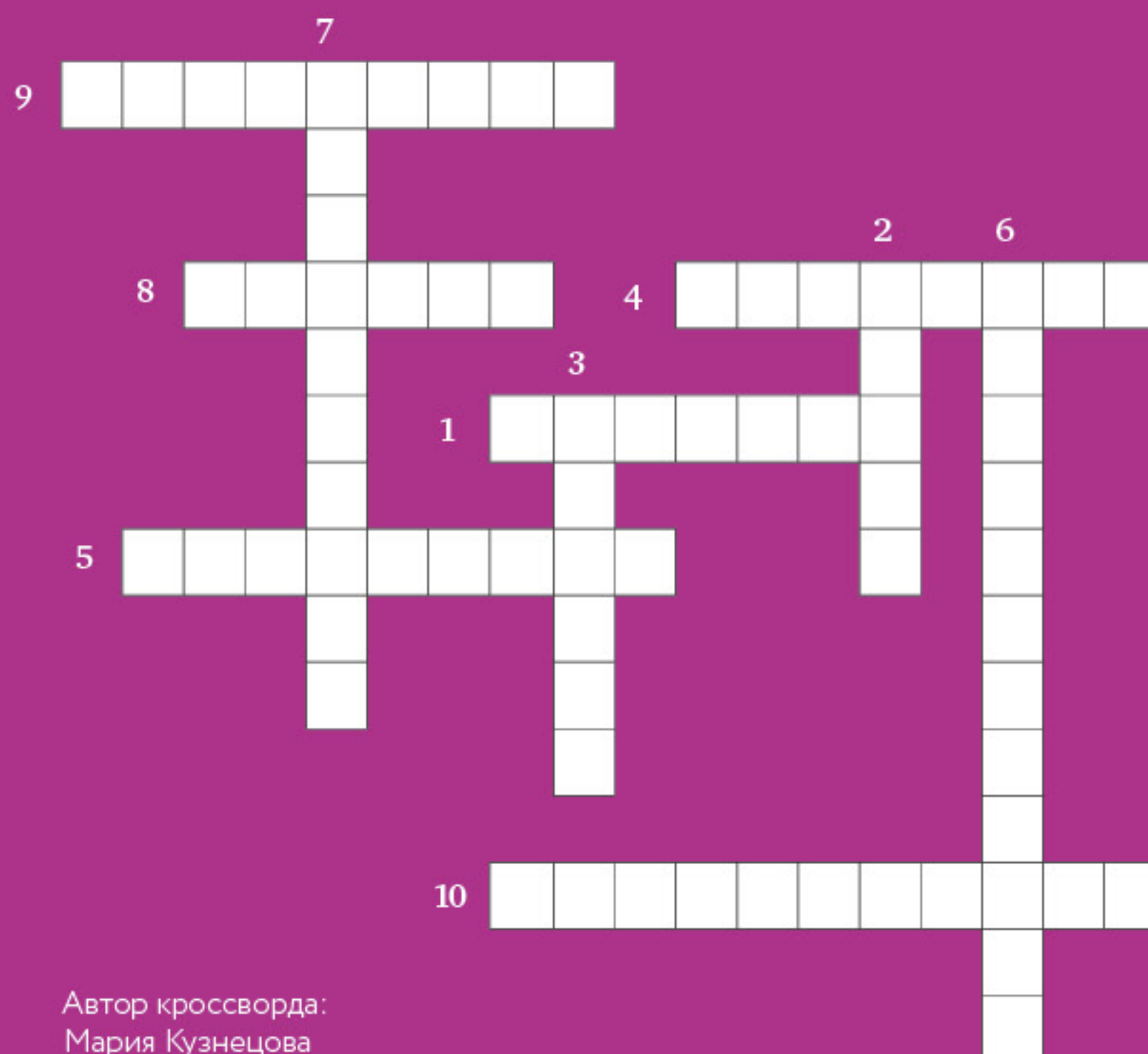
КРОССВОРД

ПО ГОРИЗОНТАЛИ

1. Похищение, добывание, собирание и передача с целью корыстного использования или выдачи конкуренту (противнику) сведений, составляющих тайну.
4. Пара букв (символов), блоков текста.
5. Свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.
8. Ограничение, накладываемое собственником, на доступ к информации, документам, базам данных и т.п.
9. Программа, используемая для преобразования исходной программы в машинный код или перемещаемую программу.
10. Изображение электронного документа на экране дисплея. В полном смысле слова документом не является.

ПО ВЕРТИКАЛИ

2. Совокупность ограничительных правил, норм, обеспечивающих контролируемый доступ и пребывание на определенной территории, регулирующих порядок ознакомления с защищаемой информацией и документами.
3. Документ, удостоверяющий исключительное право, авторство и приоритет изобретения, полезной модели либо промышленного образца.
6. Документ, изготовленный автоматически средствами вычислительной техники на бумажном носителе в машиночитаемой форме и предназначенный для оформления в установленном порядке.
7. Средство защиты информации, реализующее математический алгоритм преобразования информации.



Автор кроссворда:
Мария Кузнецова

С НОВЫМ ГОДОМ!



ЮМОР ИБ

ИЗ НОВОГОДНЕГО ОБЗОРА

Вспоминая 2017 год, понимаешь: нам есть, что вспомнить (WannaCry, Ретя...), но нечего обсудить. Депутаты штамповали законы. Регуляторы регулировали. Хакеры хакали. Банки плакали...

Хакеров в мире мало, но они распределились по всемирной паутине так, что встречаются практически на каждом шагу...

«Чудес в мире — как мух в сортире, а нужного — не видать» (про искусственный интеллект, машинное обучение, блокчейн, биткойн и др.).

Ресурсы для повышения ИБ в компании есть всегда, нужно только взломать пару компьютеров в совете директоров.

Вендоры настойчиво предлагают решения «следующего поколения», не уточняя, что делать с решениями, приобретёнными у них вчера.

Чем круче джип, тем дольше идти за трактором (про системы защиты ИБ).

Хорошее взаимодействие служб ИБ — следствие плохого законодательства.

Сегодня новости «кибермошенники взломали сервис/компанию/банк» воспринимаются как «ожидается кратковременный дождь». Только у практикующих ИБ-шников при этом почему-то начинает дергаться глаз.

Все более реальным становится риск, что в ходе широкомасштабной атаки будет уничтожен весь Интернет.

Поделится Валерий Естехин
<https://estekhin.blogspot.ru>

ОБЛАЧНЫЙ ТОКЕН С НЕИЗВЛЕКАЕМЫМИ КЛЮЧАМИ



НАИВЫСШАЯ СТЕПЕНЬ ЗАЩИТЫ КЛЮЧЕЙ ОТ КОМПРОМЕТАЦИИ

Ключи пользователей создаются и хранятся в защищенном криптографическом модуле HSM, оставаясь неизвлекаемыми. HSM снабжен датчиками вскрытия, контролем портов, механизмами доверенной генерации и уничтожения ключей, защитой от утечек по побочным каналам – и это далеко не все. Ключи надежно защищены даже от внутреннего нарушителя, являющегося администратором. Схемы аутентификации пользователей имеют уровень безопасности не ниже, чем у самих хранимых ключей. Ключи становятся не просто неизвлекаемыми, но и некомпromетируемыми.



ПОДЛИННАЯ МОБИЛЬНОСТЬ ПОДПИСИ

Забудьте про связку из токенов, USB-хаб и установку драйверов. Вы больше не будете привязаны к одному рабочему месту – к вашему ключу в облаке вы можете получить доступ из любого места и с любого устройства: с настольного компьютера, ноутбука, планшета, смартфона и простого «телефона-звонилки» даже без Интернета.

УСТАНОВКА СРЕДСТВ ЭЛЕКТРОННОЙ ПОДПИСИ НЕ ТРЕБУЕТСЯ

На рабочее место пользователя, которым может быть и мобильное устройство, нужно установить лишь простое в использовании легковесное средство аутентификации. Отсутствие средств электронной подписи на рабочем месте позволяет обеспечить централизованное управление ключами пользователей в корпоративной сети.



ПРОИЗВОДИТЕЛЬНОСТЬ, НАДЕЖНОСТЬ И ОТКАЗОУСТОЙЧИВОСТЬ

Вычисление электронной подписи на облачном токене происходит со скоростью, сравнимой со скоростью работы «фермы» из тысяч USB-токенов. Простым увеличением аппаратных ресурсов можно масштабировать производительность до любого необходимого уровня. В отличие от физического, облачный токен никогда не сломается и не потеряется. Аппаратное резервирование серверных компонент позволит пережить любой сбой незаметно для пользователей.

СОХРАНЕНИЕ ИНВЕСТИЦИЙ

Вам не придется менять или дорабатывать систему документооборота. Не нужно отказываться от привычного ПО для работы с электронной подписью. Все, что умеет работать со стандартом де-факто российского рынка средств ЭП – КриптоПро CSP, при установке облачного криптопровайдера бесшовно сможет использовать облачные токены. Не спешите выбрасывать и аппаратные токены, они смогут послужить в качестве средств аутентификации к ключам пользователей в облаке. Для перехода на алгоритм ГОСТ Р 34.10-2012 не нужно покупать ни новые токены, ни новое ПО – переход не потребует дополнительных вложений*.

*В рамках расширенной технической поддержки.



СНИЖЕНИЕ СТОИМОСТИ ВЛАДЕНИЯ

По сравнению с локальными средствами ЭП, аппаратными токенами и смарт-картами, при использовании облачных токенов существенно упрощаются процедуры передачи СКЗИ пользователям и установки средств ЭП на рабочие места. Централизованное хранение ключей с аппаратным резервированием, высокая производительность и возможность обслуживания множества пользователей одним сервером значительно уменьшают стоимость владения данным решением.

ПЕРВОЕ СЕРТИФИЦИРОВАННОЕ СРЕДСТВО ОБЛАЧНОЙ ПОДПИСИ

Сервер электронной подписи КриптоПро DSS является первым и единственным сертифицированным ФСБ России облачным средством электронной подписи. Идет процесс сертификации исполнений с новыми способами аутентификации и облачным криптопровайдером.



АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Книжное
издательство

ib-bank.ru