



13> Артем СЫЧЕВ
(Банк России)
Прямая линия



20> Ольга ДЕРГУНОВА
(Банк ВТБ)
**«Цифровая экономика –
сервис эволюции, рынка...»**

26> Григорий МАРШАЛКО
(ТК 26)
**Угрозы безопасности
биометрических систем**

36> Василий ОКУЛЕССКИЙ,
Евгений СОЛОВЬЕВ
(АО НСПК)
**MirAccert – революция
платежных систем**

49> Александр БОДРИК,
Евгений СОКОЛОВ
(ANGARA Professional Assistance)
Живая вода для SOC

ЦИФРОВАЯ ЭКОНОМИКА: КАЧАЯ ЦИФРУ



22 ноября 2017 года, г. Москва,
Конгресс-парк гостиницы
«Рэдиссон Ройал Москва»

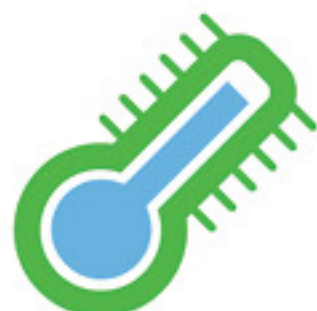


SOC-ФОРУМ 2017

ПРАКТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ И ПОСТРОЕНИЯ ЦЕНТРОВ МОНИТОРИНГА ИБ



Самая масштабная конференция
в отрасли — более 1200 участников



Более 50 докладов, охватывающих
наиболее «горячие» темы



Собственные секции проведут
флагманы российской отрасли ИБ



Демонстрация решений и сервисов
государственных ведомств



Пристальное внимание
федеральных и отраслевых СМИ

Регистрация:
SOC-FORUM.IB-BANK.RU





Игорь НЕКРАСОВ
главный редактор
BIS Journal

Безусловно, цифровая экономика — это совсем близкое будущее России. Но известно об этом будущем пока очень мало. В конце июля Владимир Путин подписал программу «Цифровая экономика Российской Федерации», в которой собственно только обозначены цели и задачи до 2025 года. В конце августа по каждому из направлений программы были определены центры компетенций и руководители рабочих групп, призванные довести эскиз до стадии рабочего проекта. По направлению «Информационная безопасность» центром компетенций стал Сбербанк, а руководителем рабочей группы Наталья Касперская.

Наталья Ивановна на просьбу рассказать, что же происходит, ответила, что программа очень сырая («цифры есть, а экономики нет»), работа только началась... и взяла тайм-аут на два-три месяца, пообещав BIS Journal первое интервью. Примерно то же самое передал через пресс-секретаря и Станислав Кузнецов, мол, работа в Сбербанке кипит, как только будет что показать, вы узнаете об этом первыми. В этом смысле, не сомневаюсь, в первом номере 2018 года BIS Journal будет что почитать, а на Уральском форуме — что обсудить.

Но это совсем не значит, что в этом номере читать нечего. Какой бы сырой ни была программа цифровой экономики, вектор движения задан, и позиция банковского сообщества должна быть озвучена. Что и сделала в своем интервью со свойственной ей яркостью зампред правления Банка ВТБ Ольга Дергунова. Конечно, с уклоном в сторону ИБ. Позицию Госдумы представил Анатолий Аксаков. Оказалось, законодатели активно работают над регулированием цифровой индустрии, и им уже есть что предъявить. А чтобы слегка остудить горячие головы, хмелеющие от футуристических слов и связывающие будущее исключительно с блокчейном, искусственным интеллектом, облаками, биометрией и т.д., мы, не отрицая стремительного взлета цифровой эволюции, завели рубрику «Обратная сторона финтеха». Там масса интересного.

Кроме того, в номере много земного и крайне полезного. Василий Окулесский выполняет обещание, данное в прошлом номере, и представляет MirAccept — маленькую революцию платежных систем. Известный гештальт-терапевт отрасли Александр Бодрик на живых примерах доказывает, что практическая ИБ и настоящий SOC — это искусство возможного, овладев которым легко защитить любую компанию от киберугроз... почти без денег (Но это не дословно!). А специалист в области повышения ИБ-осведомленности персонала Игорь Долотин учит, как правильно выбивать всё те же деньги из руководства...

И конечно, есть нота праздника. Пришла пора юбилеев. Нашему издателью Медиа Группе «Авангард» — 10 лет, РКІ-форуму — 15 лет, а впереди — самое грандиозное торжество — 10 лет Уральскому форуму.

Пора собираться.

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

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. — главный советник, компания «РНТ», кандидат технических наук

Левинов Д.О. — председатель Совета НП «Партнерство специалистов по информационной безопасности»

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

Некрасов И.В. — главный редактор журнала

Окулесский В.А. — начальник управления безопасности АО «НСПК», кандидат технических наук

Пазин С.В. — начальник Управления по обеспечению информационной безопасности ОАО Банк ВТБ, кандидат физико-математических наук

Шумский Л.С. — начальник Управления контроля информационных рисков, ДОР (АО) Связной Логистика

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

ЭКСПЕРТНАЯ ГРУППА

Одувалов М.В. — эксперт BIS Journal

Филиппчук А.А. — вице-президент АБ «ГПБ-ипотека» (группа «Газпромбанка»)

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**

Шеф-редактор: **Былевский П.Г.**

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

Арт-директор: **Мельников Н.С.**

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

Северный В.П., Хвастунова О.Н.

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

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

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

Цветокорректор: **Науменко М.Б.**

Корректор: **Бальтерманц Л.Ф.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»

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

Координаты: 55.779380, 37.61150

Тел./факс: +7 499 271-70-85

Интернет-версия: journalib-bank.ru

E-mail: bis@ib-bank.ru

Отдел рекламы: reklama@ib-bank.ru

Отдел распространения: tirazh@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство ПИ № ФС77-55062 от 14 августа 2013 г. Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность банков».

Перепечатка и воспроизведение иными способами без разрешения редакции запрещаются.

При использовании материалов

ссылка на журнал обязательна.

Мнение редакции может не совпадать с мнением авторов.

Присланные материалы не рецензируются и не возвращаются.

Подписан в печать 03.11.2017. Тираж 7000 экз.

Заказ № 987/56. Цена договорная.

Отпечатан в «Типографии на Угрешской»

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

Тел.+7 495 720-62-28

© BIS Journal, 2017



НОВОСТИ

5 В России, в мире, компании, образование

РЕГУЛЯТОРЫ

- 10 Антифрод**
Павел БЫЛЕВСКИЙ (BIS Journal)
На смену сенсациям пришла плановая работа
- 13 Прямая линия**
Артём СЫЧЕВ (Банк России)
«Безопасность немыслима без специального образования»



ТЕМА НОМЕРА: ЦИФРОВАЯ ЭКОНОМИКА

- 18 Законодательство**
Анатолий АКСАКОВ (Государственная Дума РФ)
Цифровой экономике — эффективность и безопасность
- 20 От первого лица**
Ольга ДЕРГУНОВА (Банк ВТБ)
«Цифровая экономика — сервис эволюции, рынка...»
- 26 Обратная сторона финтеха**
Григорий МАРШАЛКО (ТК 26)
Не панацея
- 28 Обратная сторона финтеха**
Алексей ПЕРЦЕВ (Digital Security)
Большие достоинства — большие недостатки
- 32 Обратная сторона финтеха**
Алексей АРХИПОВ (QIWI)
Экономика токенов
- 33 Обратная сторона финтеха**
Андрей КУРИЛО (НП НСФР)
Трудный путь к универсуму





БАНКИ

36 НСПК

Василий ОКУЛЕССКИЙ (эксперт ИБ), Евгений СОЛОВЬЕВ (АО НСПК)
MirAssert. Чтобы покупать с удовольствием!

УГРОЗЫ И РЕШЕНИЯ

46 Судебная практика

Евгений ЦАРЕВ (RTM Group)
Многоликая экспертиза

49 SOC

Александр БОДРИК, Евгений СОКОЛОВ
(ANGARA Professional Assistance)
Живая вода для SOC

52 SOC

Евгений АФОНИН (Micro Focus),
Виктор СЕРДЮК (АО «ДиалогНаука»)
SOC не равен SIEM

56 SOC

Максим ФИЛИППОВ (Positive Technologies)
Может ли эффективная SIEM-система стоять дешевле?

58 SOC

Станислав МЕРЗЛЯКОВ (АМТ-ГРУП)
Нужен ли SOC? Решать вам!

60 Системы контроля

Дмитрий МИХЕЕВ («АйТи БАСТИОН»)
Никак иначе

62 Аутсорсинг

Алексей ЦВЕТКОВ («Информзащита»)
Финансы в порядок!

64 Удаленный доступ

Владимир ГЕРАСИМЕНКО,
Иван ГРИГОРЬЕВ (ООО «САФИБ»)
Рука помощи

66 Аутсорсинг

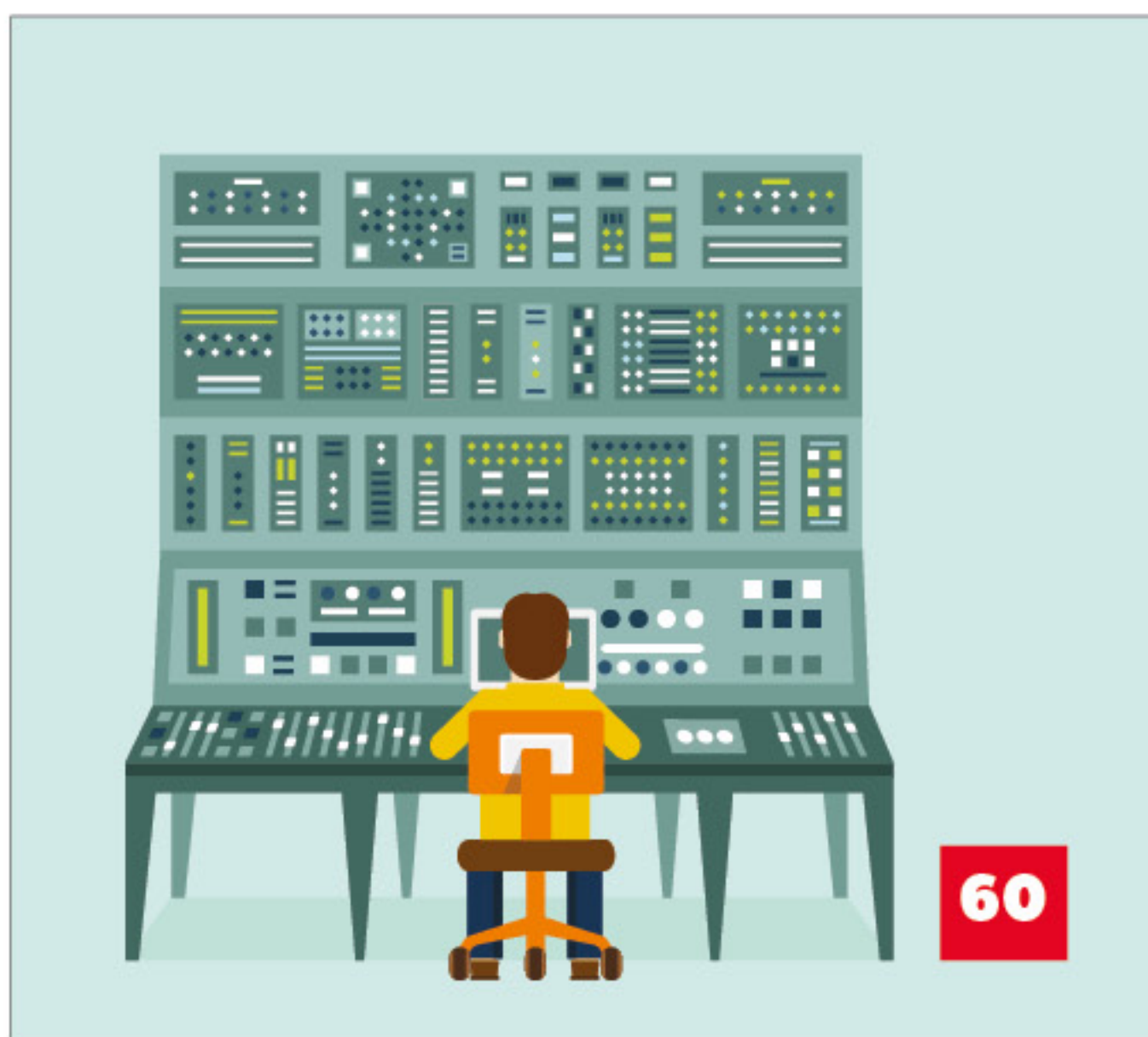
Евгений АКИМОВ (ГК Softline)
Победа над временем

68 Symantec

Дарья ОРЕШКИНА (Web Control)
Защита самого ценного

71 На правах рекламы

Мария ЛУРЬЕ (ООО «С-Терра СиЭсПи»)
Как Мартын информацию защищал



ИНФРАСТРУКТУРА

- 74** **Деловые мероприятия**
Салют над Невой
- 78** **Деловые мероприятия**
InfoSecurity Russia 2017
- 80** **Деловые мероприятия**
Валерий КУЛИКОВ (BIS Journal)
Табун троянских коней
- 83** **Деловые мероприятия**
Николай КОЛЬСКИЙ (BIS Journal)
Skolkovo Cyberday 2017



ОБРАЗОВАНИЕ И КАРЬЕРА

- 86** **Персонал**
Игорь ДОЛОТИН (UBS)
Как повысить?
- 88** **Обзор**
Марина БРОДСКАЯ (BIS Journal)
Путевка в жизнь
- 94** **Обзор**
Марина БРОДСКАЯ (BIS Journal)
Конкурс растет



СУБЪЕКТЫ

- 98** **Корифеи**
Борис СТОЛПАКОВ (историк криптографии)
Реликвия русского флота
- 102** **Корифеи**
Геннадий ЕМЕЛЬЯНОВ (Академия криптографии РФ),
Дмитрий ЛАРИН (кандидат технических наук)
Криптографы Великой Отечественной
- 106** **Мысли вслух**
Валерий КУЛИКОВ (BIS Journal)
Как в медицине...
- 110** **Мысли вслух**
Александр БОДРИК
(ANGARA Professional Assistance)
Сила простоты



ОФФТОПИК

- 112** **Блогеры усмеваются**
Кроссворд, юмор

КЛЮЧЕВЫЕ ТЕХНОЛОГИИ ОТ ГРЕФА

В своем выступлении на дискуссии Международного клуба «Валдай» в Сочи Герман Греф назвал четыре технологии, которые, по его мнению, определяют будущее страны в ближайшие 5–10 лет.

«Если говорить о Сбербанке, то это, во-первых, искусственный интеллект, который сегодня является уже доминирующей технологией. Во-вторых, блокчейн. И третья технология — робототехника. Для государства будет важна еще и четвертая технология — квантовый компьютер и все, что связано с квантовыми сенсорами, с квантовой криптозащитой», — приводит ТАСС слова Грефа.

Герман Греф также прокомментировал вступление Сбербанка в некоммерческий альянс Enterprise Ethereum Alliance (EEA). «Мы считаем платформу Ethereum одной из самых продвинутых для прикладных задач технологии блокчейн. Мы хотим участвовать в развитии самой технологии, её возможностей и имплементации этих



возможностей в России. Блокчейн может радикально изменить банковский сектор».

EEA создан в феврале 2017 года для поиска возможностей применения технологии блокчейн на платформе Ethereum в реальном бизнесе. Альянс объединяет крупнейшие компании и научно-исследовательские организации: CME Group, Credit Swiss, DTCC, ING, JPMorgan, Santander, UBS, Accenture, Deloitte, Intel, Microsoft и др.

ОПЕРАТОРЫ ОЧИСТЯТ БАЗЫ ОТ АНОНИМОВ

В июне 2018 года в России вступит в силу закон, согласно которому операторы мобильной связи будут обязаны идентифицировать личности всех своих абонентов, в том числе и держателей «серых карт», достоверных данных о которых в клиентских базах сотовых компаний нет.

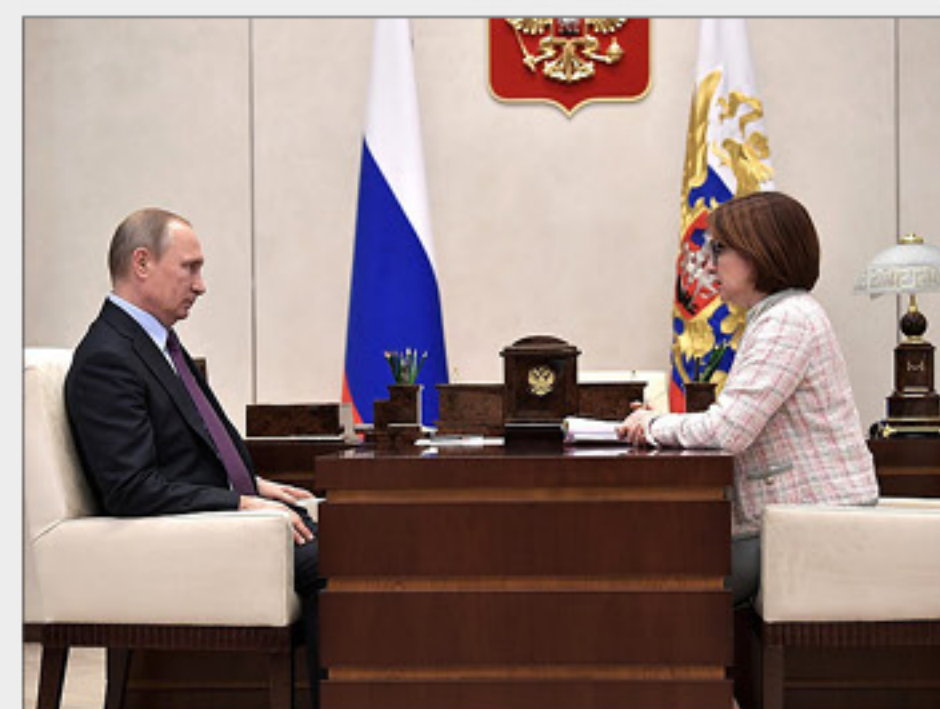
Для идентификации всех пользователей мобильной связи и очистки баз данных от анонимных абонентов Правительство РФ предоставит доступ всем «сотовым» операторам к ЕСИА (Единая система идентификации и аутентификации), дающей возможность подтвердить личность человека через



интернет, и СМЭВ (Система межведомственного электронного взаимодействия), с помощью которой можно проверить достоверность паспортных данных, как это делают кредитные финансовые организации или государственные органы власти.

Изменения в закон «О связи» приняты летом 2017 года, но до этого времени мобильные операторы не были «подключены» к СМЭВ, а разрешение на это не предоставила государственная подкомиссия департамента информационных технологий. На заседании 19 октября «добро» дали, что и позволит «сотовикам» выполнить требования законодательства.

Стоит отметить, что в России насчитывается порядка 250 млн. активных SIM-карт, многие из которых «серые» — их владельцы либо не идентифицированы, либо не верифицированы в сотовых сетях.



ВСТРЕЧА В НОВО-ОГАРЕВО

На встрече в Ново-Огарево Председатель Центрального банка Эльвира Набиуллина информировала Президента России Владимира Путина о ситуации в банковской сфере, текущей работе Центробанка.

Э. Набиуллина: Мы видим новые тенденции на банковском рынке. Многие финансовые услуги стали представляться дистанционно. Растёт интернет-торговля. По показателю развития финансовых технологий Россия не отстает от других стран, а по некоторым показателям даже превосходит.

Развитие технологий ставит перед Центральным банком задачи: развитие инфраструктуры; защита прав граждан при использовании финансовых технологий; защита от кибератак.

В финансовых технологиях мы также должны выстроить национальную инфраструктуру, которая позволит нам развиваться на собственной базе. Это, прежде всего, касается удаленной системы идентификации, сейчас идут поправки в законодательство. Это очень важно, потому что люди хотят уже получать услуги вне зависимости от того, где они находятся, в любое время суток. Должна быть удаленная система идентификации, в том числе на основе биометрических данных. Некоторые банки начинают развивать эту систему. Но, на наш взгляд, она должна быть единая государственная, с уровнем защиты этих персональных данных, с возможностью обмена информацией, чтобы все могли развивать эти технологии, не только большие банки, но и мелкие участники.

СТРАНЫ ЕС ПОМОГУТ СО ВЗЛОМОМ

В рамках антитеррористического пакета Европейская комиссия предложила странам-участницам Евросоюза помогать друг другу в вопросах взлома зашифрованных устройств.

В настоящее время неуклонно растет число сервисов, использующих шифрование. Спецслужбы многих стран, в том числе РФ, требуют от них предоставлять ключи шифрования для проведения оперативно-розыскных мероприятий. С технической стороны это не всегда возможно (как в случае с Telegram), а практика внедрения бэкдоров подвергается критике со стороны общественности. Еврокомиссия предложила альтернативу — правоохранительные органы стран ЕС будут помогать друг другу в проведении экспертизы.

Как к данной инициативе относятся сами правоохранители, и захотят ли они делиться своим опытом и технологиями, пока неизвестно.

АУТЕНТИФИКАЦИЯ ОТ «ДИАСОФТ»

Новые возможности продукта Diasoft FA# Beans позволяют использовать многофакторную усиленную идентификацию при авторизации в системе банка. Это исключает риск действий от имени другого пользователя, даже если он знает данные для входа.

Создан алгоритм аутентификации временными паролями (TOTP), которые действуют одну минуту и обеспечивают защиту от перехвата данных извне. Для установки достаточно приобрести лицензию и перенастроить способ авторизации, что можно сделать без участия разработчика.

Игорь Легезин, директор «Диасофт»: «Помимо аутентификации TOTP-алгоритмом, мы настраиваем и другие устройства: от токенов с неизвлекаемыми ключами до EMV банковских карт. Наши высококлассные программисты могут реализовать практически любой вариант, требующийся банку».



GOOGLE ПРИЗВАЛ ХАКЕРОВ

Google объявила о старте программы вознаграждения за поиск уязвимостей в самых популярных приложениях сторонних разработчиков. Искать пробелы в программах будут хакеры, работающие через платформу HackerOne. За найденные уязвимости они будут получать от \$1 тыс.

Хакеры не могут взять любое приложение из онлайн-магазина для проверки. Google составила список из самых популярных программ в Google Play: пока это Dropbox, Duolingo, Line, Snapchat, Tinder, Alibaba, Headspace и Mail.ru. При этом на изучение хакерам отданы только «критичные и основополагающие сервисы» российской компании. Среди них: «Почта», «Ка-

лендарь», «Код доступа» и «Облако Mail.ru». Отметим, что мобильные приложения социальных сетей «Одноклассники» и «ВКонтакте», а также мессенджера ICQ не входят в программу сотрудничества Google и HackerOne.

Хакеры должны будут искать в указанном ПО сторонних разработчиков уязвимости и сообщать о них не Google, а самим компаниям — создателям приложений. После чего хакеры и представители службы ИБ разработчиков вместе будут искать способы устранения проблемы. Как только решение будет найдено и подтверждено, хакер сможет обратиться в Google за вознаграждением. Чем серьезнее уязвимость, тем выше сумма.

ВТБ ПОЛУЧИЛ СЕРТИФИКАТ СООТВЕТСТВИЯ PCI DSS V3.2

В августе Банк ВТБ (ПАО) получил сертификат соответствия требованиям стандарта безопасности данных индустрии платежных карт PCI DSS v3.2 по итогам аудита, проведенного специалистами компании АО «ДиалогНаука».

Действие указанного стандарта распространяется на организации, в информационной инфраструктуре которых хранятся, обрабатываются или передаются данные платежных карт. Данный аудит проводился в объединенной инфраструктуре, созданной после присоединения Банка Москвы в 2016 году и на фоне готовящегося объединения с Банком ВТБ24 в январе 2018 года.

Заместитель председателя правления Банка ВТБ Ольга Дергунова отметила: «Для банка ВТБ обеспечение информационной безопасности является одним из приоритетов, поэтому для нас важно успешное прохождение

сертификации PCI DSS v3.2. Это дало нам возможность проанализировать, насколько полно учтены все моменты, связанные с обеспечением безопасности».





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.

ЦЕНТР КИБЕР-БЕЗОПАСНОСТИ ОТКРОЮТ В ПРИМОРЬЕ

Научно-образовательный центр кибербезопасности «Лаборатории Касперского» будет открыт в Дальневосточном федеральном университете на острове Русский.

«Открытие центра — важный шаг в реализации соглашения о сотрудничестве между ДВФУ и «Лабораторией Касперского». Центр будет предоставлять образовательные и консультационные услуги, помогать студентам осваивать новые информационные технологии и программные продукты», — говорится в сообщении пресс-службы ДВФУ.

Руководитель образовательных программ «Лаборатории Касперского» Дмитрий Постельник отметил, что компания планирует совместные научные исследования с университетом. Тем более, что со спецификой местных киберугроз в ДВФУ хорошо знакомы.

СКОЛКОВО. ДЕБАТЫ О БЕЗОПАСНОСТИ

На кампусе Московской школы управления СКОЛКОВО состоялся II Ежегодный Форум «Safety Leaders», посвященный вопросам безопасности человека и общества. Дебаты состояли из 4 секций: «Кибербезопасность», «Финансовая грамотность», «Безопасность на дорогах» и «Охрана труда».

Как в эпоху повсеместного распространения информационных технологий защитить ребенка от психологической травмы? Генеральный директор медиапроекта [Б]езопасность Елена Ульянова заявила следующее: «Сегодня изменить ментальность наших детей уже нереально. Мир остановить невозможно, а вот научить безопасно жить в этом мире — задача посильная, и каждый из нас должен ее перед собой поставить».

Директор по развитию бизнеса АО «Группа Т-1» Игорь Хереш отметил: «Отличительная особенность дан-

ного мероприятия в том, что здесь собраны эксперты с совершенно разными точками зрения. Это чрезвычайно важно, как для формирования целостной картины происходящего, так и для того, чтобы тщательно разобрать тему и найти способы реально решить проблемы».



QIWI — безопасность без компромиссов

Более 18 миллионов пользователей доверяют QIWI свои деньги



Вершина успеха!

ФИНАНСОВЫЙ ОЛИМП

Национальная премия ФИНАНСОВЫЙ ОЛИМП 2017

01.10 – 15.11.2017 Прием заявок на участие

15.11 – 01.12.2017 Экспертный совет

06.12.2017 Конференция-брифинг

Фуршет в честь лауреатов

Оргкомитет премии: best@best.ru / 8 495 989 58 59

При поддержке

ОБЩЕРОССИЙСКАЯ
ДЕЛОВАЯ
РОССИЯ

Официальное
рейтинговое
агентство

RAEX ЭКСПЕРТ РЯ
РЕЙТИНГОВОЕ АГЕНТСТВО

Официальный
аудитор

pwc

Официальный
медиа
партнер

 **BANKIR.RU**

Официальный
печатный
партнер

БО

Информационные партнеры

ДНИ.РУ ИНТЕРНЕТ
ГАЗЕТА

Утро.ru
www.uto.ru

AK&M
ИНФОРМАЦИОННОЕ АГЕНТСТВО

ФИНАНСОВАЯ
ГАЗЕТА

ПРО БИЗНЕС

Босс

РАДИО **ХО** **С** **М**

журнал
стратегия

BIS
JOURNAL

FutureBanking™

[NR]
NEW RETAIL

the
Retail
Finance

SOTNIBANKOV.RU
Банковский информационно-аналитический портал

НА СМЕНУ СЕНСАЦИЯМ ПРИШЛА ПЛАНОВАЯ РАБОТА

ФИНЦЕРТ БАНКА РОССИИ ПРЕДСТАВИЛ ГОДОВОЙ
ОТЧЁТ О РАБОТЕ ЗА ПЕРИОД С 1 ИЮНЯ 2016 ГОДА
ПО 1 СЕНТЯБРЯ 2017 ГОДА

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) является структурным подразделением Главного управления безопасности и защиты информации Банка России. Полный текст очередного отчёта (период с 1 июня 2016 года по 1 сентября 2017 года) опубликован на официальном сайте Банка России (<http://www.cbr.ru/StaticHtml/File/14435/GUBZI-4.pdf>).

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОГО ОБМЕНА

Для эффективного обнаружения и предупреждения информационных атак ФинЦЕРТ организует информационное взаимодействие Банка России с:

- ♦ поднадзорными организациями;
- ♦ компаниями-интеграторами;
- ♦ разработчиками ПО, включая средства антивирусной защиты;
- ♦ интернет-провайдерами и операторами связи;
- ♦ правоохранительными и иными государственными органами, курирующими информационную безопасность отрасли (МВД России, ФСБ России, ГосСОПКА).

Взаимодействие представляет собой обмен информацией о компьютерных атаках в кредитно-финансовой сфере, актуальных угрозах информационной безопасности и уязвимостях программного обеспечения. На его основе разрабатываются аналитические материалы и рекомендации по обеспечению защиты информации при осуществлении переводов денежных средств.

Для выполнения поставленных целей производятся:

- ♦ мониторинг открытых ресурсов сети Интернет;
- ♦ криминалистические компьютерные исследования (форензика);
- ♦ дистанционный контроль защиты информации при осуществлении переводов денежных средств;
- ♦ участие в инспекционной деятельности Банка России.

На конец сентября 2017 года количество участников информационного обмена ФинЦЕРТ с организациями кредитно-финансовой сферы достигло 526. Среди участников — 418 кредитных ор-

ганизаций и филиалов, это около 95% всех банков. Среди них 14 кредитных организаций из стран, входящих в ОДКБ, 26 небанковских кредитных организаций, 7 разработчиков банковского программного обеспечения, 4 оператора связи, 10 органов государственной власти и иные организации.

За отчётный период доля активных участников информационного обмена, которые регулярно передают данные о выявленных угрозах и уязвимостях, увеличилась почти в два раза. Активно делятся информацией с ФинЦЕРТ 45% всех участников, больше всего — банки среднего размера. Их способность выявлять, классифицировать и отражать атаки позволяет выстраивать объективную картину информационных атак в финансовой сфере, поддерживать удовлетворительный уровень безопасности.

Порядок работы ФинЦЕРТ с поступающей информацией предполагает анализ, классификацию и перепроверку. Эти процедуры в среднем занимают от 40 до 90 минут, что является хорошим показателем, позволяющим оперативно отражать массовые таргетированные атаки. В рассылках ФинЦЕРТ содержатся только подтвержденные сведения.

АНАЛИЗ И КЛАССИФИКАЦИЯ АТАК

Получая от участника обмена сообщение об атаке, ФинЦЕРТ проводит его анализ, после чего, если атака является массовой и затрагивает нескольких участников, формируется и рассылается информационный бюллетень — в среднем около 14 бюллетеней за месяц. ФинЦЕРТ публикует в рассылках информацию не об инцидентах, а о выявленных ата-

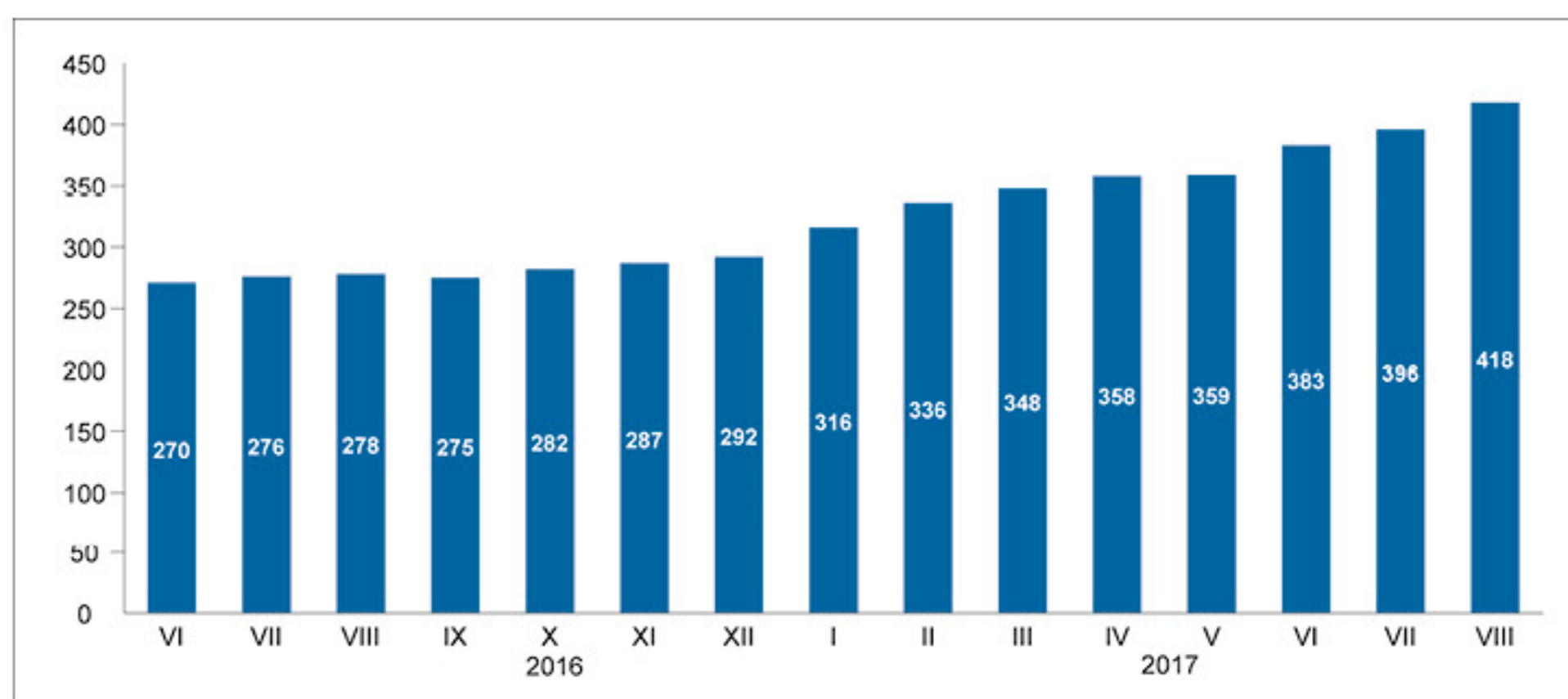


Рисунок 1. Количество кредитных организаций, присоединившихся к информационному обмену с ФинЦЕРТ

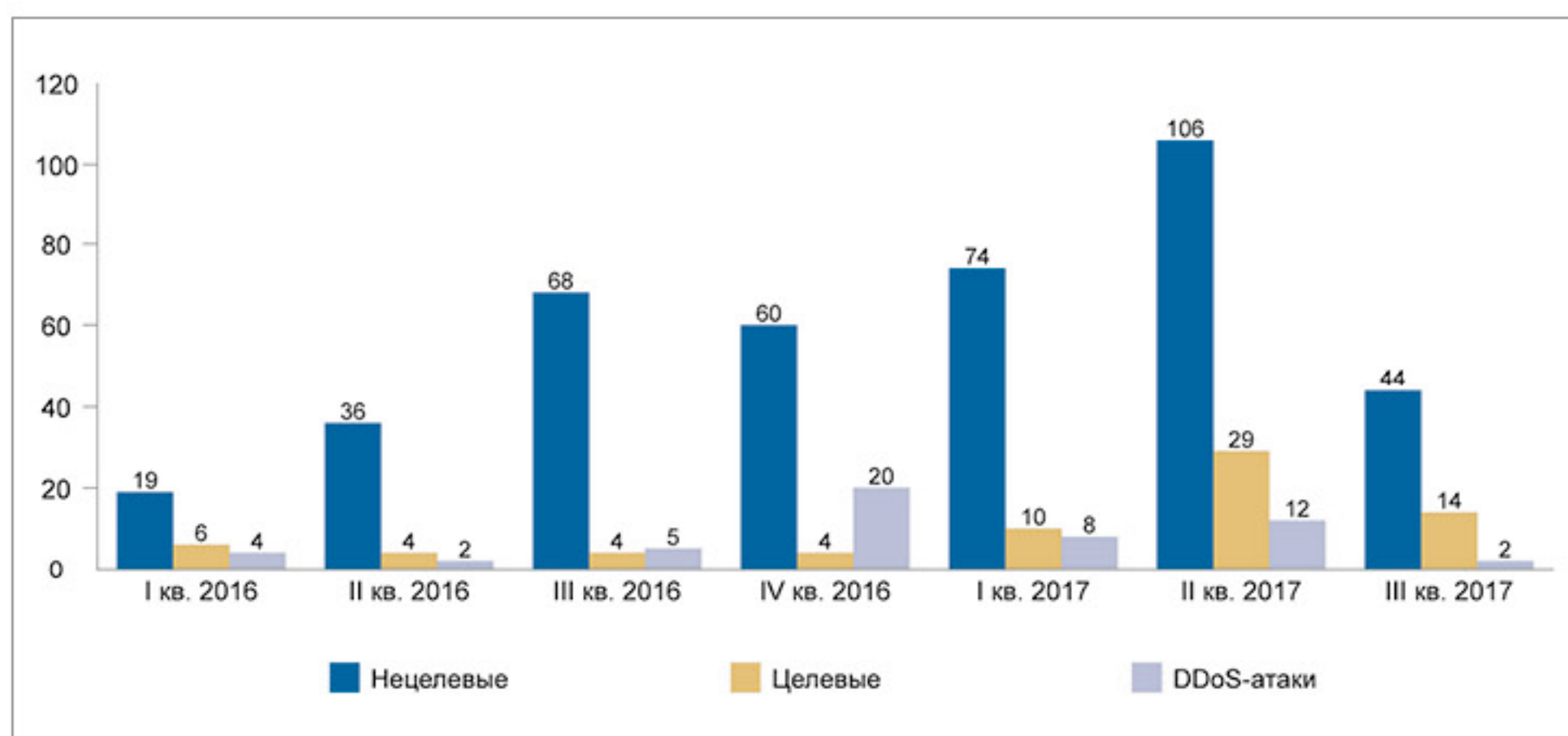


Рисунок 2. Динамика основных типов атак (по кварталам)

ках: их адресатах (без указания конкретных организаций), целях, инструментарии и «почерке» злоумышленников.

Условно компьютерные атаки в финансовой сфере можно разделить на три группы. Первая — **нецелевые атаки**, которые обычно носят относительно массовый характер. Обычно в ходе таких атак по обширным спискам получателей из различных финансовых организаций рассылаются электронные письма с вредоносными вложениями. Либо, если целями атак являются не сами финансовые организации, а их клиенты, вредоносные программы распространяются через сайты в сети Интернет. Вторая группа — **целевые атаки**, ориентированные на конкретные цели — определенные организации кредитно-финансовой сферы. Целевых атак может фиксироваться по две-три в неделю. О целевой атаке становится известно, только если она своевременно выявлена и пресечена. Третий тип — **DDoS-атаки** — атаки, направленные на отказ в обслуживании.

Увеличение количества участников информационного обмена позволило выявлять намного больше атак, удалось выстроить реалистичную картину угроз. Стало ясно, что российская финансовая система имеет адекватную имеющимся угрозам систему защиты.

БЛОКИРОВКА ФАЛЬШИВЫХ САЙТОВ

На основании мониторинга выявляются интернет-сайты, используемые для противоправных действий в финансовой сфере. Данные интернет-сайты могут использоваться для:

- ♦ рассылки вредоносных программ и управления бот-сетями;
- ♦ мошеннических действий, связанных с платежными картами, (включая сбор данных номеров карт, их держателей, сроков действия и т.д.);
- ♦ размещения фишинговой информации, предназначенной для клиентов кредитно-финансовых организаций;
- ♦ имитации ресурсов Банка России.

Имитируются сайты различных организаций финансовой сферы: банков, микрофинансовых организаций, операторов по переводу денежных средств, платёжных систем, обменников, торговых площадок, государственных органов, баз данных и процессинговых центров.

После подтверждения проверкой осуществления мошеннической деятельности ФинЦЕРТ уведомляет регистратора соответствующего домена (ресурса) о целесообразности снять домен с делегирования или инициировать проверку документов его администратора. Среднее время блокировки составляет от од-

ного до трёх дней. Если фальшивые интернет-ресурсы находятся за пределами компетенции ФинЦЕРТ, сведения о них направляются иным компетентным организациям.

За восемь месяцев 2017 года ФинЦЕРТ отправил информацию о 481 домене различной мошеннической тематики, подлежащем делегированию. 367 доменов по итогам рассмотрения заблокированы регистраторами. В среднем за месяц делегированию подлежат около 50 доменов, находящихся в различных зонах.

Кроме того, ФинЦЕРТ в течение рабочего дня с интервалом примерно в два часа осуществляет мониторинг СМИ, блогов, социальных сетей и других подобных ресурсов сети Интернет на наличие недостоверных публикаций, порочащих репутацию Банка России и банковских организаций.

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА (ФОРЕНЗИКА)

ФинЦЕРТ активно сотрудничает с правоохранительными органами. Его сотрудники привлекаются в качестве специалистов при проверках сообщений о преступлениях и расследованиях уголовных дел, связанных с хищениями у финансовых организаций и их клиентов. Задействуются технические и финансовые компетенции специалистов ФинЦЕРТ в вопросах работы систем дистанционного банковского обслу-

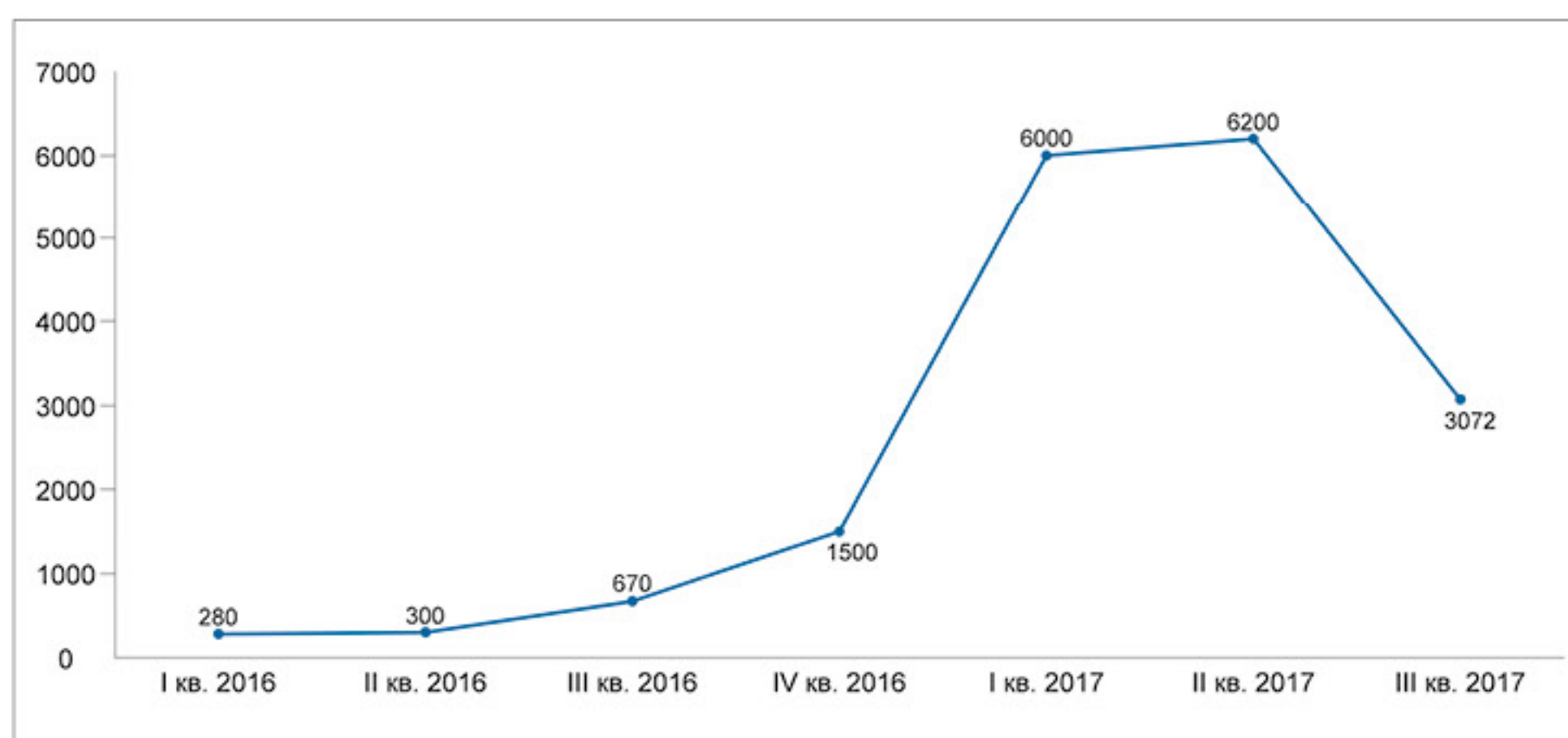


Рисунок 3. Статистика по мощности DDoS-атак (Мбит/с)



Рисунок 4. Шиммер, устанавливаемый в POS-терминал

живания, технологий проведения операций и технического анализа вредоносных программ.

С декабря 2016 года в структуре ФинЦЕРТ действует специализированное подразделение — отдел технического анализа. Фактически — это **криминалистическая лаборатория**. По запросам правоохранительных органов лабораторией были проведены:

- ♦ шесть исследований электронных носителей информации, подвергшихся воздействию вредоносных программ при совершении хищений денежных средств со счетов клиентов кредитных организаций;
- ♦ три исследования аппаратных средств, предназначенных для скрытого хищения платежной информации;
- ♦ несколько исследований мобильных устройств и поддельных платежных карт.

Также лаборатория осуществляет углубленный технический анализ компьютерных атак и используемого вредоносного программного обеспечения. Производится анализ поступающих образцов вредоносных программ и используемых для их распространения сетевых ресурсов, выявление индикаторов компрометации (ИОС) и выработка мер противодействия.

За отчетный период были зафиксированы следующие основные типы атак:

- ♦ DDoS-атаки, в том числе угрозы DDoS-атак (мощность атак возросла до 6200 Мбит/с — в 10 раз по сравнению с началом 2016 года);
- ♦ массовые рассылки почтовых сообщений, содержащих загрузчики вредоносного программного обеспечения (в том числе с элементами применения социальной инженерии);
- ♦ атаки, направленные на устройства самообслуживания (банкоматы, терминалы).

В отчете содержится подробное описание используемых технологий и программно-аппаратного инструментария новых актуальных типов атак. Эта информация полезна специалистам по обеспечению информационной безопасности организаций финансовой сферы.



Рисунок 5. Пример устройства Black Box, подключаемого к разъему SDC

Отдельная задача, которую решает ФинЦЕРТ — **повышение грамотности в сфере информационной безопасности финансовых инструментов**. Отдельные обучающие мероприятия проводятся для сотрудников правоохранительных органов.

ДИСТАНЦИОННЫЙ КОНТРОЛЬ

На сегодняшний день основными инструментами дистанционного контроля, осуществляемого ФинЦЕРТ, является анализ:

- ♦ сведений форм отчетности 0403203 и 0409258;
- ♦ обращений граждан;
- ♦ результатов оценки соответствия, проводимой субъектами национальной платежной системы в рамках выполнения требований Положения Банка России № 382-П;
- ♦ правил платёжных систем на соответствие требованиям, касающимся обеспечения защиты информации при осуществлении переводов денежных средств в платежной системе.

С начала 2017 года ФинЦЕРТ участвует в инспекционной деятельности Банка России. За отчетный период специалисты подразделения приняли участие в проверках семи банков, четырех страховых организаций и одной расчётной небанковской кредитной организации.

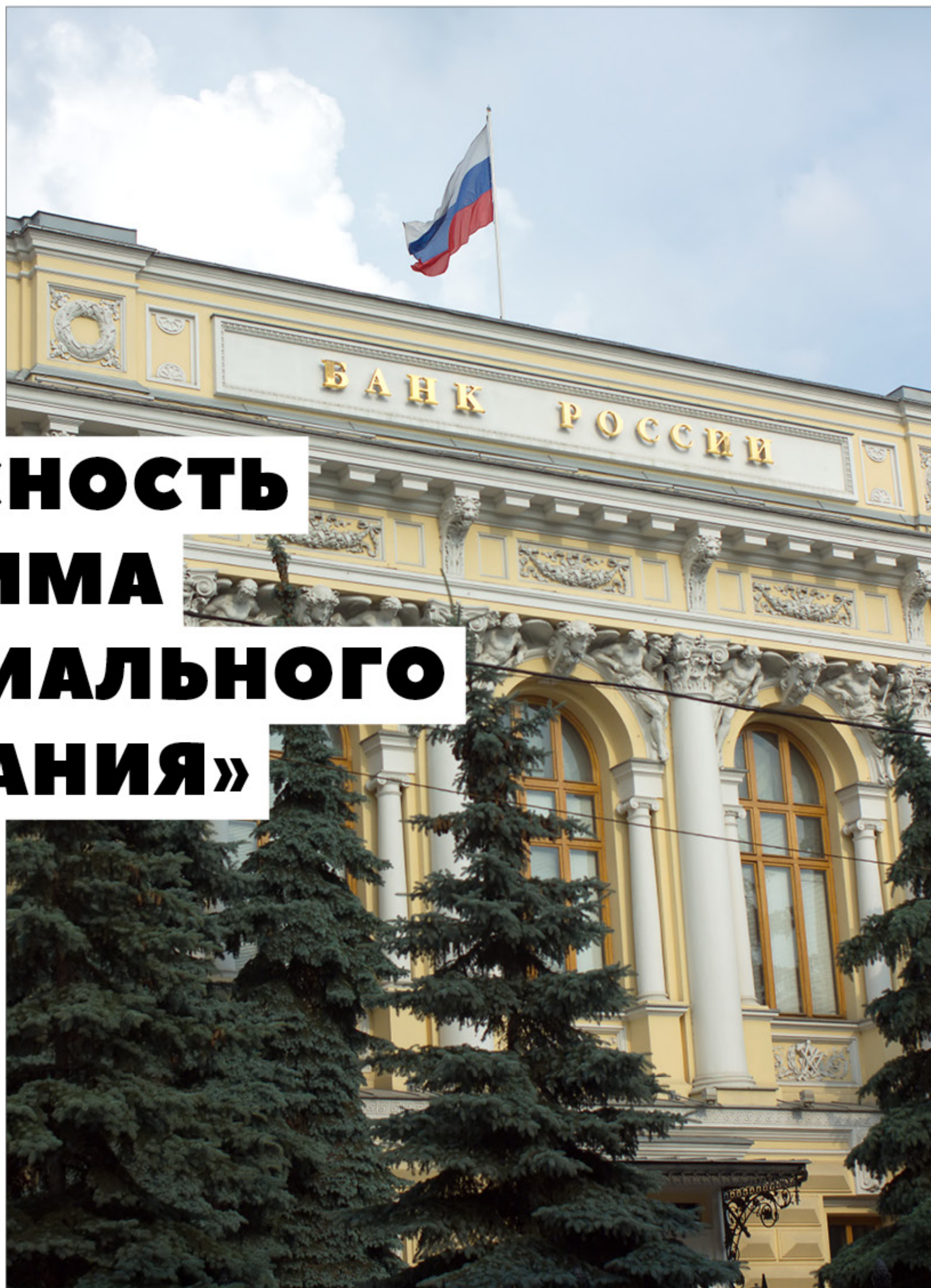
* * *

В настоящее время кадровый состав ФинЦЕРТ укомплектован для выполнения поставленных задач. В штате 28 квалифицированных работников, средний возраст которых составляет 34 года. Они обладают богатым практическим опытом анализа защищенности и уязвимостей информационных систем, а также векторов атак.

Среди сотрудников ФинЦЕРТ — выпускники МГТУ им. Н.Э. Баумана, НИЯУ МИФИ и МГУ им.М.В. Ломоносова, обладатели учёных степеней. Есть и те, кто имеют большой опыт работы в правоохранительных органах, а также в региональных банках. Регулярно проводится повышение квалификации.



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



«БЕЗОПАСНОСТЬ НЕМЫСЛИМА БЕЗ СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ»

Новым современным форматом общения представителей Банка России с внешней аудиторией становятся онлайн-трансляции выступлений руководителей и ведущих специалистов профильных подразделений в социальных сетях.

20 сентября заместитель начальника Главного управления безопасности и защиты информации Банка России Артём Сычев в режиме онлайн отвечал на вопросы пользователей «Фейсбука». Предлагаем вниманию наших читателей журнальный вариант выступления и ответов на самые важные вопросы.

ИНФОРМИРОВАННОСТЬ— УСЛОВИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Вопросы информационной безопасности приоритетны для Банка России — главного регулятора финансовой отрасли. От решения этих вопросов во многом зависит стабильное функционирование финансовой системы страны, защите прав клиентов коммерческих банков.

ПОЗИЦИЯ БАНКА РОССИИ
ПО ВОПРОСАМ ИБ БЫЛА
ПРЕДСТАВЛЕНА ПОЛЬЗОВАТЕЛЯМ
СОЦИАЛЬНОЙ СЕТИ
В ХОДЕ «ПРЯМОЙ ЛИНИИ»
С ПРЕДСТАВИТЕЛЕМ РЕГУЛЯТОРА

Как именно Банк России обеспечивает информационную безопасность в финансовой сфере? Как государственный регулятор он устанавливает нормативные требования к информационной безопасности своим поднадзорным организациям. Нормативное регулирование осуществляется по двум основным направлениям. Первое — формирование стандартов и рекомендаций. Второе — выпуск нормативных документов с требованиями, обязательными для исполнения.

Например, таких, как Положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». В этом документе подробно написано, что должна делать кредитная организация, чтобы обеспечить на должном уровне информационную безопасность своих платежей и платежей своих клиентов.

Кроме того, Банк России уделяет много внимания повышению грамотности в вопросах информационной безопасности. Организуются обучающие программы для разных аудиторий: клиентов банков, сотрудников СМИ и правоохранительных органов, а также для учащихся. Программы информируют о новых высокотехнологичных финансовых сервисах, о возможных способах мошенничества и о том, как обезопаситься от них. Благодаря проводимой работе современный уровень информационной безопасности финансовых технологий можно оценивать как адекватный существующим рискам.

Успешно противостоять злоумышленникам, которые охотятся за деньгами банков и клиентов, можно только совместными усилиями Банка России, самих кредитно-финансовых организаций и правоохранительных органов. Именно для этого в Банке России действует Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере — специальное подразделение Главного управления безопасности и защиты информации, известное как ФинЦЕРТ (FinCERT). Одной из главных задач которого является организация информационного обмена между участниками финансового рынка, правоохранительными органами,



органами государственной власти и другими заинтересованными сторонами. Информационный обмен позволяет оперативно выявить новую проблему, классифицировать её и выработать меры решения.

ОТВЕТЫ НА ВОПРОСЫ

Итак, первый вопрос: **Насколько безопасен мобильный банкинг?**

Я сам им пользуюсь и всегда отвечаю, что риски, конечно же, есть. И Банк России, и сами банки, думающие о сохранении своей клиентской базы, прикладывают немалые усилия, чтобы свести эти риски к минимуму. Риски эти можно подразделить на относящиеся к самому мобильному банкингу и к его пользователям.

Пользователи иногда забывают об элементарных правилах «сетевой гигиены», или «кибергигиены», чрезмерно доверяя сервисам. Например, одно и то же устройство используется и для финансовых сервисов, и для просмотра самых разных сайтов. В таком случае, чтобы защититься от зловредных программ, обязательно устанавливать антивирусное программное обеспечение на компьютеры, планшеты и смартфоны. Это позволит существенно снизить риск получения злоумышленниками доступа к логину и паролю, которые позволяют распоряжаться денежными средствами на счёте.

Со своей стороны, большинство банков выполняют требования Банка России к обеспечению безопасности на всех этапах жизненного цикла банковского программного обеспечения. В том числе и приложений мобильного банкинга. Среди этих требований выявление и устранение уязвимостей,

внедрение систем антифрода — автоматизированного обнаружения подозрительных транзакций. Также операторам переводов денежных средств предписывается предлагать клиентам ограничения — лимиты на операции, снижающие риски мошенничества.

Следующий вопрос: действительно ли программное обеспечение компании Apple надёжнее, чем Microsoft?

БЛАГОДАРЯ ПРОВОДИМОЙ РАБОТЕ СОВРЕМЕННЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВЫХ ТЕХНОЛОГИЙ МОЖНО ОЦЕНИВАТЬ КАК АДЕКВАТНЫЙ СУЩЕСТВУЮЩИМ РИСКАМ

Считаю такой вопрос не вполне корректным. Программисты тоже люди, допускают ошибки, а защиту, созданную человеком, может преодолеть другой человек. Особенно в случае таких сложных, объёмных проектов, как операционные системы. Оценивать, какая операционная система лучше, не совсем правильно. Более верно говорить, какая более распространена, и насколько злоумышленники заинтересованы искать в ней уязвимости.

Задают вопрос и о том, насколько целесообразно покупать у банков дополнительно **страховку от хищений денежных средств с карт**. У нас это пока новшество. Практика страхования рисков широко распространена на Западе.

ЗАКОНОДАТЕЛЬСТВО ИДЁТ В НОГУ СО ВРЕМЕНЕМ

Следующий вопрос о юридической квалификации хищений денег с банковских карт: кража это или мошенничество? Когда на улице отбирают деньги — это называется воровство или грабёж, которые наказываются годами лишения свободы, а когда крадут с банковского счёта — всего лишь мошенничество. Почему? Это серьёзный и правильный вопрос, над которым работает банковское сообщество и Банк России.

Дело в том, что при высокотехнологичных финансовых преступлениях не происходит контакта злоумышленника и жертвы, происходит подмена электронного документа, его реквизитов. Пока что преступники, совершающие такие преступления, получают сроки, несоразмерные опасности их деяний. Это не удовлетворяет ни Банк России, ни банки, ни их клиентов, ни правоохранительные органы. Поэтому сейчас в Государственной Думе РФ находится на рассмотрении законопроект об ужесточении наказания за подобные преступления. Банк России поддержал инициативу правоохранительных органов и банковского сообщества по разработке и продвижению этого законопроекта.

Также специалисты Банка России участвуют в разработке и продвижении законопроекта **об обмене информацией между банками и операторами мобильной связи**. Такая работа ведётся совместно с Минкомсвязи России. Цель — обезопасить клиентов банков от мошенничеств, совершаемых посредством подмены SIM-карт. В зоне риска этого вида мошенничества находятся клиенты, у которых на счетах значительные средства. Но, учитывая быстроту технического прогресса, нужно быть готовыми к тому, что защищать от подмены SIM-карт придётся и других клиентов. В принятии этого законопроекта заинтересованы и банки, и операторы мобильной связи.

Вопрос профессионала: **организует ли Банк России онлайн-взаимодействие между подразделениями банков, занимающимися антифродом, и управлением «К» МВД России, для оперативного реагирования на инциденты?** Такое взаимодействие, хотя и не в режиме онлайн, уже эффективно организовано ФинЦЕРТ (FinCERT). Возросло количество предотвращённых попыток хищений денежных средств, результатами стали возбуждённые уголовные дела и задержания злоумышленников. Теперь нужно автоматизировать это взаимодействие, перевести его в онлайн-режим,



Банк России

Центральный банк Российской Федерации

ОТ «ЛИКБЕЗА» К ВСЕОБУЧУ

**О ПОЛИТИКЕ БАНКА
РОССИИ, НАПРАВЛЕННОЙ НА
ПОВЫШЕНИЕ ГРАМОТНОСТИ
В СФЕРЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ФИНАНСОВЫХ СЕРВИСОВ**

Недостаток финансовых знаний у российских граждан отчетливо виден при анализе поступающих в Банк России жалоб на финансовые организации. Людям не всегда легко разобраться в нюансах, тонкостях и рисках, присущих тому или иному финансовому продукту, тем более что ассортимент этих продуктов увеличивается, а сами они становятся более сложными. Именно поэтому задача по повышению уровня финансовой грамотности значится как одна из приоритетных в разработанных Банком России **Основных направлениях развития финансового рынка на 2016–2018 годы**.

В последнее время развитие финансовых сервисов активно движется в сторону оказания дистанционных услуг. Мошенники также активно переходят в онлайн сферу. Например, после появления возможности заключить договор ОСАГО в электронном виде в интернете стали появляться сайты — клоны крупных страховых компаний. Эти сайты частично или полностью повторяли дизайн сайта страховой компании, а адрес сайта-клона незначительно отличался от адреса страховой компании в сети. Важно, чтобы люди знали о существовании таких мошеннических сайтов и могли их отличать от настоящих. Банк Рос-

сии считает, что в значительной степени: предупрежден — значит вооружен!

По мере увеличения доступа к интернету в регионах (надо отметить, что уровень его проникновения в России не отстает от среднеевропейского) растут и возможности использования цифровых (дистанционных) финансовых сервисов. Простота использования и доступность цифровых финансовых услуг имеет неоспоримые преимущества, но и несет определенные риски. Граждане должны быть проинформированы об этих рисках и опасностях, и значительную роль в этом процессе играет Банк России.

Банк России проводит собственные мероприятия по повышению финансовой грамотности, в том числе в области информационной безопасности финансовых сервисов, а также активно участвует в мероприятиях, проводимых другими министерствами, ведомствами и общественными организациями. Такая работа проводится как в крупных городах, так и в регионах.

При участии Банка России выпущено учебное пособие для школьников «Основы финансовой грамотности», по которому ведется преподавание этого предмета в пилотных школах. Отдельная глава учебника посвящена информационной безопасности в финансовой сфере. В ходе выездных мероприятий, где представители Банка России совместно с представителями финансовых и общественных организаций проводят лекции и семинары по финансовой грамотности для региональных образовательных учреждений, пожилых граждан, а также на предприятиях, обязательно затрагиваются вопросы информационной безопасности, учитывая высокий интерес к этой теме аудитории любого возраста. Кроме того, в конце прошлого 2016 года Банк России запустил информационную кампанию в региональных СМИ, цель которой — подробно рассказать гражданам об основных видах мошенничества на финансовом рынке.

Каждая добросовестная финансовая организация заинтересована в том, чтобы ее клиенты были финансово грамотными и могли оценить весь спектр предлагаемых ею услуг. Это актуально и в контексте информационной безопасности. В частности, если клиент осведомлен об опасности сообщения посторонним лицам PIN-кода своей карты или CVV-кода, если он предупрежден о необходимости внимательно относиться к СМС-сообщениям о блокировке карты или снятии с нее денег, это поможет самой финансовой организации избежать возможных репутационных и финансовых потерь.

планируемый срок начала подключения участников информационного обмена — середина 2018 года.

Есть важная подзадача: оперативное определение счетов, на которые злоумышленники пытаются перевести похищенные денежные средства. Чаще всего эти счета оформлены на подставные юридические и физические лица. Список таких счетов крайне интересен банкам — и отправителям, и получателям платежей, совершаемых злоумышленниками. Банк России совместно с коллегами и кредитными организациями подготовил законопроект, который узаконит обмен этой информацией. Он находится в Государственной Думе РФ и готовится к первому чтению. После его принятия можно будет наладить онлайн-обмен такой информацией в кратчайшие сроки, что намного улучшит профилактику подобных правонарушений.

Вопрос, который часто задают, **обязан ли банк вернуть деньги, украденные с банковской карты**. Статья 9 действующего Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» подробно описывает порядок этой процедуры. Банк обязан в таком случае либо вернуть средства, либо представить мотивированное обоснование отказа. В любом случае банк обязан провести расследование инцидента. К счастью, не так много случаев обращений, когда у банков и правоохранительных органов есть основания предполагать попытки мошенничества.

КАК ОБЕЗОПАСИТЬ РОДСТВЕННИКОВ

Спрашивают и о том, **нужно ли из соображений безопасности заклеивать непрозрачным скотчем веб-камеру на ноутбуке**. Один из рисков, не только на ноутбуках, но и на других устройствах, — захват злоумышленником управления веб-камерой. Заклеивать или нет, дело каждого. Я этого не делаю, поскольку уверен в надёжности средств защиты, которые использую, той самой «кибергигиены».

Важен **вопрос о социальной инженерии**; это один из самых важных вопросов информационной безопасности. Это вечный вопрос, известный даже по детскому фильму о приключениях Буратино: пока живут на свете дураки, обманом жить нам, стало быть, с руки... Мошенники пытаются на доверии заставить человека предоставить им доступ к распоряжению своими деньгами или прямо им их перечислить. Например, присылают мошенническое SMS-сообщение, что якобы Ваша банковская карта заблокирована, при этом указывают телефон, по которому нужно перезвонить, чтобы решить проблему. Правильно реагировать нужно так: перезвонить в Ваш банк по номеру телефона, указанному на банковской карте, после чего уточнить, заблокирована она или нет. Если сообщение оказалось ложным, то нужно сообщить о попытке мошенничества в свой банк.

Мошенники изобретательны и идут в ногу со временем. Сообщения, или письма по электронной почте они могут слать от Ваших контрагентов: банков, операторов телекоммуникаций, государственных органов и т.д. Цель — открыть файл или ссылку на вредоносную программу, после чего на ваше устройство загружается вредоносное программное обеспечение.

Интересный вопрос: какие самые изощрённые способы мошенничества Вы встречали на практике? По моему опыту, главная «отмычка» — обманным путём завоевать доверие, которое потом используется как плацдарм. Сейчас, например, это спам организованных преступных группировок, персонализированный «под интересы» человека. Вы специалист по информационной безопасности? Ознакомьтесь, пожалуйста, с прайс-листом на такие услуги...

На мой взгляд, важен вопрос, **какие советы можно дать родственникам — пожилым людям, чтобы уберечь их деньги от мошенников.** Эта категория граждан оказывается самой привлекательной для злоумышленников. Которые рассылают ложные SMS-сообщения о том, что банковская карта якобы заблокирована, или что родственник попал в беду и надо срочно перечислить деньги для него. Пожилым людям нужно объяснить, что при получении подобных сообщений они не должны верить на слово незнакомцам, а позвонить родным и близким людям, которым доверяют и посоветоваться с ними.

Вместе с тем вектор атак злоумышленников в последнее время сместился **на граждан возраста до сорока лет.** Потому что они активно пользуются информационными технологиями, не вникая в механизмы работы, и излишне им доверяют. Но удобствам дистанционных финансовых сервисов сопутствуют определённым рискам. Поэтому всем нужно знать правила кибергигиены и соблюдать их: устанавливать и регулярно обновлять антивирусные программы, не открывать подозрительных сообщений, проверять, какое программное обеспечение загружаем, на какие сайты заходим. Тогда можно говорить о безопасном использовании информационных финансовых технологий.

ОБУЧАТЬСЯ ДОЛЖНЫ ВСЕ

Задают вопрос **о превращении рекомендаций по информационной безопасности в обязательные требования.** Требования позволяют обеспечить базовый уровень, дальше — вопрос политики управления информационными рисками. Банк России совместно с коллегами из отрасли разработал государственный стандарт информационной безопасности для финансовой сферы. Таким образом, посредством ссылок на этот ГОСТ обязательная нормативная база расширяется.

Спрашивают, планирует ли Банк России делиться лучшими практиками повышения осведомлённости клиентов банков в вопросах информационной безопасности сервисов? Это уже достаточно активно делается. Ежегодно проводится главное отраслевое деловое мероприятие — Уральский форум, посвящённый информационной безопасности финансовой сферы, в следующем году — уже в десятый раз. Часть обсуждаемых вопросов обязательно посвящаются затронутой теме. Банк России формирует программу, подбирает самых интересных докладчиков.

БАНК РОССИИ ГОТОВИТ ПРОЕКТ КВАЛИФИКАЦИОННЫХ ТРЕБОВАНИЙ К СПЕЦИАЛИСТАМ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФИНАНСОВОЙ СФЕРЕ

Ещё одна такая площадка для обмена опытом — форум инновационных финансовых технологий FINOPOLIS, проводимый в начале октября в Сочи. Там также рассматриваются вопросы повышения осведомлённости о правилах информационной безопасности.

В самую точку попадает вопрос, **каких навыков не хватает специалистам по информационной безопасности.** Банк России готовит проект квалификационных требований к специалистам по информационной безопасности в финансовой сфере. Готова программа магистратуры, дальнейший шаг — формирование образовательных стандартов для этого профиля.

Проблема в специфике финансовой отрасли, в переплетении информационных и финансовых технологий, а также обычной бухгалтерии. Специалист должен быть достаточно универсален: разбираться в технологиях и механизмах совершения операций, оценивать сопутствующие риски. Явно **не хватает специалистов, которые хорошо разбираются в юридических и технических аспектах информационной безопасности финансовой сферы.** Эти умения необходимы для правильного оформления юридически значимых доказательств, предоставляемых в правоохранительные органы и в суд, в случае инцидентов в сфере кибербезопасности.

Также ощущается дефицит **специалистов по управлению информационной безопасностью,** которые владели бы профессиональным языком, терминологией основных бизнес-процессов. К сожалению, таких специалистов пока крайне мало. Разрабатываемые образовательные документы направлены на то, чтобы таких специалистов готовили в нужном количестве.

* * *

На взгляд Банка России, для обеспечения кибербезопасности на высоком уровне необходимы следующие составляющие:

Первая — повышение осведомлённости о правилах кибергигиены и у сотрудников, и у клиентов банков, превращение их выполнения в повседневную практику.

Вторая — консолидация усилий Банка России, финансовых организаций и правоохранительных органов для противодействия киберпреступности, развитие информационного обмена.

Третья — развитие нормативной базы, которое Банк России стремится вести так, чтобы не создавать препятствий для внедрения новых финансовых технологий, но обеспечивая их безопасность.

ЦИФРОВОЙ ЭКОНОМИКЕ— ЭФФЕКТИВНОСТЬ И БЕЗОПАСНОСТЬ



Анатолий АКСАКОВ
председатель комитета
Государственной Думы
РФ по финансовому
рынку

ПЕРСПЕКТИВЫ ЗАКОНОДАТЕЛЬНОГО ОБЕСПЕЧЕНИЯ РАЗВИТИЯ НОВЫХ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И ИНСТРУМЕНТОВ

В конце сентября состоялось расширенное заседание Совета по законодательному обеспечению развития цифровой экономики при Председателе Государственной Думы РФ. Законодатели активно работают над законодательным регулированием цифровой индустрии. Какие назревшие изменения наиболее актуальны?

НОВЫЕ ФИНАНСОВЫЕ ТЕХНОЛОГИИ И СЕРВИСЫ

Ещё в ходе весенней сессии 2017 года был принят федеральный закон, создавший правовые основы взаимодействия Банка России с подведомственными финансовыми институтами через электронные личные кабинеты. Можно рассчитывать, что в течение 2018 года весь документооборот в отрасли по вопросам нормативным, контроля, надзора и рефинансирования кредитных организаций будет осуществляться в электронной форме. Будут сэкономлены время, усилия сотрудников, а также затраты на десятки и даже тысячи тонн бумаги, снижено потребление природного ресурса — древесины.

Находится в работе законопроект, формулирующий правовую базу использования биометрических данных для идентификации клиентов финансовых институтов, прежде всего кредитных организаций. В результате его

принятия физические лица смогут более широко дистанционно пользоваться финансовыми услугами — не выходя из квартиры, кабинета, автомобиля.

Идентификация клиентов с помощью биометрических данных будет осуществляться, с одной стороны, удобно и быстро. С другой стороны, — безопасно, поскольку храниться будут в единой защищённой базе, формируемой только на основе согласия их владельцев.

В развитие этой темы, на рассмотрении в Государственной Думе РФ находится следующий законопроект, о так называемой «ладошке», разработанный совместно со специалистами Сбербанка России. Этот документ создаст правовую возможность использовать в учебных заведениях технические устройства, идентифицирующие учащихся по биометрическим особенностям ладони. Как для доступа на территорию, так и для оплаты завтраков, обедов. Такие возможности откроются, когда будет принят и реализован предыдущий законопроект, создана единая защищённая база биометрических данных.

БЛОКЧЕЙН: НУЖНО ЛИ ПРАВОВОЕ РЕГУЛИРОВАНИЕ?

Стоит вопрос о законодательном регулировании применения технологии блокчейн, которая быстро развивается в настоящее время. Организации финансовой сферы активно стремятся

использовать её для повышения прозрачности и эффективности своей работы, например, Внешэкономбанк и Сбербанк России.

Эта технология позволяет более эффективно осуществлять различные банковские операции, такие как транзакции между клиентами банка. Росреестр — Федеральная служба государственной регистрации — также работает над созданием распределённой базы неизменяемых данных, которую позволяет сделать технология блокчейн.

Эксперты, к которым мы обращались, высказывали мнение, что использование технологии блокчейн не требует правового регулирования. Это пока новая технология, которая ещё не может конкурировать с традиционными, в частности, в скорости транзакций в платёжных системах. Поэтому лучше сконцентрироваться на привлечении к её развитию инвестиций, специалистов, других ресурсов. Для того, чтобы преимущества этой новой технологии можно было эффективно использовать.

ПЕРСПЕКТИВЫ ЛЕГАЛИЗАЦИИ КРИПТОВАЛЮТ

Большое внимание и общества и депутатов Государственной Думы РФ привлечено к криптовалютам, — новому, быстро развивающемуся рынку. Это, как правило, не обеспеченный финан-



совый инструмент, которому сопутствуют серьёзные риски, такие как создание финансовых пирамид. Поступают сигналы, что граждане России, получая из средств массовой информации сообщения о быстром росте курса криптовалют, продают дома, квартиры, чтобы в них вложиться.

Чтобы защитить интересы наших граждан, нужно легализовать, то есть законодательно определить такой финансовый инструмент как криптовалюта. У представителей государственного регулятора отрасли, Банка России, есть мнение, что легализация может способствовать нездоровому интересу к криптовалютам. Но и игнорировать это явление мы не можем, также как и связанные с ним факты мошенничества. Криптовалюты могут быть использованы и как средство отмывания нелегальных доходов и финансирования терроризма. Введение криптовалюты в законодательное поле позволит найти верные решения для защиты интересов общества и граждан от возможных злоупотреблений.

Главный вопрос — ICO (Initial Coin Offering), первичное размещение то-

БЛОКЧЕЙН — ЭТО ПОКА НОВАЯ ТЕХНОЛОГИЯ, КОТОРАЯ ЕЩЁ НЕ МОЖЕТ КОНКУРИРОВАТЬ С ТРАДИЦИОННЫМИ, В ЧАСТНОСТИ, В СКОРОСТИ ТРАНЗАКЦИЙ В ПЛАТЁЖНЫХ СИСТЕМАХ

кенов криптовалюты для привлечения средств в новые проекты и стартапы. Может быть использовано как для мошенничества и других противоправных действий, так и служить источником возможных инвестиций, в том числе зарубежных, в экономику России. Необходимо определить правила и площадки для ICO, требования к эмитентам и приобретателям этих новых финансовых инструментов. Для чего потребуются изменения действующего законодательства.

Комитетом Государственной Думы РФ по финансовому рынку создан экспертный совет, который организует дискуссию с привлечением лучших отечественных и зарубежных специалистов. Результатом работы в короткие сроки должны стать предложения о развитии

законодательства, чтобы позволить развиваться новым финансовым технологиям, использовать их для привлечения инвестиций в российские проекты.

* * *

Примеры таких начинаний уже есть — НП РТС работает над созданием площадки для торговли криптовалютами, электронной системы «Восход». Задача законодателей — создать такие правила игры, чтобы защитить интересы российских граждан, не допустить использования криптовалют в криминальных целях и способствовать притоку инвестиций в новые финансовые технологии и проекты, реализуемые с их помощью.



ОЛЬГА ДЕРГУНОВА:
«ЦИФРОВАЯ ЭКОНОМИКА —
СЕРВИС ЭВОЛЮЦИИ, РЫНКА...»

На Форуме инновационных финансовых технологий FINOPOLIS 2017 в Сочи заместитель председателя правления Банка ВТБ Ольга Дергунова выделялась как один из самых интересных, запоминающихся спикеров. Ее профессионализм, увлеченность, энергия, глубокие, яркие речи на пленарных дискуссиях произвели сильное впечатление на аудиторию. Она виртуозно балансировала на стыке двух подходов к регулированию банковского бизнеса: государственного и рыночного. На вопрос Эльвиры Набиуллиной о драйвере «цифровизации» экономики она ответила: «Сначала человек — потом идея. Главный локомотив всех изменений — люди, которые не останавливаются на достигнутом, и неважно, где зарождаются инновации — по инициативе государства, частной компании или юного гениального пионера. Они всегда зарождаются в головах отдельных людей».

На вопрос о том, что прежде всего должен сделать регулятор для развития цифровой экономики — она ответила: «Зафиксировать дату, когда 100% населения Российской Федерации будут иметь цифровой идентификатор, необходимый для получения финансовых услуг в электронном виде. Индия обеспечила такими идентификаторами свое население — 1,2 млрд человек — за десять лет. Наши 147 млн потребуют гораздо меньше времени». Интересной была реакция председателя Центробанка: «Я поддержу Ольгу. Создание идентификатора — давно назревшая проблема. Не очень понятно, почему она не решается: там, по-моему, один закон и два подзаконных акта. И все. Это просто необходимая индустрия».

Представляя стенд ВТБ на выставке FINOPOLIS — впечатляющую стильную конструкцию из синих плоскостей, соединенных под разными углами, Ольга Дергунова с гордостью заявила: «Ни одного бумажного документа, буклета или проспекта! Если мы говорим о 21 веке и цифровизации — значит, только цифра!». Пред-



Эльвира Набиуллина, Ольга Дергунова и Олег Тиньков на пленарном заседании FINOPOLIS 2017



Стенд ВТБ на выставке FINOPOLIS

ставленные решения были не менее футуристичны, чем сам стенд: прототип системы получения и регистрации биометрических образцов, программная платформа электронного голосования акционеров, сайт-экосистема для малого бизнеса «Бизнес онлайн ВТБ24»... Все представлено четко, наглядно и ясно, при этом без единого «бумажного костыля».

Ольга Дергунова любезно согласилась ответить на вопросы BIS Journal.

— Ольга Константиновна, Президент России обозначил одним из приоритетов ближайшего буду-

щего построение цифровой экономики, программа «Цифровая экономика Российской Федерации» утверждена, ее реализация началась. Что, по вашему мнению, могут привнести банки в этот процесс? Какие результаты планируют получить для себя?

— Для банков такая программная цифровизация в государственном масштабе — это прекрасная возможность и отличный стимул пересмотреть существующие банковские процессы и предложить рынку и контрагентам новые продукты и сервисы. Не стоит забывать, что банки всегда были пионерами в применении информационных

ВИЗИТНАЯ КАРТОЧКА



ДЕРГУНОВА
Ольга Константиновна
заместитель президента-
председателя правления
Банка ВТБ (ПАО)

Окончила факультет кибернетики Российской экономической академии народного хозяйства им. Плеханова, диплом с отличием.

Начало профессиональной деятельности О. Дергуновой связано с развитием отрасли информационных технологий в России. В 1994 г. О. Дергунова пришла в Microsoft, где проработала более 10 лет. С 2004 г. по 2007 г. в должности президента Microsoft, Russia&CIS занималась разработкой и реализацией долгосрочных стратегических планов корпорации, вопросами защиты интеллектуальной собственности, развитием образования в области ИТ.

В 2007 г. О. Дергунова вошла в состав Правления ОАО Банк ВТБ. В разные периоды зоной её ответственности являлись:

- ♦ работа с крупными корпоративными клиентами рыночных отраслей (товарно-сырьевые отрасли, инфраструктурный сектор, ИТ, связь);
- ♦ работа с дочерними банками ВТБ в СНГ, Европе, Азии и Африке с целью укрепления позиций Группы ВТБ как глобального игрока на мировом финансовом рынке и построения эффективного бизнеса.

В 2012 г. О. Дергунова перешла на работу в Правительство РФ, где заняла пост заместителя министра экономического развития РФ — руководителя Федерального агентства по управлению государственным имуществом. Под её руководством была утверждена новая концепция управления федеральной собственностью, разработана система показателей, характеризующих эффективность управления, создан единый общедоступный реестр по управлению госсобственностью.

В 2016 г. О. Дергунова вернулась в Банк ВТБ на должность заместителя президента — председателя правления. В настоящее время курирует вопросы технологической трансформации и интеграции банковского бизнеса, развития цифровых каналов, инструментов анализа данных, разработки комплексной программы автоматизации процессов.

технологий в сфере бизнеса. Первые мейнфреймы, профессиональные компьютеры, потом персональные. Только появлялось что-то новенькое, банки сразу брали это на вооружение.

— Да, так было, а сегодня?

— Сегодня, когда речь идет о цифровом финтехе — блокчейне, криптовалютах, хранении данных в облаках... — информационные технологии по-прежнему в центре внимания банковского сообщества, поэтому наличие у государства цели отказаться от бумажных документов, перевести бизнес-процессы в более удобный формат, чтобы дать потребителю возможность получать услуги в любой точке мира, в любое время вне зависимости от рабочих часов министерств и ведомств — все это мы приветствуем и поддерживаем.

Стоит отметить, что именно сами банки во многом и развивают эту программу. Например, для нас удаленное открытие счетов как для физических лиц, так и для бизнеса, является очевидной необходимостью. Мы эту задачу решаем и частично она уже выполнена. Многие банки предлагают свои способы подтверждения личности. Более того, масса сервисов и разного рода удаленных услуг сегодня оказывается не только банками, эстафету от них приняли и родственные организации — страховые, пенсионные, телекоммуникационные и другие, то есть уже возникло и работает то, что мы называем «экосистема».

— Затраты большие, а выгода?

— Банки первыми осваивают этот рынок. Например, когда будет принято решение о необходимости единой биометрической идентификации, все контрагенты начнут закладывать ее как принцип в свои системы. Но банки — первые, кто ее предложил, первые, кто ее разработал и начал использовать. И соответственно, наши клиенты в первую очередь получают — и уже получают — доступ к такого рода сервису.

— Если сравнить этот процесс цифровизации со стратегическим наступлением, где флагманами выступают крупные банки — ВТБ, Сбербанк, Альфа-банк и другие, можно ли сказать, что каждый из них выполняет свою тактическую задачу, строго обозначенную функцию под руко-

водством Банка России, или процесс имеет больше стихийный, рыночный характер? Можете ли вы обозначить функции лидеров?

— Главным драйвером этого процесса, конечно, является рынок. Именно он определяет, какой из банков будет внедрять ту или иную технологию. Когда, например, будет создана национальная биометрическая платформа и определена как универсальный способ идентификации граждан, для банков это будет очень удобно. Мы все воспользуемся этой услугой из рук государства и перестанем заниматься ею на рыночных основаниях. Но пока каждый из банков строит свою биометрию по своим принципам, т.к. данные процессы еще недостаточно стандартизированы.

Наличие единого стандарта позволяет государству масштабировать технологию, контролировать ее и развивать. Банкам это удобно, так как сокращаются издержки в этом направлении, и открываются возможности активизировать конкуренцию в других рыночных нишах. После биометрии, например, мы вплотную займемся улучшением machine learning в департаментах рисков. И станем совершенствовать эту технологию до тех пор, пока она не будет масштабирована до универсальной функции с единой платформой. Именно так мы конкурируем, предлагая новые функции, внедряя новые технологии, создавая новые процессы и сервисы. Кто-то быстрее, кто-то медленнее. Это и есть развитие, прогресс.

НАЛИЧИЕ ЕДИНОГО СТАНДАРТА ПОЗВОЛЯЕТ ГОСУДАРСТВУ МАСШТАБИРОВАТЬ ТЕХНОЛОГИЮ, КОНТРОЛИРОВАТЬ ЕЕ И РАЗВИВАТЬ. БАНКАМ ЭТО УДОБНО

— Какую роль в этом играют непосредственно регуляторы?

— Регуляторы очень активно работают в области финтеха. Банк России создал Ассоциацию финансовых технологий — своеобразный «защитный купол» над экспериментальной площадкой. Под ним разные банки тестируют и испытывают инновации, которые еще и законодательно никак не закреплены. Например, ряд банков пилотирует технологию распределенных реестров. Это дает возможность опробовать ее с разных сторон, разработать технологические и законодательные требования к ней, чтобы позволить рынку ее использовать в дальнейшем.

Рамки ассоциации не ограничивают какую-либо инициативу участников. Некоторые банки сразу параллельно с пилотами выстраивают целые технологические системы. Логика регулятора проста: чем многочисленнее и разнообразнее попытки рыночных игроков попробовать ту или иную технологию, получить опыт, обменяться им, тем более точно и надежно в итоге будет сформулирована задача. Эти проверенные устойчивые требования позволят создать новую технологическую платформу, на

которую дальше смогут все опираться. Регулятор задает вектор, в котором следует направить рыночную энергию и банковский ресурс, но при этом нет никакого диктата, жесткого распределения, кто чем должен заниматься.

— Группа ВТБ сегодня проводит масштабные внутренние преобразования — уже проведено одно и в ближайшее время будет завершено другое крупное слияние банков группы. С учетом уже имеющегося у ВТБ опыта, можно ли утверждать, что такая ситуация благоприятна для внедрения новых цифровых финансовых технологий, или указанные преобразования только отвлекают ресурсы от целей развития? Что вообще сегодня происходит в ВТБ с точки зрения развития финтеха?

— Объединение дало мощный толчок к переоценке оказываемых банком услуг и соответственно его информационных систем. По сути, мы сегодня строим банк в новом качестве. Пришло время создать новую архитектуру.

Команда нашего сводного ИТ департамента почти год анализировала каждую из нескольких сотен информационных систем на предмет целесообразности их сохранения в неизменном или слегка модернизированном виде на горизонте пяти лет. Параллельно мы спроектировали новую архитектуру информационных систем и прописали когда, что и как в течение пяти лет нужно изменить, достроить, усовершенствовать или создать заново.

Через несколько лет мы создадим удобный современный сборно-разборный модуль, состоящий из множества модулей меньшего размера, части которых легко заменяются с учетом потребностей клиентов чуть ли не каждую неделю. При такой конструкции навесить новый бантик на какой-либо сервис, добавить или изменить функции не составит труда.



Ольга Дергунова и Олег Тиньков

Этот красивый архитектурный и инженерный проект наш ИТ департамент сегодня воплощает в жизнь, а для клиентов это означает, что новые продукты будут появляться чаще, услуги предоставляться лучше и быстрее. Собственно, именно таким образом делается все, что необходимо для успешной конкуренции на рынке.

— Масштаб деятельности, качество предоставления финансовых услуг и уровень развития финтеха — это очевидные достижения ВТБ. А какое место в системе ценностей ВТБ занимает информационная безопасность?

— Еще несколько лет назад ИТ и ИБ были подразделениями с разными, можно сказать, базовыми философиями. Сегодня это по сути единая команда, они работают как близнецы-братья, но при этом у каждого из них есть своя четко определенная зона ответственности. Информационная безопасность — это во многом функция контроля, а ИТ — вопросы построения систем и дальнейшего их соответствия требованиям этого контроля. Но, как только заканчивается контрольная функция, начинается общее стратегическое планирование.

— Что изменилось?

— Изменились требования к банковским продуктам и сервисам. Теперь они изначально должны быть безопасными. Соответственно, изменились и подходы к их созданию. Сегодня безопасность закладывается в информационные системы с момента начала их разработки. Но подразделение ИБ выступает не в роли оторванного постановщика задач, а работает над проектами совместно с ИТ в режиме Scrum и Agile — как часть команды-разработчика. Еще одна важная задача, которую ИТ и ИБ решают совместно — сопровождение систем, построенных ранее. Это не-

прерывный пересмотр систем, закрытие изъянов, контроль функционирования того, что называется IT Health. За здоровьем, как известно, нужно следить постоянно, и показатели информационной безопасности тут — один из важнейших индикаторов.

И следующая большая задача — защита всех систем от текущих атак. Тут обе службы также работают как единый механизм.

— В последнее время Agile, как метод групповой работы над проектами, часто критикуют. Мол, работа ведется быстро, но небрежно, без должного документирования, чем закладывается мина на будущее...

— Agile — всего лишь инструмент, с которым нужно уметь работать. Мы активно используем Scrum и Agile. Несколько лет назад этот подход был детально описан и превратился в типовой, легкий для массового использования. Но надо помнить, что Agile — не панацея, он успешен для определенного класса задач, там, где требуется многофункциональный подход. У нас по такому принципу работает более сорока команд. Но мы так же используем и технологию Waterfall, требующую детальной спецификации.

— Как Банк ВТБ относится к необходимости выполнять требования регуляторов и стандартов, связанных с информационной безопасностью? Являются ли они помехой для развития цифровых финансовых технологий?

— У нас нет противоречий. Мы работаем совместно и с уважением относимся к требованиям, которые предъявляют регуляторы. Тут очень важно, что мы одновременно учимся новым подходам к разработке программных продуктов и систем информационной безопасности, смена стандартов проходит

для нас естественно, это — эволюция. В чем-то требования к безопасности меняются в сторону облегчения для нас, в чем-то наоборот ужесточаются, но мы прекрасно понимаем, что стандарты эволюционируют так же, как и информационные системы, вместе с ними.

— Проблема идентификации личности — одна из принципиальных в сфере банковской безопасности. По мнению многих специалистов она до сих пор не имеет универсального решения, и разные финансовые структуры вынуждены решать ее каждая по-своему. Например, Амазон планирует идентифицировать пользователей... по ушам. Как эту проблему решают в ВТБ?

— ВТБ активно участвует в разработке Единой системы идентификации и аутентификации (ЕСИА). ЕСИА — это цифровая платформа, позволяющая удаленно идентифицировать человека по его биометрическим характеристикам. Система создается по инициативе ЦБ и Минкомсвязи.

Пока клиенту для первичной идентификации все же необходимо явиться в банк. Мы надеемся, что в скором времени система будет масштабирована практически на все банки. Это позволит проводить идентификацию без предъявления документов и посещения офиса.

В начале этого года ВТБ завершил пилотный проект «Голосовая биометрия. Распознавание клиентов по голосу в контакт-центре», что позволяет создать удобный для людей и достоверный для банка процесс подтверждения операций. Мы ожидаем, что за счет внедрения голосовой биометрии произойдет оптимизация, повысится безопасность процедуры идентификации клиентов в контакт-центрах, а также появится возможность оперативного выявления мошенников. Эта технология готовится к внедрению в ряде сегментов в 2018 году.

В апреле 2017 г. мы завершили пилотный проект «Распознавание лица и голоса в мобильном банке». Это совсем новая технология, она работает по принципу «селфи + голос». На первом этапе создавался эталон лица и голоса пользователя, затем тестировалась

**ПОДРАЗДЕЛЕНИЕ ИБ ВЫСТУПАЕТ
НЕ В РОЛИ ОТОРВАННОГО
ПОСТАНОВЩИКА ЗАДАЧ, А РАБОТАЕТ
НАД ПРОЕКТАМИ СОВМЕСТНО
С ИТ В РЕЖИМЕ SCRUM И AGILE — КАК
ЧАСТЬ КОМАНДЫ-РАЗРАБОТЧИКА**

возможность верификации клиента по лицу и голосу при входе в мобильное приложение и при совершении платежа без подтверждения ОTR-кодом.

В июле 2017 г. также был запущен проект по речевой аналитике в контакт-центре. Механизм работы этой технологии заключается в том, что все диалоги сотрудников банка с клиентами в автоматическом режиме переводятся в текстовые сообщения и в дальнейшем анализируются специальной системой, которая позволяет получить информацию о соблюдении каждым сотрудником алгоритмов, стандартов и норм общения с клиентами во время разговора.

— Банк ВТБ участвует в пилоте по использованию облачной подписи для удаленной регистрации бизнеса. Можете ли вы прокомментировать результаты данной работы?

— Да, мы завершили экспериментальный пилотный проект по заказу Правительства РФ «Создание механизма удаленной идентификации физических лиц для дистанционного открытия банковских счетов и вкладов». ИТ-специалисты Группы ВТБ создали прототип системы, разработали и стандартизировали бизнес-процессы по удаленной регистрации бизнеса и дистанционному открытию счетов клиентам. В результате за три месяца пилотирования проекта на территории Москвы сервисом воспользовались 567 юридических лиц и индивидуальных предпринимателей. Из них 384 стали клиентами банка. Дальнейшие шаги по развитию этого сервиса зависят от регулятора.

— Сравнительно недавно в сфере банковских технологий возникла тема блокчейна. Сначала о нем говорили чуть ли не как о панацее, но теперь все чаще слышатся сомнения. Планирует ли развивать эту технологию ВТБ? Если да, то что для этого делается?

— В рамках Ассоциации финансовых технологий Банк России создает Мастерчейн — блокчейн-платформу для финансового рынка, которая готовится к массовому коммерческому использованию с 2019 года. В этом большом проекте мы взяли на себя развитие пилотного проекта по замене бумажных банковских гарантий на цифровые аналоги.



Финальной целью проекта является полный уход от бумажных гарантий, что избавит компании от необходимости собирать многочисленные документы в бумажном виде. В текущем пилотном проекте речь идет об удобном хранении, верификации и предоставлении выданных гарантий. Банки-участники будут иметь свои узлы в Мастерчейне для сбора информации и каналы ее выдачи заинтересованным сторонам. Доступ к информации будет быстрым, сама информация — актуальной, полной и защищенной от мошенничества и подделки. Тут, не сомневаюсь, наше подразделение ИБ сделает все возможное.

Первые результаты ожидаем к январю 2018 года. Но это только начало. Главным результатом развития платформы Мастерчейн должно стать создание общей инфраструктуры, которая будет способствовать эффективному взаимодействию между финансовыми организациями. Это позволит снизить издержки на создание различных сервисов и оперативно внедрять новые решения всеми участниками рынка.

— Одна из острейших проблем информационной безопасности — проблема квалифицированных кадров. Финтех сам по себе остро нуждается в таких кадрах, а ИБ в сфере финтеха — в квадрате. Например, Сбербанк был вынужден создать свою собственную программу подготовки кадров по информационной безопасности. А как эта проблема решается в ВТБ?

— Подразделение информационной безопасности у нас не настолько большое, чтобы создавать собственные учебные программы для подготовки кадров в сфере ИБ. Тут мы исходим из того, что требования и к ИБ, и к ИТ в целом стремительно меняются, усложняются. Через пять лет составленной сейчас учебной программы для выпускников ВУЗов будет недостаточно, чтобы свободно ориентироваться в актуальных проблемах профессиональной сферы. А что их ждет конкретно, какой будет эта профессиональная ситуация — предсказать невозможно. Поэтому мы стараемся набирать специалистов с хорошей базовой подготовкой, в первую очередь математической. Также они обязательно должны уметь учиться « всю свою жизнь » и меняться в зависимости от потребностей времени. По сути мы делаем ставку на личности.

— Наше интервью проходит на Форуме инновационных финансовых технологий FINOPOLIS 2017. Как вы оцениваете это мероприятие?

— Прекрасная повестка, интересные докладчики и очень актуальные темы. Мне нравится, что на этом форуме обсуждаются технологии, которые банки еще широко не применяют: искусственный интеллект и machine learning, распределенные реестры, блокчейн и другие. Очень важно смотреть вперед, в будущее, и говорить о том, что нас ожидает, а не только о текущих проблемах.

Беседовал Игорь Некрасов



Григорий МАРШАЛКО

эксперт технического комитета по стандартизации
ТК 26, эксперт ISO/IEC JTC 1/SC 27, ISO TC 307

НЕ ПАНАЦЕЯ

УГРОЗЫ БЕЗОПАСНОСТИ БИОМЕТРИЧЕСКИХ СИСТЕМ

Появление новых информационных технологий всегда несет не только новые возможности по оптимизации процессов взаимодействия, но и сопровождается появлением новых угроз безопасности, которые в случае их игнорирования могут свести на нет потенциальные выгоды от внедрения таких технологий. Своевременная оценка таких угроз и выработка адекватных мер противодействия является краеугольным камнем развития информационно-телекоммуникационной области.

Одной из таких активно внедряемых в настоящее время технологий является биометрическая идентификация. Биометрия, оформившаяся как самостоятельная наука в 19 веке, уже к его второй половине использовалась для идентификации преступников в виде т.н. бертильонажа — измерения и регистрации антропометрических данных человека.

В настоящее время с развитием цифровых технологий биометрические методы идентификации личности все активнее внедряются в системах контроля доступа, банковской сфере, транспорте и т.п.

Биометрические методы идентификации заключаются в измерении уникальных параметров человека, таких, например, как ДНК, отпечатки пальцев, радужная оболочка глаза, почерк, голос или походка, и сравнении их с заранее зарегистрированными эталонами.

Отметим, что могут рассматриваться как статические признаки (отпечатки пальцев, геометрия руки или вен, сетчатка глаза), так и динамические (голос, почерк, походка).

В целом, система биометрической идентификации подразумевает наличие процессов (см. рис 1):

- ♦ регистрации пользователя, при котором биометрические данные заносятся в систему в виде биометрического шаблона;

- ♦ верификации, при котором биометрический шаблон пользователя сравнивается с хранящимся в базе эталоном.

Важно понимать, что в силу возможной нестабильности биометрического образа во времени (например, при использовании голосовой идентифика-

ции), ошибок при записи, возникающих в силу аппаратных ограничений считывающего сенсора, влияния окружения (шум, освещение), биометрические характеристики пользователя могут не в полной мере соответствовать полученным при регистрации и хранящимся в базе. Это приводит к возникновению ошибок идентификации, вследствие чего все процедуры биометрической идентификации являются вероятностными и характеризуются:

- ♦ ошибкой первого рода (false rejection rate) или вероятностью того, что человек может быть не распознан системой;

- ♦ ошибкой второго рода (false acceptance rate) или вероятностью того, что один человек может быть принят за другого.

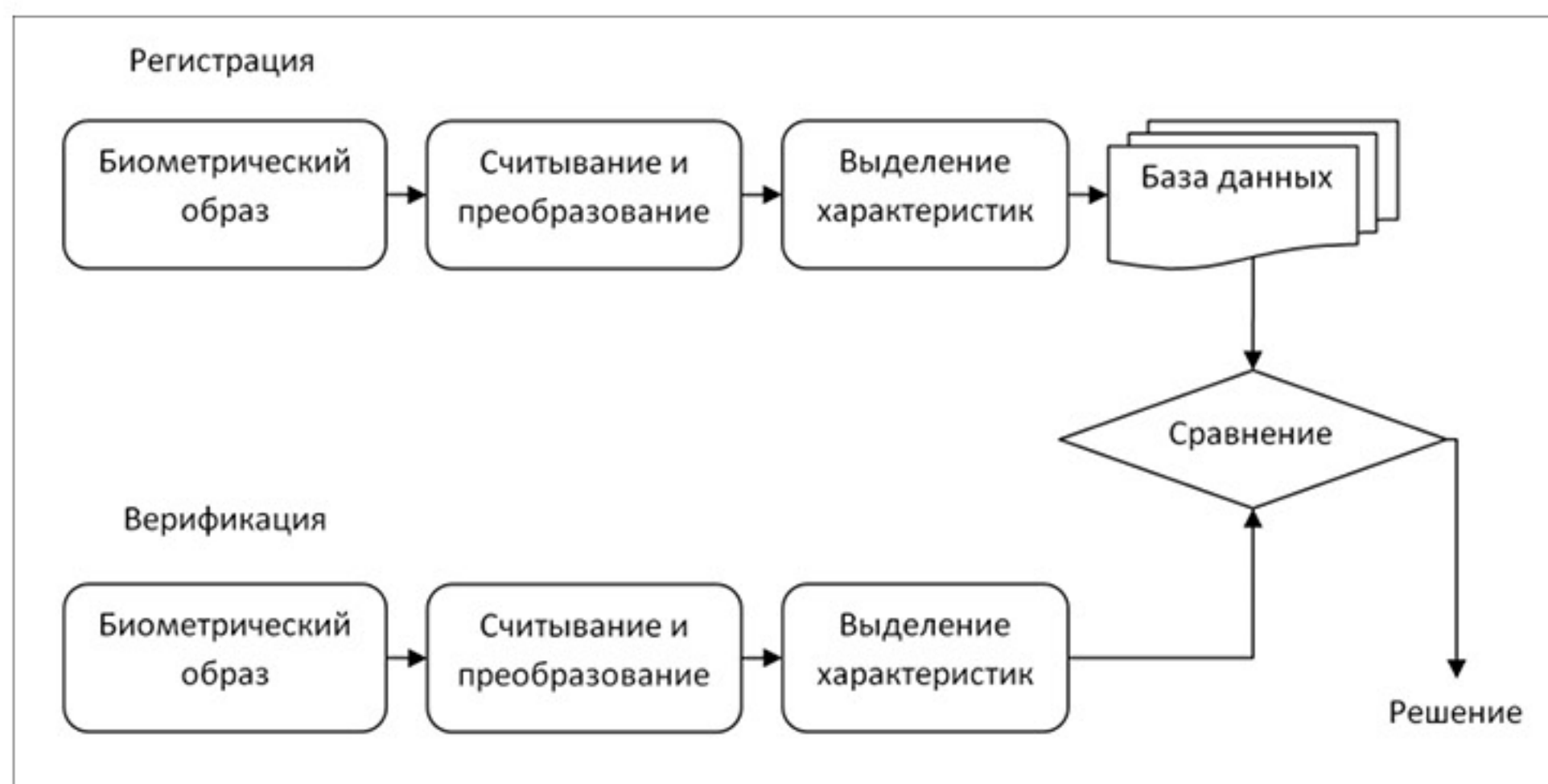


Рисунок 1. Общая схема работы системы биометрической идентификации

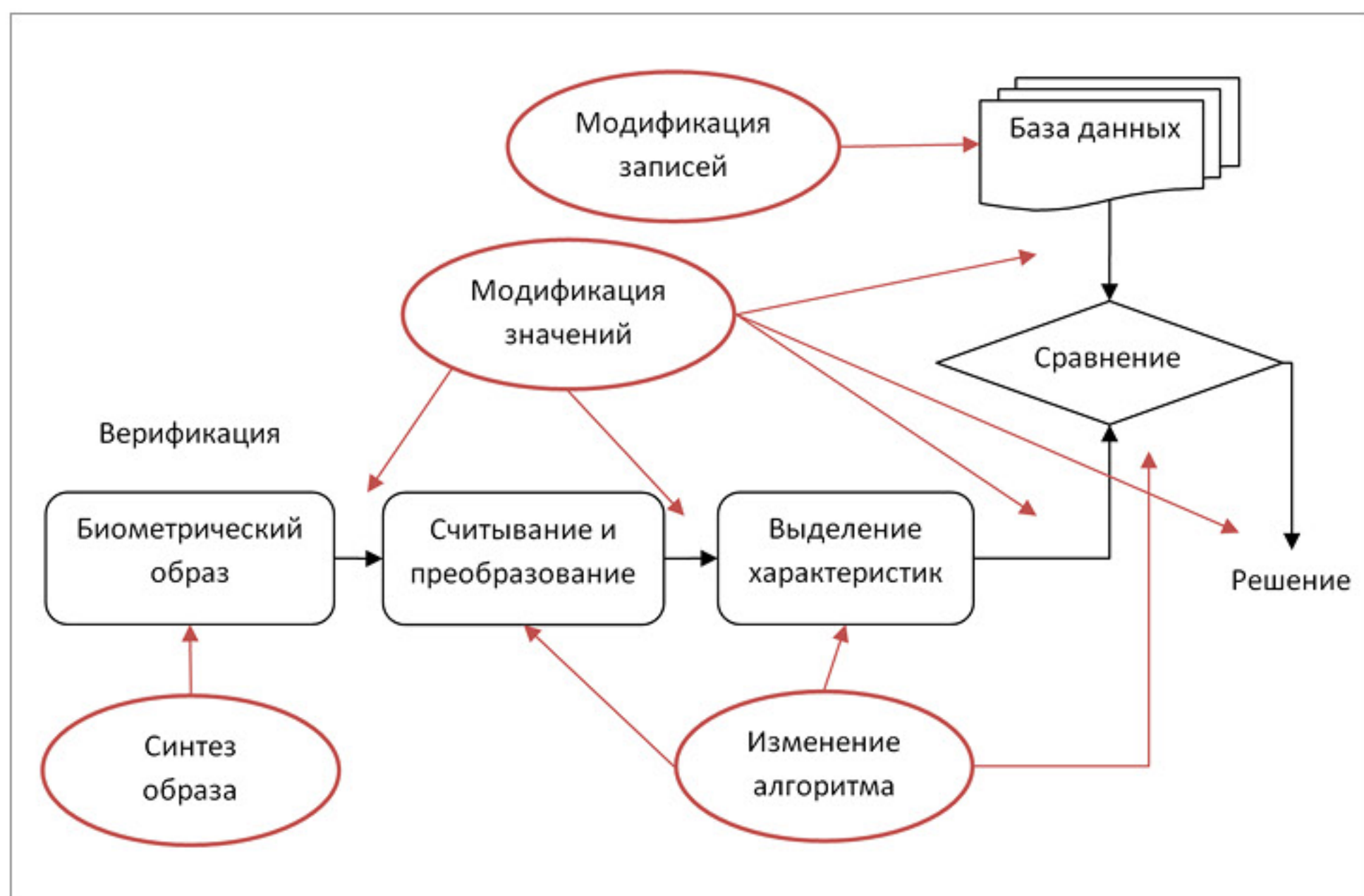


Рисунок 2. Возможные векторы атак, ISO/IEC 30107-1:2016

С точки зрения обеспечения информационной безопасности на каждом этапе функционирования биометрической системы возможно возникновение тех или иных векторов атак (рис. 2).

Большинство из них характерно для любой информационной системы и требует стандартных подходов к защите. Специфическими для биометрических систем является проблема синтеза (подделки) биометрического образа.

Наибольшую проблему с точки зрения практического применения биометрических систем представляет невозможность отчуждения биометрического образа человека в случае его компрометации. Для наиболее широко используемых биометрических параметров, таких как отпечатки пальцев, голос, лицо, эта проблема стоит наиболее остро.

При этом развитие науки, которое, с одной стороны, позволяет существенно повысить качество распознавания, одновременно позволяет создавать более простые и совершенные способы обхода биометрических систем.

Например, в работе K. Cao, A.K. Jain, *Hacking Mobile Phones Using 2D Printed Fingerprints*, авторы демонстрируют возможность обхода биометрической идентификации ряда смартфонов с помощью отпечатанного токопрово-

дящими чернилами отпечатка пальца (рис. 3).

Как показано в работе A. Roy, N. Memon, A. Ross, *MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems*, несовершенство считывающих сенсоров отпечатков пальцев, используемых, например, в смартфонах, а именно ограничение считываемой поверхности пальца, приводит к возможности синтеза «универсальных» отпечатков пальцев, которые могут быть использованы для доступа к большому числу смартфонов пользователей.

Подобные ситуации характерны и для других биометрических параметров. Например, в работе K. Yerra, M. Prasad, *Acessorize to a crime, Real and Stealthy attacks on state-of-the-art face recognition* показана возможность модификации изображения лица посредством специальным образом синтезированных очков таким образом, чтобы биометрическая система принимала изображенного человека за другого.

Широко внедряемые в банковской сфере системы голосовой идентификации, как показано в работе D. Mukhopadhyay, M. Shirvanian, N. Saxena, *All Your Voices Are Belong to Us: Stealing Voices to Fool Humans and Machines*, так же могут быть достаточно просто обойдены с помощью систем синтеза речи.

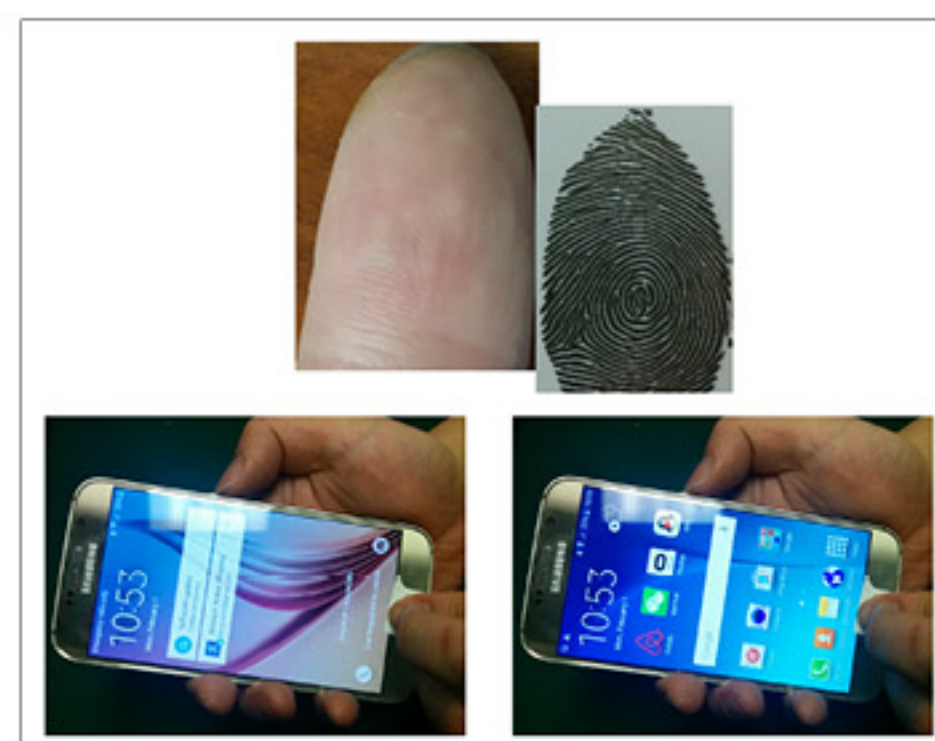


Рисунок 3. Исходный биометрический, отпечатанный синтетический образы и разблокировка телефона

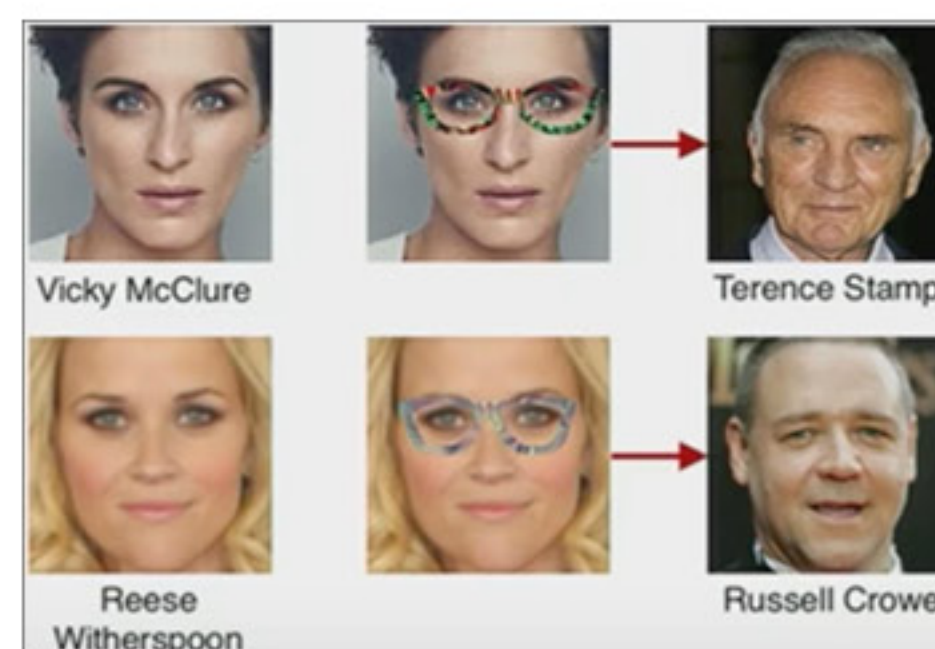
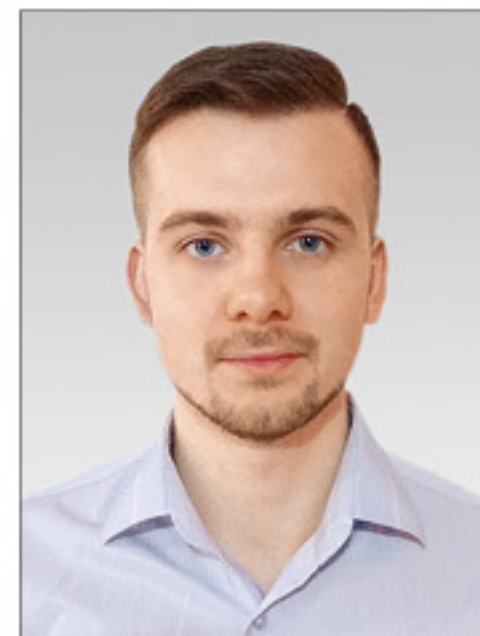


Рисунок 4. Модификация изображения и некорректная идентификация

Зачастую биометрию рассматривают как технологию, которая в ближайшее время вытеснит существующие методы идентификации и даже аутентификации. Однако приведенные нами примеры показывают, что, как и любая другая технология, биометрия не является панацеей и подвержена своим, зачастую достаточно специфичным, угрозам. Несмотря на то, что человек идентифицирует другого человека фактически по набору биометрических параметров, он это делает в широком контексте окружающей обстановки и учитывает существенный набор внешних факторов.

В этой связи не следует рассматривать биометрию исключительно в качестве единственной альтернативы существующим методам идентификации и аутентификации. Но в то же время ее совместное использование с другими существующими технологиями, такими, например, как электронная подпись, может дать определенный положительный результат.

БОЛЬШИЕ ДОСТОИНСТВА — БОЛЬШИЕ НЕДОСТАТКИ



Алексей ПЕРЦЕВ
специалист
Департамента аудита
защищенности
Digital Security

БЛОКЧЕЙН, КРИПТОВАЛЮТЫ И ВОТ ЭТО ВОТ ВСЁ

ОСНОВНЫЕ ПОНЯТИЯ

Прежде, чем мы начнем непосредственно рассматривать основные тенденции мира криптовалют, стоит определить с ключевыми понятиями.

Блокчейн (blockchain). Если не вдаваться в детали, блокчейн — это постоянно растущий список записей, называемых блоками (block), которые связаны в цепочку (chain) с помощью криптографии. Каждый блок содержит время его создания, набор транзакций (не обязательно денежных) и криптографический хеш¹ предыдущего блока (так они и связываются в цепочку). Он похож на бухгалтерскую книгу, хранящую транзакции между участниками сети, причем у каждого участника есть своя копия этой книги, и он взаимодействует с другими непосредственно, то есть напрямую (peer-to-peer network). Благодаря особенностям дизайна, блокчейн устойчив к «редактированию» данных — единожды внесенная запись не может быть изменена без изменения всех лежащих ниже блоков (это является сложной математической задачей, на практике не разрешимой).

Идея блокчейна появилась уже давно (1991 г.)², однако впервые получила практическое применение для создания криптовалюты Bitcoin в 2008 году.

¹ Хеширование (hashing) — преобразование входных данных произвольной длины в (выходную) строку фиксированной длины (хеш).

² <https://link.springer.com/article/10.1007/BF00196791>

Криптовалюта (на примере Bitcoin). В основе каждой³ криптовалюты лежит идея блокчейна — все новые транзакции пользователей сети собираются в блок, и далее находится его хеш для помещения в цепочку. Эта операция может быть выполнена любым участником сети, причем в блокчейн будет помещен блок того, кто это сделает первым. На данном этапе любую криптовалюту поджидает нюанс (оставим в стороне проверку действительности самих транзакций). Нахождение хеша от данных произвольной длины занимает у современных компьютеров мгновение, поэтому теоретически любой может переписать всю историю блокчейна в свою пользу. Чтобы этого не происходило, любой криптовалюте нужен некий механизм консенсуса, который позволял бы всем участникам сети убедиться в существовании одной и единственной версии блокчейна, а также делал бы нахождение хеша блока сложной, алгоритмически неразрешимой задачей, либо каким-либо другим способом реализовывал децентрализацию.

В криптовалюте Bitcoin такой механизм консенсуса называется proof-of-work. Заключается он в следующем: для всех участников сети объявляется правило, согласно которому полученный хеш блока должен быть меньше определенного числа или, как еще говорят, должен быть «краси-

³ На самом деле не каждой, но в данном обзоре мы касаемся только таких.

вым», т.е. содержать определенное количество нулей в начале, например, «000000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d»⁴. Это и является неразрешимой задачей — нельзя написать алгоритм, выдающий такие хеши для произвольных данных. Поэтому участники используют для своих целей перебор — добавляют некий кусочек данных (nonce) в блок, выполняют хеширование и проверяют, выполнено ли условие proof-of-work. Если оно не выполнено, то изменяют nonce и повторяют заново. Этот процесс называется майнингом (mining), а участников, выполняющих эту работу, именуют «майнерами». Майнер, нашедший подходящий хеш, получает вознаграждение — так, помимо прочего, образуются новые монеты в сети (эмиссия).

Таким образом, заранее неизвестно, кто именно найдет хеш для следующего блока — за счет этого достигается децентрализация, а также это дает возможность участникам не доверять друг другу. Bitcoin и другие криптовалюты обладают еще массой других замечательных свойств. Однако эти два самые «продающие». Следует так же знать, что существуют другие механизмы консенсуса, избавляющие участников от необходимости делать «бесполезные» энергозатратные вычисления, такие как proof-of-stake, proof-of-burn и др.⁵

⁴ Шестнадцатеричная запись числа

⁵ <https://www.coindesk.com/short-guide-blockchain-consensus-protocols/>



Последнее, перед тем как мы перейдем к следующей части, — это ответ на вопрос: «А что мешает майнеру изменить мою транзакцию, чтобы я остался без денег?». Отвечает Сатоши Накомото (создатель Bitcoin): «Каждая выпущенная участником транзакция обладает цифровой подписью!». То есть любой в сети может проверить подпись и удостовериться, что транзакция не подделана. Если изменить данные в транзакции (например, адрес получателя), то подпись станет недействительной и не будет включена в блок.

Данное описание не является исчерпывающим (заинтересовавшийся читатель может найти более детальное описание в *whiterpaper* конкретной криптовалюты), однако, оно было необходимо для того, чтобы перейти к следующему блоку.

Смарт контракты. В 2013 году Виталий Бутерин представил миру криптовалюту под названием Ethereum. Одним из ее плюсов по сравнению с Bitcoin является возможность реализации смарт контрактов. Смарт контракт в контексте сети Ethereum — это некая сделка между участниками сети, описанная языком логики с помощью специального языка программирования. Смарт контракт существует в блокчейне и наследует его ключевое свойство: контракт не может быть изменен ни одной из сторон или другими участниками сети. Участники взаимодействуют со смарт контрактом посредством транзакций. А исполняется⁶ контракт в процессе майнинга. Поскольку результаты

⁶ Имеется в виду исполнения инструкций машинного кода.

работы смарт контракта записываются в блокчейн, майнеру необходимо выполнить те действия, которые предписывает контракт, прежде чем начинать искать необходимый хеш.

Рассмотрим подробнее типы смарт контрактов:

- ♦ Обычный смарт контракт — минимальная единица автоматизации. Может и не принимать никаких финансовых решений вовсе;

- ♦ DApp (decentralized application) — один или несколько контрактов, выполняющих функции доверенного лица при взаимодействии участников;

- ♦ DO (decentralized organization) — обычно масса контрактов, описывающих участников организации (инвесторы, работники, потребители и т.д.), а также протокол взаимодействия между ними. От DApp, главным образом,

отличается тем, что больше похожа на организацию, чем на сервис;

♦ DAO (decentralized autonomous organization) — в сущности, то же, что и DO, однако, меньше зависит от людей. Слово autonomous здесь — маркетинговый ход, на самом деле такая система должна полностью сама жить в сети и принимать решения самостоятельно, что очень близко к искусственному интеллекту;

♦ DAC (decentralized autonomous corporation) — в отличие от DAO, DAC приносит дивиденды держателям внутренней валюты.

ПРИМЕНЕНИЕ В РЕАЛЬНОЙ ЖИЗНИ

Теперь можно перейти к тому, какое применение блокчейн, криптовалюты и смарт контракты нашли в реальной жизни.

Замена фиатных денег. Валюты с блокчейном в их основе способны полностью заменить существующие деньги различных государств (фиат), причем в процессе взаимодействия между участниками не будет третьих лиц. Также различные криптовалюты реализуют такие полезные свойства, как анонимность и необратимость. Комиссия, как и в обычных денежных переводах, взимается, но не зависит от суммы и зачастую может регулироваться самим отправителем — чем больше комиссия, тем быстрее пройдет транзакция. Иногда она и вовсе отсутствует.

Медицина. Внедрение блокчейна в процесс организации страхования в здравоохранении могло бы серьезно улучшить систему в целом. Во-первых, такие технологии позволяют организовать единую БД, в которой данные сверялись бы одним нажатием воображаемой компьютерной клавиши. Во-вторых, оплата счетов по страховым полисам может быть полностью автоматизирована, поскольку сама структура блокчейна будет препятствовать ошибкам при оплате, двойным расходованиям и т.д. Освободившиеся от обслуживания раздутого штата контролёров и учётчиков средства можно было бы пустить на повышение качества медицинских услуг⁷.

⁷ <http://forklog.com/longrid-blokcheyn-i-meditsina/>

ЕСЛИ КТО-ТО НЕ СОГЛАСЕН С МНЕНИЕМ СООБЩЕСТВА ИЛИ РАЗРАБОТЧИКОВ, ОН МОЖЕТ ПРОСТО УБЕДИТЬ УЧАСТНИКОВ СЕТИ ПЕРЕЙТИ НА СВОЮ ВЕТВЬ БЛОКЧЕЙНА ИЛИ КАКОЙ-ЛИБО КРИПТОВАЛЮТЫ. И ЕСЛИ НЕОБХОДИМОЕ ЧИСЛО СОГЛАСИТСЯ, В МИРЕ ПОЯВИТСЯ ЕЩЕ ОДНА КРИПТОВАЛЮТА

Банковское дело. Поскольку технология хорошо зарекомендовала себя в финансовом секторе, многие банки стремятся ее задействовать. Например, Сбербанк готовит запуск платформы торгового финансирования на «блоковой цепи». На блокчейн должны перейти внутренний документооборот и обслуживание клиентов по большинству вопросов⁸.

Казино. Технология блокчейна способна серьезно изменить мир азартных игр. На ее основе можно построить казино целиком. Доверия к такому казино будет больше, ведь его логика — в неизменяемом блокчейне⁹.

Сфера услуг. Здесь блокчейн облегчит взаимодействие между исполнителем и заказчиком. Как пример можно привести фриланс-биржу Ethlance¹⁰, основанную на взаимодействии участников посредством смарт контрактов.

ВАЖНОЕ О БЕЗОПАСНОСТИ

Недостатки блокчейна. Механизм консенсуса proof-of-work опирается на то, что в сети не должно быть майнера, обладающего > 51% вычислительной мощности сети. Иначе он может единолично создать свою альтернативную ветвь текущего блокчейна (fork), смайнить в ней на один блок больше, чем в основной цепи (это может получиться, подсказывает нам теория вероятности), и тогда эта альтернативная ветвь будет

⁸ <https://bosfera.ru/press-release/blokcheyn-v-bankovskoy-sisteme-vzglyad-sberbanka>

⁹ <https://dao.casino/>

¹⁰ <https://ethlance.com/>

принята всеми остальными участниками сети как оригинальная (по правилам proof-of-work).

Пример. Одна из российских компаний подверглась атаке Ransomware, в ходе которой вымогатели попросили выкуп за зашифрованные данные в биткоинах. Поскольку организация обладает огромными вычислительными мощностями (как раз больше 51% мощности сети Bitcoin), решено провернуть следующий трюк:

1. Компания совершает транзакцию на адрес вымогателей, которая попадает в следующий блок. Параллельно начинает майнить альтернативную ветвь блокчейна, в которой она ничего не платила вымогателям.

2. Кто-то из участников сети находит действительный хеш для блока с транзакцией на счет вымогателей, те видят у себя в кошельке прибавление на нужную сумму и на радостях публикуют ключ для расшифровки у себя в Twitter.

3. К этому моменту компания уже нашла валидный хеш для своего альтернативного блока и вступила в гонку с остальной сетью за то, чтобы найти нужный хеш для следующего блока с новыми транзакциями. Скорее всего, она сделает это быстрее остальной сети, поскольку обладает большей мощностью. В любом случае, можно попробовать со следующими блоками.

4. В случае успеха, компания рассылает всем остальным участникам свою альтернативную ветвь, и вся сеть ее принимает — по правилам proof-of-work все участники принимают за основную цепь наибольшей длины. Та-

ким образом, в кошельке компании так и останется отправленная сумма, а вымогателям не достанется ничего.

Читателю предлагается самому решить, кто в этой истории отрицательный персонаж — криптовымогатели или компания, совершившая атаку на криптовалюту Bitcoin.

Альтернативные цепочки иногда создаются и без каких-либо атак. Насколько часто — зависит от настроек proof-of-work. Поэтому, если вы получили транзакцию, рекомендуется дождаться нескольких подтверждений (confirmations), прежде чем «отгружать товар». Чем глубже блок с вашей транзакцией в блокчейне, тем больше вероятность, что не была случайно создана другая цепь без вашей транзакции и ее примет вся сеть. А это, как вы понимаете, занимает время, — в случае с биткоином каждый блок добывается каждые десять минут, а дожидаться рекомендуется хотя бы до трех подтверждений. Отметим, что есть и другие криптовалюты, которые обладают гораздо меньшим временем транзакций, в том числе совершаемые мгновенно.

Если кто-то не согласен с мнением сообщества или разработчиков, он может просто убедить участников сети перейти на свою ветвь блокчейна или какой-либо криптовалюты. И если необходимое число согласится, в мире появится еще одна криптовалюта. Так, например, произошло во время скандала с криптовалютой Ethereum Classic, когда хакеры украли \$60M у организации TheDAO. И когда появилась Bitcoin Cash как улучшенная версия оригинальной валюты Bitcoin.

Также сети могут подвергаться DDoS-атакам. Например, в сентябре 2016 года сеть Ethereum практически не функционировала, поскольку майнеры были заняты обработкой миллионов транзакций злоумышленников. Для этого требовалось выполнить одну дешевую, но затратную для майнеров операцию — нужно было перечитать информацию о состоянии блокчейна с диска. И все майнеры в сети были заняты именно этим вместо того, чтобы осуществлять работу сети.

Недостатки смарт контрактов. Поскольку смарт контракт является

программой, написанной человеком, всегда есть шанс наличия в нем уязвимостей. Ситуацию усугубляют такие моменты:

- ♦ языки смарт контрактов очень свежие;
- ♦ документация не всегда целиком отражает возможности языка;
- ♦ присутствует своя специфика работы на блокчейне;
- ♦ отсутствуют полноценные среды разработки, к которым все так привыкли;
- ♦ список можно продолжать...

Поэтому неизменяемость смарт контрактов не только их преимущество, но и недостаток. Ошибки программистов порой приводят к потерям серьезных денег^{11,12}, а исправить уже ничего нельзя. Единственный способ — это выпустить новый исправленный смарт контракт и перевести на него Ether (внутренняя валюта сети Ethereum) со старого, если он еще остался.

Но даже если исключить человеческий фактор в написании контракта, то при работе более-менее крупного приложения (организации) избавиться от него вряд ли получится. Ведь смарт контракт не вездесущ, он не сможет, например, подключиться к метеостанции и проанализировать, что погубило урожай и нужно ли выплатить компенсацию фермеру.

Поэтому для получения данных из внешних источников нужны Оракулы. А это либо люди, либо так или иначе подконтрольная им техника. Создатели прикладывают серьезные усилия, чтобы сеть была как можно менее зависимой от людей, однако это не всегда возможно.

Под сомнение можно поставить и успех широко афишируемой «децентрализации» криптовалют. Рынок майнинга Bitcoin представляет собой около 20 компаний (пулов), в руках которых сосредоточена огромная вычислительная мощность сети. Произошло это потому, что были изобретены специальные устройства ASIC (Appli-

cation-specific integrated circuit), которые пригодны лишь для того, чтобы майнить, но делают они это гораздо эффективнее современных процессоров или видеокарт. Так вот, компании обладают тысячами таких устройств и, договорившись, они способны проворачивать различные неприятные трюки.

Разработка ASIC для майнинга в сети Ethereum — слишком дорогое удовольствие (сеть специально так спроектирована). Однако есть другие нюансы. Для того, чтобы со смарт контрактами было удобно взаимодействовать прямо из браузера без установки дополнительного ПО, разработчики используют библиотеки (например, web3), которые обращаются к специальным шлюзам между сетью интернет и сетью Ethereum. Компаний, предоставляющих такие шлюзы, пока всего две. Если использовать подобный подход, теряется чуть ли не главное преимущество криптовалюты — децентрализация. Из этой ситуации можно выйти, подняв свой собственный шлюз, но это слегка выходит за рамки привычного user experience среднестатистического фермера.

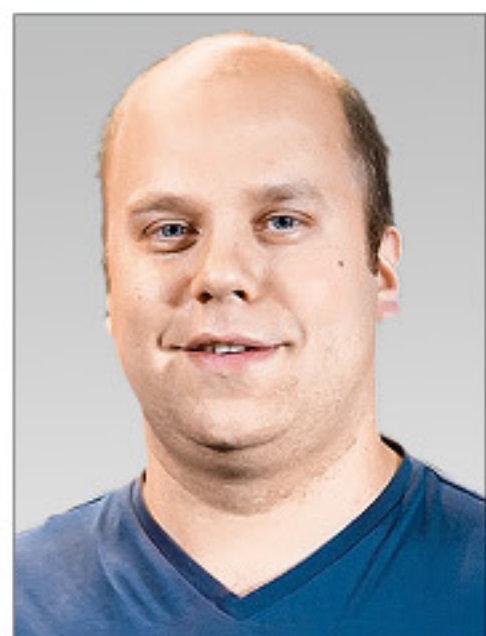
* * *

Итак, мы познакомились с миром криптовалют, получили представление о том, что такое блокчейн, криптовалюта и смарт контракты. Наверняка интуиция уже подсказывает вам, где все это можно применить. Из новых словечек, релевантных бизнесу, привнесенных в нашу жизнь вместе с блокчейном, осталось разве что понятие ICO (Initial coin offering), но и это не что иное, как IPO (Initial public offering), разве что проходит чаще всего под контролем смарт контракта.

Также мы прошли по основным нюансам, о которых не говорят перед ICO. И теперь, слушая очередную презентацию криптовалюты, спасающей мир, вы сможете лучше оценить идею проекта и задать правильные вопросы, не только с точки зрения бизнеса, но и реализации. Удачи!

¹¹ <https://www.coindesk.com/understanding-dao-hack-journalists/>

¹² <https://www.ethnews.com/massive-hack-hits-ethereum-parity-clients-more-than-30m-of-ether-still-at-large>



Алексей АРХИПОВ
руководитель блока
QIWI-блокчейн

ЭКОНОМИКА ТОКЕНОВ

НОВАЯ ЭКОНОМИКА —
НОВЫЙ ТИП ОТНОШЕНИЙ

Тема блокчейна и криптовалют становится все популярнее, иногда блокчейн даже называют «новым интернетом». Но мне кажется, что это скорее важное продолжение того, что нам дал информационный обмен.

ПО СПИРАЛИ РАЗВИТИЯ

Каждый период развития интернета прибавлял новое качество — сначала это был просто обмен информацией, потом обмен товарами, затем общение людей в социальных сетях, потом цифровые продукты, и наконец — своя замкнутая экономика. Этой цифровой экономике нужна своя, изначально цифровая, система обмена ценностями.

В ПОИСКАХ НОВОЙ СУЩНОСТИ

В этой цифровой экономике личности также цифровые, а товары и активы могут быть токенизированы. Из-за того, что в цифровом мире все подвержено изменениям, копируется, изменяется — нужны и надежные технологии, которые гарантировали бы неизменность.

К тому же устоявшиеся на сегодняшний день технологии проектировались для физического, а не цифрового мира, и с их помощью реализовать эти потребности оказалось очень сложно.

Физический мир «скрепляют» физические законы, для цифрового мира также нужны системы и способы, которые делают базовую, ценностную часть этого мира неизменной. В этом случае в цифровом мире появляется опора, которая может свободно существовать без подтверждения в физическом мире — самостоятельная сущность, а не просто цифровая копия.

БЛОКЧЕЙН

Для свободного перемещения ценностей нужны новые методы их передачи и хранения, то есть подобие собственной финансовой системы и инструментов, применимых в интернет-среде. Такими методами могут быть криптовалюты и токены.

Блокчейн, при всех своих характеристиках, в данном случае идеально подходит в качестве фундамента, способного обеспечивать базовую безопасность и бесперебойность работы системы.

КУРС ВЗЯТ

И самые успешные проекты в блокчейн в последнее время — проекты, делающие ICO (initial coin offering), показывают, что рынок активно развивается в этом направлении.

При большом количестве недостатков, ICO тренд стал первым крупным

свидетельством того, как актив или товар может быть трансформирован в токен и привлекать деньги, опять же в форме, свойственной для интернета — криптовалюте.

ПОЛЕЗНЫЙ ФЕНОМЕН

На первый взгляд кажется, что драйвером ICO является только стимул собрать деньги с инвесторов. Однако это и способ перевести ваши товары и отношения с клиентами в новую цифровую форму.

Механизм ICO создал новый феномен — ситуацию, когда вы совершенно иначе можете монетизировать свой бизнес. Вы можете создать платформу с открытым кодом, которая управляется пользователями, не влияя на свой продукт и сервис никак, или влияя только идеологически. При этом токен, который вы выпустили под эту платформу, может расти в цене и, тем самым, приносить вам доход.

НОВЫЙ ТИП ОТНОШЕНИЙ

Мне кажется, это совершенно новый способ монетизации идей, когда, не создавая частную компанию и не управляя бизнесом, вы тем не менее имеете шанс заработать на том, что вы придумали.

**ИЗ-ЗА ТОГО, ЧТО В ЦИФРОВОМ МИРЕ
ВСЕ ПОДВЕРЖЕНО ИЗМЕНЕНИЯМ,
КОПИРУЕТСЯ, ИЗМЕНЯЕТСЯ — НУЖНЫ
И НАДЕЖНЫЕ ТЕХНОЛОГИИ, КОТОРЫЕ
ГАРАНТИРОВАЛИ БЫ НЕИЗМЕННОСТЬ**

Такая новая экономика, на мой взгляд, формирует новый тип отношений — экономику токенов, где люди обмениваются услугами и товарами в открытых платформах, но это тем не менее все равно приносит доход их создателям.

ТРУДНЫЙ ПУТЬ К УНИВЕРСУМУ

ВОПРОСЫ ОБЛАЧНОГО ХРАНЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ С ОБЕСПЕЧЕНИЕМ ЮРИДИЧЕСКОЙ СИЛЫ

(Окончание. Начало в № 3/2017)



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

ДОВЕРИЕ И ВРЕМЯ

С учетом «конечности во времени» электронной подписи возможны следующие подходы:

- ♦ Снятие ЭП с документа;
- ♦ Использование сертификатов ключа проверки электронной подписи на срок более (или существенно более) 5 лет;
- ♦ Использование специальных форматов ЭП. К ним относится «усиление ЭД» в соответствии со стандартами, принятыми, например, в ЕС;
- ♦ Снятие ЭП через оформление специального внутреннего электронного акта (служебного ЭД) и включение его в состав метаданных, содержащих, помимо прочего, сведения о достоверности, целостности и аутентичности ЭД принятого на хранение.

На последнем из указанных подходов следует остановиться более подробно.

На рис. 1 приведена логическая схема представления содержания единицы хранения электронного документа в соответствии с ГОСТ Р ИСО 23081-1-2008. Если рассмотреть частоту обращений и операций с представленными элементами, то оказывается, что файл, содержащий сам документ (контент), практически не изменяется в ходе жизненного цикла его хранения. В отличие от этого наиболее подвижной составляющей единицы хранения являются метаданные документа, в которые на регулярной основе вносится дополнительная информация. При этом все компоненты, включенные в состав едини-

цы хранения, должны быть неразрывно связана как между собой, так и с самим сохраняемым документом, чем обеспечивается возможность сохранения аутентичности документа, позволяющей придавать ему юридическую силу тогда, когда это будет необходимо. Таким образом, речь идет о создании и использовании инструментов доверия.

Каждая такая операция должна регистрироваться, что служит надежным источником сведений о совершенном действии, в связи с чем эта процедура представляет собой некий «электронный акт».

ЦЕПОЧКА «ЭЛЕКТРОННЫХ АКТОВ»

Обеспечение доверия к создаваемому электронному акту в перспективе наиболее целесообразно осуществлять через механизм криптографической привязки

к хранимому ЭД, регистрацию фактов проверки исходного ЭД, полномочий проверяющего, времени, статуса, результатов проверки, видов подписей, принятие решения и т.д. Таким образом, возникает цепочка связанных электронных актов, оформленная в блок и включаемую в блок безопасности метаданных.

Данный подход позволяет существенно упростить организацию долговременного хранения ЭД с обеспечением юридической силы, так как выделяет два практически независимых процесса:

- ♦ непосредственное хранение самих ЭД (контента) с выполнением стандартных процедур обеспечения аутентичности хранимых данных, созданием резервных, страховых и архивных копий;
- ♦ хранение и сопровождение самих метаданных документа с поддержанием их аутентичности.

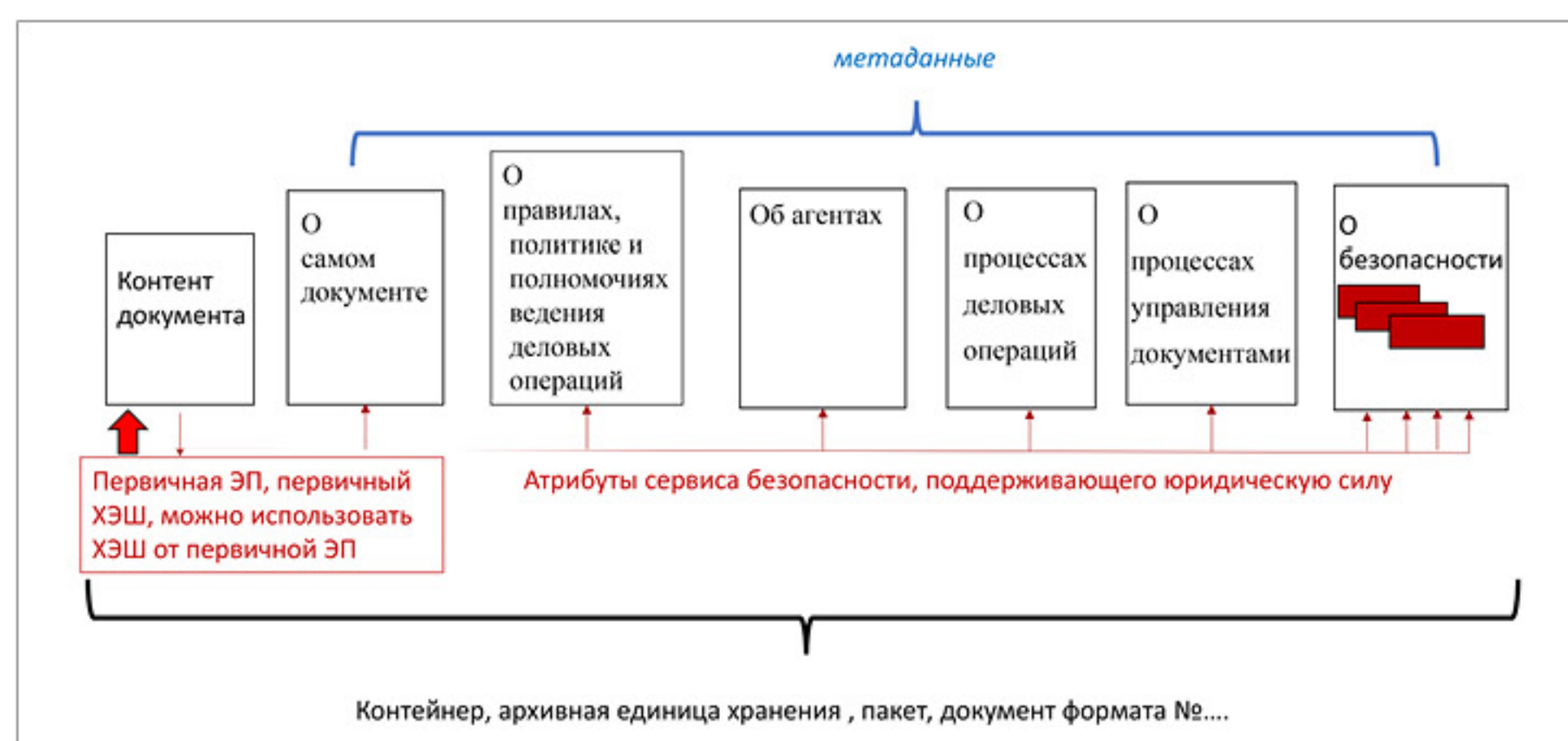


Рисунок 1. Полная структура электронного документа и его метаданных

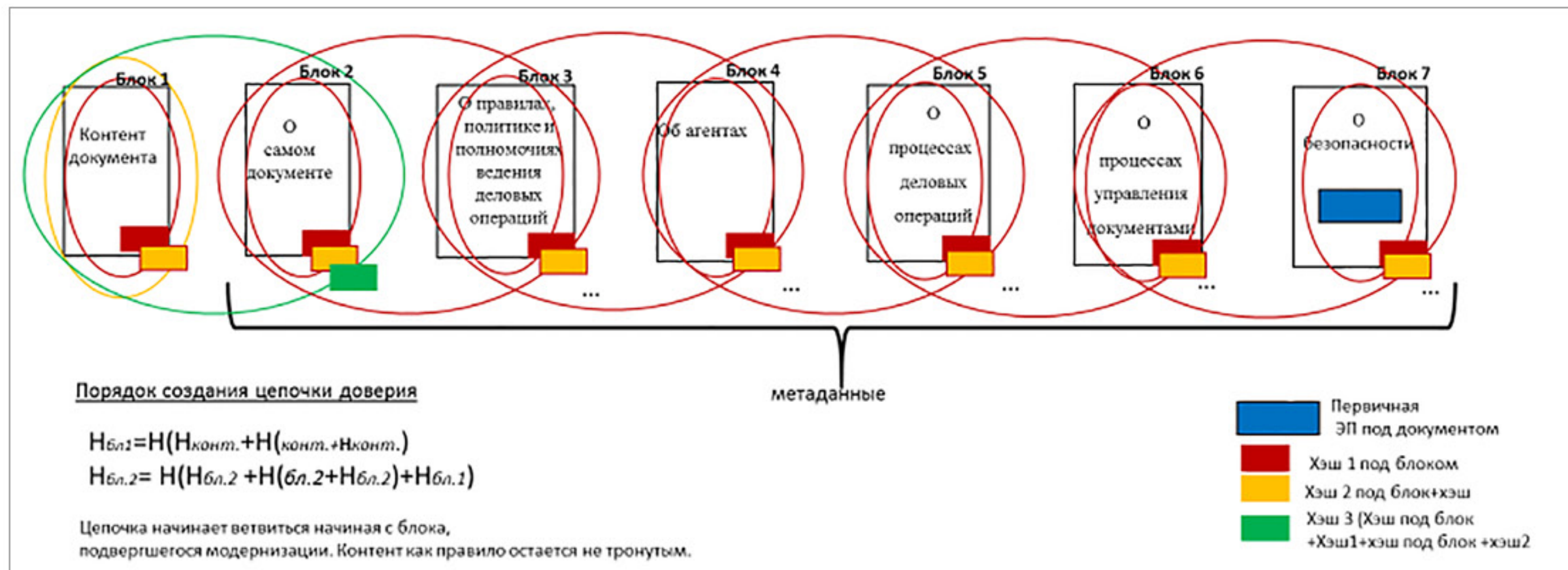


Рисунок 2. Цепочки доверия в единице архивного хранения

А ЕСЛИ БЛОКЧЕЙН?

Самой близкой аналогией такой процедуры является технология блокчейн. Применительно к задаче длительного хранения ЭД технология цепочек хэшчейн выглядит следующим образом (рис. 2).

На основе доверенных сервисов выстраивается следующая схема работы с архивным документом:

- ♦ Прием ЭД;
- ♦ Проверка первичной ЭП;
- ♦ Создание цепочки доверия для единицы хранения в составе ЭД (контент) + метаданные;
- ♦ Хранение с поддержанием сервисов доверия;
- ♦ Выдача документа по запросу с выполнением следующей процедуры:
 - Проверка сервисов доверия;
 - Проверка правил метаданных;
 - Простановка актуальной УКЭП хранилища;
 - Направление ЭД с УКЭП адресату.

В качестве надежного алгоритма получения хэш-функции используется ГОСТ Р 34.11–2012 на вычисление хэш-функции. Он надежен, принят ИСО. Особенностью хэш является то, что он практически не требует замены, в отличие от стандарта на ЭП, и может существовать весьма долго. Кроме того, вычисленное значение имеет всегда определенную и небольшую длину, что весьма удобно, так как не сильно увеличивает размер метаданных. Иных, лучших методов обеспечения доверия к сервисам хэш-функции в настоящее время нет.

Также важным преимуществом данной схемы является то, что внесение каких-либо изменений в состав данных без выполнения процедуры переформирования цепочки хэшчейн, начиная с той точки, в которой были внесены изменения, невозможны.

Управление всей процедурой, так же как проверка первичной ЭП на документе и простановка ЭП при выдаче документа по запросу, осуществляется специально уполномоченным лицом, отвечающим за архив электронных документов.

ЦЕНТРАЛИЗОВАННОЕ И ДЕЦЕНТРАЛИЗОВАННОЕ

Как уже отмечалось, в настоящее время существует две альтернативы организации системы долговременного хранения электронных документов: децентрализованное хранение ЭД в системе практически не связанных между собой локальных хранилищ, размещаемых в организациях или у граждан, и хранение документов в едином архиве, (может быть в нескольких крупных логически связанных централизованных архивах).

Оба этих варианта имеют свои достоинства и недостатки, однако опыт ведомств, работающих в смежных областях, например, в системе Банка России, системе пенсионного обеспечения и налоговой службе, ряде подразделений МВД (паспортная служба, ДПС), говорит о том, что выбор решения по построению архивов электронных до-

кументов сделан однозначно в пользу централизованной схемы.

ХРАНИТЬ В ОБЛАКЕ

В настоящее время весьма модным трендом является создание централизованных «облачных» хранилищ, в полной мере реализующих преимущества централизованного хранения.

Понятие «облачные вычисления» используются на практике достаточно часто, однако часто в него вкладывается несколько разный смысл, в связи с чем применительно к рассматриваемому вопросу следует уточнить, что имеется в виду.

Википедия дает следующее определение облачных вычислений: «Облачные вычисления (англ. cloud computing) — технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис».

Предоставление пользователю услуг как Интернет-сервиса является ключевым. Однако под Интернет-сервисом не следует понимать доступ к сервису, предоставляемому облачным хранилищем ЭД только через Интернет, он может осуществляться также и через обычную локальную сеть с использованием веб-технологий, выделенную сеть и т.д.

Общепринято в настоящее время использовать следующую классификацию моделей развёртывания «Облака»:

- а) частное облако (англ. private cloud);

- b) публичное облако (англ. public cloud);
- c) общественное облако (англ. community cloud);
- d) гибридное облако (англ. hybrid cloud).

ХОРОШАЯ МОДЕЛЬ

Представляется, что наиболее предпочтительным вариантом является общественное облако, SaaS + Workplace as a Service + Security as a Service. В такой модели потребителю предоставляется рабочее место как услуга, хранение и безопасность ЭД как сервис, а также возможность использования прикладного программного обеспечения провайдера, работающего в облачной инфраструктуре и доступного из различных клиентских устройств, состав которых определен провайдером облачного сервиса. Контроль и управление основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, операционных систем, систем хранения, систем безопасности и индивидуальных возможностей приложения (за исключением ограниченного набора пользовательских настроек конфигурации приложения) осуществляется облачным провайдером.

Такой подход предполагает использование конкретным сообществом (субъектами финансового рынка), имеющим общие задачи (например, миссии, тре-

бования безопасности, политики, и соответствия требованиям регулятора), общей инфраструктуры, находящейся в кооперативной (совместной) собственности, управлении и эксплуатации одной или более из организаций сообщества или третьей стороны (или какой-либо их комбинации). На рабочих местах сотрудников устанавливается все необходимое программное обеспечение, включая средства надежной аутентификации, электронной подписи, средства шифрования канала связи, необходимое для взаимодействия с облачным сервисом и, если необходимо, для работы персонала.

В ЧЕМ ДОСТОИНСТВА?

К достоинствам данной схемы следует отнести:

- ♦ Доступность — облачное хранилище доступно всем, из любой точки, где есть доступ к соответствующей сети.
- ♦ Экономия на закупке высокопроизводительных, дорогостоящих компьютеров для создания собственных систем хранения.
- ♦ Низкая стоимость хранения данных.
- ♦ Гибкость, неограниченность вычислительных ресурсов (память, процессор, диски) за счет использования систем виртуализации. Процесс масштабирования и администрирования «облаков» становится достаточно легкой задачей, так как «облако» самосто-

ятельно может предоставить вам ресурсы, которые вам необходимы, а вы платите только за фактическое их использование.

♦ Надежность. Надежность «облаков», особенно находящихся в специально оборудованных ЦОД, очень высокая, так как такие ЦОД имеют резервные источники питания, охрану, профессиональных работников, регулярное резервирование данных, высокую пропускную способность Интернет канала, высокую устойчивость к DDOS- и компьютерным атакам, предварительную фильтрацию трафика.

♦ Большие вычислительные мощности. Пользователь «облачной» системы может использовать все ее вычислительные способности, заплатив только за фактическое время использования.

♦ Высокая безопасность и надежность хранения данных. «Облако» само по себе является достаточно надежной системой, однако при реализации выбранной модели развертывания и предоставления услуг и сервисов решается главная задача — деятельность провайдера по выполнению требований безопасности находится под контролем регулятора. В этом случае облачное хранение становится целесообразным и оправданным.

ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

Данные в облачном хранилище хранит большое количество субъектов. В чем преимущество «облаков» для них:

- ♦ реализован безопасный доступ пользователей в систему;
- ♦ пользователю предоставлены возможности совершать все без исключения юридически значимые действия, в полной мере использовать возможности применения УКЭП;
- ♦ с пользователя сняты все обременения по хранению ЭД с обеспечением юридической силы;
- ♦ пользователю даны гарантии обеспечения безопасности его данных, сохранения юридической силы его ЭД;
- ♦ пользователь может убедиться в наличии таких гарантий;
- ♦ пользователь застрахован от чрезвычайных ситуаций и инцидентов;
- ♦ стоимость хранения документов в облаке невысока.

НИЗКАЯ СТОИМОСТЬ ХРАНЕНИЯ ДАННЫХ

Основные факторы, в принципе снизившие стоимость использования облаков, следующие:

- ♦ снижение расходов на обслуживание виртуальной инфраструктуры, вызванное развитием технологий виртуализации, за счет чего требуется меньший штат для обслуживания всей ИТ инфраструктуры предприятия;
- ♦ оплата фактического использования ресурсов. Пользователь облака платит за фактическое использование вычислительных мощностей облака, что позволяет ему эффективно распределять свои денежные средства;
- ♦ экономия на покупке лицензий к ПО;
- ♦ использование облака на правах аренды позволяет пользователям снизить расходы на закупку дорогостоящего оборудования, и сделать акцент на вложение денежных средств на наладку бизнес процессов предприятия, что в свою очередь позволяет легко начать бизнес;
- ♦ развитие аппаратной части вычислительных систем, в связи с чем снижается стоимость оборудования.

MirАссерт. ЧТОБЫ ПОКУПАТЬ С УДОВОЛЬСТВИЕМ!

ВВЕДЕНИЕ В РЕВОЛЮЦИЮ ПЛАТЕЖНЫХ СИСТЕМ



**Василий
ОКУЛЕССКИЙ**
эксперт
по информационной
безопасности



Евгений СОЛОВЬЕВ
эксперт Департамента
архитектуры и разработки
программного
обеспечения АО НСПК

Наш мир стал totally мобильным. Это произошло незаметно — через недорогие и дорогие смартфоны и планшеты, низкие тарифы на интернет, навигаторы (спасибо, Яндекс!), приложения сервисов такси, социальных сетей и мессенджеров, через сверхудобные мобильные приложения банков, электронные кошельки и т.д. и т.п. Мобильность захватила нас бесповоротно!

Мы сегодняшние — часть глобальной мобильности, элемент новой экосистемы потребления информации.

На фоне такой «всеобщей мобилизации», когда о нас знают, встречают по имени, предвосхищают наши желания и превращают наши мечты в реальность, на фоне всего этого нового и одновременно уже такого привычного мира инструментарий платежей по картам выглядит архаичным динозавром, который вот-вот вымрет после очередной «мобильной бомбардировки» инновационными решениями. К примеру, от электронных кошельков.

И слава богу, скажем мы, что дух мобильности проник в мир платежных систем! Потому что платежные системы, наконец, осознали, как необходимо догнать эту новую реальность, освоить ее, опередить конкурентов и — возглавить всеобщую мобилизацию!

Платежная система «Мир» — лидер этого движения, ее участники и поставщики программных решений активно готовятся к появлению в 2017 году нового поколения электронной коммерции под товарным знаком MirАссерт. В основе нового MirАссерт — спецификация EMV-Co 3-D Secure, в которую платежной системой «Мир» внесены необыкновенно полезные уточнения и конкретизированы некоторые особенности реализации функций компонентов информационного обмена.

ЧТО ЭТО ТАКОЕ?

Когда мы говорим про MirАссерт, то в первую очередь подразумеваем товарный знак или знак обслуживания, используемый платежной системой «Мир» для обозначения безопасной электронной коммерции (с надежной аутентификацией Держателя карты Эмитентом), когда Эмитент имеет возможность в процессе аутентификации Держателя карты принять на себя ответственность, в том числе и финансовую, за операцию Держателя карты (без обращения или с обращением к нему).

Чтобы подчеркнуть полное соответствие стандартов электронной коммерции ПС «Мир» спецификациям EMVCo, применяется следующее обозначение: MirАссерт (EMV 3-D Secure). Из него следует соответствие MirАссерт (электронной коммерции платежной системы «Мир» с надежной аутентификацией) спецификациям EMVCo.

Товарным знаком MirАссерт обозначаются:

- ◆ технологии безопасной электронной коммерции платежной системы «Мир»;
- ◆ продукты и/или сервисы безопасной электронной коммерции платежной системы «Мир» для участников и Держателей карт;
- ◆ все, что имеет отношение к технологиям безопасной электронной коммерции платежной системы «Мир», в частности, не ограничиваясь перечисленным: инфраструктура, фреймворк, протокол, его функциональные компоненты, его информационные потоки, отдельные сообщения внутри упомянутых информационных потоков, элементы данных внутри этих сообщений, алгоритмы, реализуемые в функциональных компонентах и прочее;
- ◆ стандарты/спецификации (документы) для безопасной электронной коммерции платежной системы «Мир»;
- ◆ страницы интернет-сайтов и загружаемых приложений, имеющих непосредственное от-

ношение к электронной коммерции платежной системы «Мир» с надежной аутентификацией Держателей карт;

♦ Любые материалы, направленные на внедрение, поддержание, популяризацию и иные шаги по использованию и продвижению безопасной электронной коммерции платежной системы «Мир» с надежной аутентификацией Держателей карт «Мир».

ОБЩИЕ ПОЛОЖЕНИЯ

MirAccept (EMV 3-D Secure) основан на так называемой трехдоменной модели.

В этой модели домен Эквайрера и домен Эмитента связаны между собой доменом совместимости (или доменом платежной системы) с целью обеспечения аутентификации Держателя карты «Мир» во время операции электронной коммерции на стадии проверки подлинности Держателя карты «Мир».

MirAccept (EMV 3-D Secure) поддерживает две возможности:

♦ **Платёжную аутентификацию.** Это такая проверка подлинности личности Держателя карты «Мир», которая выполняется во время операции оплаты товаров (работ, услуг) в сети Интернет (электронной коммерции).

♦ **Неплатёжную аутентификацию.** Проверка подлинности личности Держателя карты «Мир», не связанная с операциями оплаты товаров (работ, услуг) в сети Интернет (далее — операции электронной коммерции).

MirAccept (EMV 3-D Secure) должен быть доступен Держателю карты «Мир» через два клиентских интерфейса:

♦ **Клиентский интерфейс на основе загружаемого приложения ТСП.** Аутентификация Держателя карты «Мир» начинается на его клиентском устройстве (смартфоне, планшете, компьютере и т.п.) во время операции электронной коммерции, в котором такую процедуру берет на себя компонент 3DS Requestor App (загружаемое приложение ТСП или иное загружаемое приложение, предоставляемое сертифицированным и зарегистрированным Платёжной системой «Мир» агентом, например, оператором электронного бумажника).

♦ **Клиентский интерфейс на основе браузера.** Аутентификация Держателя карты начинается на веб-сайте, доступ к которому Держателю карты «Мир» предоставляет браузер на его клиентском устройстве. Например, при завершении операции электронной коммерции (на стадии чекаута), на веб-сайте, открытом в браузере клиентского устройства (смартфоне, планшете, компьютере и т.п.) Держателя карты «Мир».

КРАТКИЙ ЭКСКУРС

В этой части статьи перечислены субъекты информационного обмена, необходимые для реализации протокола MirAccept (EMV 3-D Secure). Описание разделено на следующие домены:

♦ Домен эквайрера (Acquirer Domain) операции MirAccept (EMV 3-D Secure) начинаются в Домене эквайрера;

♦ Домен платёжной системы (Interoperability domain) операции MirAccept (EMV 3-D Secure) маршрутизируются между доменом Эквайрера и доменом Эмитента;

♦ Домен Эмитента (Issuer Domain). Операции MirAccept (EMV 3-D Secure) подвергаются проверке подлинности (аутентификации) в домене Эмитента.

На рисунке 1 изображено взаимодействие трех доменов и компонентов каждого из них.

Поскольку реализация информационной среды 3DS Requestor Environment может варьироваться, изображение на рис. 1 не подразумевает какую-либо конкретную реализацию этих компонентов или порядка, в котором они взаимодействуют.

Например, в частности, компонент 3DS Client может напрямую общаться с компонентом 3DS Server или компонент 3DS Server и компонент 3DS Requestor могут быть объединены в один компонент.

Внимание! Пунктирными стрелками на рисунке 1 (и на всех остальных рисунках) изображены процессы, не являющиеся частью MirAccept (EMV 3-D Secure). 3DS Requestor также не является его частью. Они приведены для большей ясности.

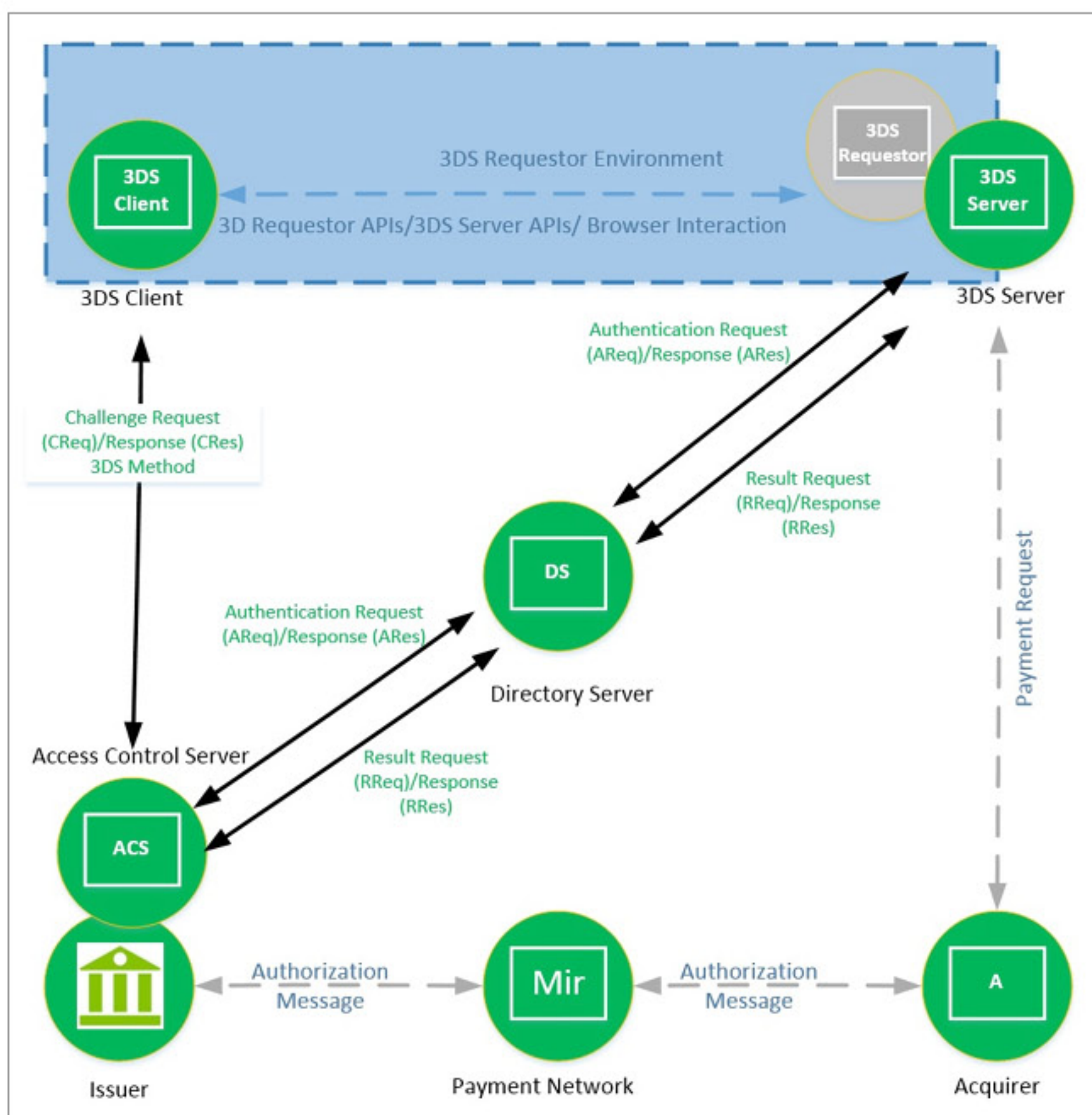


Рисунок 1. Домены и компоненты информационного обмена MirAccept (EMV 3-D Secure)

ДОМЕН ЭКВАЙРЕРА

Домен Эквайера состоит из следующих компонентов:

- ◆ Среда 3DS Requestor Environment:
 - ◆ 3DS Requestor,
 - ◆ 3DS Client,
 - ◆ 3DS Server;
- ◆ 3DS Integrator;
- ◆ Acquirer (для платёжной аутентификации).

ДОМЕН ПЛАТЕЖНОЙ СИСТЕМЫ (INTEROPERABILITY DOMAIN)

Interoperability domain состоит из следующих компонентов:

- ◆ Directory Server (DS);
- ◆ Directory Server Certificate Authority (DS CA);
- ◆ Система авторизации.

ДОМЕН ЭМИТЕНТА

Домен Эмитента состоит из следующих компонентов:

- ◆ Держатели карт «Мир»;
- ◆ Клиентское устройство (умные часы, смартфон, планшет, ноутбук, компьютер, умный телевизор и т.п.);
- ◆ Эмитент;
- ◆ Access Control Server (ACS).

КОМПОНЕНТЫ (СУБЪЕКТЫ ИНФОРМАЦИОННОГО ОБМЕНА) MIRACCEPT

3DS Requestor. 3DS Requestor — компонент, который инициирует сообщение AReq и который является каналом для данных MirAccept (EMV 3-D Secure), получаемых от клиентского устройства. Например, при платёжной аутентификации, 3DS Requestor обычно представляет из себя веб-сервер магазина для онлайн-покупок.

3DS Requestor связан с компонентом 3DS Client через компонент 3DS Requestor App либо через метод 3DS Method / Browser на клиентском устройстве. Компонент 3DS Requestor имеет соединение с компонентом 3DS Server или же полностью интегрирован с ним.

Операция MirAccept (EMV 3-D Secure) может быть выполнена:

- ◆ Через приложение (App-based) — компонент 3DS Requestor App интегрируется с компонентом 3DS SDK. 3DS SDK отображает пользовательский интерфейс (UI) для держателей карт.
- ◆ Через браузер (Browser-based) — компонент 3DS Requestor на основе браузера использует метод 3DS Method, чтобы собрать информацию о браузере / клиентском устройстве и предоставленную компонентом ACS страницу в формате HTML для отображения интер-

фейса Держателю в браузере, когда необходима Проверка (Challenge).

3DS Client. 3DS Client — это компонент, расположенный на клиентском устройстве, который инициирует операцию аутентификации MirAccept (EMV 3-D Secure). Например, в операции платёжной аутентификации компонент 3DS Client интегрирован с системой чек-аута интернет-магазина, являясь для клиента частью процесса интернет-покупки.

Компонент 3DS Client может быть реализован в двух вариантах:

- ◆ Через приложение (app-based). Компонент 3DS Client фактически является компонентом 3DS SDK, который интегрирован с компонентом 3DS Requestor App и обеспечивает, таким образом, взаимодействие с держателем карты «Мир». Компонент 3DS SDK (1) собирает необходимую для протокола MirAccept (EMV 3-D Secure) информацию клиентского устройства (device information), (2) поддерживает взаимодействие с компонентом Access Control Server (ACS) для аутентификации, и (3) защищает поток данных аутентификации держателя карты «Мир».

- ◆ Через браузер (browser-based). В этом случае компонент 3DS Client — это метод 3DS Method, который интегрирован с веб-сайтом компонента 3DS Requestor и вызывается в браузере на клиентском устройстве. Метод 3DS Method — это скриптовый вызов со стороны 3DS Integrator, который размещен на сайте, с которым держатель карты взаимодействует. Например, в платёжной аутентификации он является страницей чек-аута интернет-магазина. Назначение метода 3DS Method — получить дополнительную информацию из браузера, чтобы помочь принятию решения на основе анализа рисков.

3DS Server. 3DS Server — это компонент, который обеспечивает взаимодействие между средой 3DS Requestor Environment и компонентом Directory Server (DS). Компонент 3DS Server отвечает за:

- ◆ сбор необходимых данных для формирования сообщений протокола MirAccept (EMV 3-D Secure);
- ◆ аутентификацию компонента DS;
- ◆ валидацию компонента DS, компонента 3DS SDK и компонента 3DS Requestor;
- ◆ обеспечение того, что содержание сообщений будет защищено.

Для того, чтобы инициировать транзакцию платёжной аутентификации MirAccept (EMV 3-D Secure), компонент 3DS Server собирает необходимые элементы данных из любого или всех компонентов внутри 3DS Requestor Environment. Например, в операции платёжной



аутентификации информация о номере карты может быть введена держателем карточки в клиентском устройстве (смартфоне, планшете, ноутбуке, компьютере), или она может храниться в файле внутри 3DS Requestor Environment. Информация клиентского устройства (device information) захватывается компонентом 3DS Client и пересылается в компонент 3DS Server.

Вслед за платежной аутентификацией MirAccept (EMV 3-D Secure), в зависимости от конфигурации компонента 3DS Requestor, компонент 3DS Server может быть также соединен с Эквайнером и инициировать авторизационные запросы.

3DS Integrator (3DS Server и 3DS Client). 3DS Integrator — это логическая абстракция, роль которой — обеспечивать функциональный интерфейс между информационными потоками сообщений среды 3DS Requestor Environment и информационными потоками сообщений MirAccept (EMV 3-D Secure).

Роль 3DS Integrator (1) представляет из себя логический комплекс из компонента 3DS Server и компонента 3DS Client, и (2) интегрирует функциональность MirAccept (EMV 3-D Secure) с бизнес-функциональностью 3DS Requestor. 3DS Integrator имеет решающее значение для взаимодействия с компонентом DS и с компонентом ACS в рамках обмена аутентификационными сообщениями, а также выступает в качестве канала для результатов Проверки (Challenge), когда она выполняется.

3DS Integrator предоставляет одобренный платежной системой компонент 3DS SDK или метод 3DS Method для 3DS Requestor для интеграции в их 3DS Requestor App и/или в веб-сайт.

3DS Integrator отвечает за регистрацию ТСП (магазинов) в компоненте DS платежной системы «Мир» и, при необходимости, иных платежных систем.

После платежной аутентификации компонент 3DS Integrator может поддерживать на стороне Эквайнера возможность авторизации.

Эквайнер (для платежной авторизации). Эквайнер является финансовым учреждением, которое:

- ◆ Заключает договоры с ТСП (магазинами) о приеме к оплате карт «Мир» и о расчетах по таким операциям;
- ◆ Определяет, будет ли ТСП принимать участие в сервисе MirAccept (EMV 3-D Secure).

После платежной аутентификации MirAccept (EMV 3-D Secure) Эквайнер выполняет свою традиционную роль:

- принимает запросы на авторизацию от ТСП;
- ◆ направляет их в систему ПС «Мир»;
- ◆ предоставляет авторизационные ответы ТСП;
- ◆ выполняет расчеты с платежной системой «Мир» и с ТСП.

Домен платежной системы (Interoperability Domain). Interoperability domain состоит из следующих компонентов:

- ◆ Directory Server (DS);
- ◆ Directory Server Certificate Authority (DS CA);
- ◆ Система авторизации.

Directory Server. Directory Server (DS) — компонент, который выполняет ряд следующих функций:

- ◆ Аутентификация компонента 3DS Server и компонента ACS;
- ◆ Маршрутизация сообщений между компонентом 3DS Server и компонентом ACS;



- ◆ Валидация компонента 3DS Server, компонента 3DS SDK, и компонента 3DS Requestor;
- ◆ Определение конкретных правил обработки операций (например, в частности, логотипы, таймауты и другие правила);
- ◆ Хранение данных обо всех компонентах 3DS Server и обо всех компонентах ACS;
- ◆ Контроль версий для компонента ACS и метода 3DS Method URL.

Directory Server Certificate Authority. Компонент Directory Server Certificate Authority (DS-CA) формирует открытый ключ для компонента DS, для компонента 3DS SDK и формирует сертификаты Transport Layer Security (TLS) для использования компонентами MirAccept (EMV 3-D Secure). Компонент DS CA управляется платежной системой «Мир» и обслуживает компонент DS платежной системы «Мир».

Сертификаты включают в себя:

- ◆ сертификаты TLS клиента и сервера, используемые в обмене данными между компонентом 3DS Server и компонентом DS, а также между компонентом DS и компонентом ACS;
- ◆ сертификаты, используемые для подписи сообщений, передаваемых из компонента ACS в компонент 3DS SDK.

Авторизационная система ПС «Мир» (ОПКЦ). Авторизационная система ПС «Мир» (ОПКЦ) выполняет свою традиционную роль после платежной аутентификации, которая включает в себя следующее:

- ◆ Получение авторизационных запросов от Эквайрера;
- ◆ Маршрутизация авторизационных запросов Эмитенту;
- ◆ Предоставление авторизационных ответов от Эмитента Эквайреру;
- ◆ Выполнение клиринга и расчетов для Эмитентов и Эквайреров.

Домен Эмитента. Домен Эмитента состоит из следующих компонентов:

- ◆ Держатели карт «Мир»;
- ◆ Клиентское устройство (умные часы, смартфон, планшет, ноутбук, компьютер, умный телевизор и т.п.);
- ◆ Эмитент;
- ◆ Access Control Server (ACS).

Держатель карты «Мир». Держатель карты «Мир» предоставляет платежную информацию через клиентское устройство. В случае необходимости Проверки (Challenge) держателю карты «Мир» будет предложено предоставить до-

полнительную информацию для подтверждения подлинности (аутентификации).

Клиентское устройство. Клиентское устройство имеет возможность запуска приложения (компонента 3DS Requestor App) или показа веб-сайта в своём браузере, который будет использоваться для аутентификации MirAccept (EMV 3-D Secure), когда это требуется.

Компоненты MirAccept (EMV 3-D Secure) среды 3DS Requestor Environment на клиентском устройстве зависят от модели:

- ◆ App-based (на основе приложения) — приложение 3DS Requestor App, в которое встроен компонент 3DS SDK;

- ◆ Browser-based (на основе браузера) — браузер, использующий метод 3DS Method.

Эти компоненты имеют особую связь с компонентом 3DS Requestor и с компонентом 3DS Server.

Эмитент. Эмитент является финансовым учреждением, которое:

- ◆ имеет договорные отношения с держателем карты «Мир» (одной или нескольких);

- ◆ определяет диапазоны номеров карт «Мир», имеющих право на участие в программе безопасной электронной коммерции MirAccept (EMV 3-D Secure);

- ◆ предоставляет данные о диапазонах номеров карт компоненту Directory Server (DS), для добавления.

Access Control Server (ACS). Компонент ACS содержит правила аутентификации и контролируется эмитентом. Функции компонента ACS включают в себя:

- ◆ Проверка того, что данный номер карты имеет право на аутентификацию MirAccept (EMV 3-D Secure);

- ◆ Проверка того, что используемый тип клиентского устройства имеет право на аутентификацию MirAccept (EMV 3-D Secure);

- ◆ Аутентификация держателя карты «Мир» в конкретной операции.

В то время как перечисленные функции могут принадлежать к одному логическому компоненту ACS, их реализация может быть разделена по функциям и иным принципам (например, по диапазонам номеров карт) между несколькими физическими серверами.

СООБЩЕНИЯ MIRACCEPT

Этот раздел знакомит с сообщениями, определенными в протоколе MirAccept (EMV 3-D Secure).

Сообщение Аутентификационный Запрос (AReq). Сообщение Аутентификационный Запрос (AReq) является начальным сообщением в информационном потоке MirAccept (EMV 3-D Secure). Компонент 3DS Server формирует со-

общение AReq в момент, когда запрашивается аутентификация держателя карты «Мир». Сообщение может содержать (а) информацию о держателе карты «Мир», (б) платежную информацию, а также (в) информацию клиентского устройства (device information) по данной конкретной операции. Для каждой операции MirAccept (EMV 3-D Secure) предусмотрено только одно сообщение AReq.

Сообщение Аутентификационный Ответ (ARes). Сообщение Аутентификационный Ответ (ARes) является ответом компонента ACS Эмитента на сообщение AReq. Оно может указывать на то, что, либо (а) держатель карты был аутентифицирован, либо (б) требуется взаимодействие с держателем карты для завершения аутентификации — Проверка (Challenge). Для каждой операции предусмотрено только одно сообщение ARes.

Сообщение Проверочный (challenge) Запрос (CReq). Сообщение Проверочный (challenge) Запрос (CReq) дает старт взаимодействию с держателем карты в информационном потоке Проверки (Challenge) и может быть использовано для передачи результатов аутентификации держателя карты.

- ◆ App-based (на основе приложения) — сообщение CReq посылается компонентом 3DS SDK. Для завершения Проверки (Challenge) может потребоваться два и даже более сообщений CReq, чтобы обеспечить информационный обмен компонента ACS с держателем карты в попытке его аутентифицировать.

- ◆ Browser-based (на основе браузера) — сообщение CReq посылается компонентом 3DS Server. Для каждой Проверки (Challenge) предусмотрено только одно сообщение CReq.

Сообщение Проверочный (challenge) Ответ (CRes). Сообщение Проверочный (challenge) Ответ (CRes) является ответом компоненту ACS на CReq. Сообщение CRes может содержать результат аутентификации держателя карты или, в случае операции на основе приложения (App-based), содержать указание на то, что, для аутентификации держателя карты нужны дополнительные действия.

- ◆ App-based (на основе приложения) — Элементы данных сообщения CRes обеспечивают необходимые данные для компонента 3DS SDK, позволяющие создать и отобразить пользовательский интерфейс (UI) для Проверки (Challenge). Чтобы выполнить аутентификацию держателя карты, на одну операцию сообщений CRes может быть два или более.

- ◆ Browser-based (на основе браузера) — сообщение CRes содержит результат аутентификации и завершает Проверку (Challenge) держате-

ля карты. На одну операцию может быть только одно сообщение CRes.

Сообщение Результат-Запрос (RReq). Сообщение Результат-Запрос (RReq) передает результат аутентификации. Сообщение направляется компонентом ACS через компонент Directory Server (DS) для компонента 3DS Server. Для каждой операции предусмотрено только одно сообщение RReq. Сообщение RReq присутствует только в том случае, если при выполнении аутентификации держателя карты требуется выполнить Проверку (Challenge).

Сообщение Результат-Ответ (RRes). Сообщение Результат-Ответ (RRes) подтверждает получение сообщения RReq. Оно направляется компонентом 3DS Server через компонент DS для компонента ACS. Для каждой операции предусмотрено только одно сообщение RRes. Сообщение RRes присутствует только в том случае, если при выполнении аутентификации держателя карты требуется выполнить Проверку (Challenge).

Сообщение Подготовка-Запрос (PReq). Сообщение Подготовка-Запрос (PReq) направляется компонентом 3DS Server компоненту DS для (а) запроса информации о версиях, поддерживаемых доступными компонентами ACS, и, (б) если хоть один из них существует, то и свя-

занный 3DS Method URL. Сообщение Подготовка-Запрос (PReq) не является частью информационного потока аутентификации MirAccept (EMV 3-D Secure).

Сообщение Подготовка-Ответ (PRes). Сообщение Подготовка-Ответ (PRes) является ответом компонента DS на сообщение PReq. Компонент 3DS Server может использовать сообщение PRes для сохранения информации о версиях, поддерживаемых доступными компонентами ACS, и, если хоть один таковой существует, сохранять информацию о соответствующем 3DS Method URL. Сообщение Подготовка-Ответ (PRes) не является частью информационного потока аутентификации MirAccept (EMV 3-D Secure).

Сообщение об ошибке. Это сообщение (error message) используется для предоставления дополнительной информации об ошибке, возникшей в процессе обработки сообщений между компонентами 3DS Server, DS и ACS.

ИНФОРМАЦИОННЫЕ ПОТОКИ MIRACCEPT

В данном разделе статьи приводится обзор информационных потоков аутентификации, определенных в MirAccept (EMV 3-D Secure).

Информационный поток Frictionless Flow. Информационный поток Frictionless Flow начинается операцию MirAccept (EMV 3-D Secure) и состоит из сообщения AReq и из сообщения ARes.

Информационный поток Frictionless Flow не требует дальнейшего взаимодействия с держателем карты для успешной аутентификации и завершает процесс аутентификации MirAccept (EMV 3-D Secure).

Информационный поток Challenge Flow. В дополнение к сообщениям AReq и ARes, составляющим вместе информационный поток Frictionless Flow, информационный поток Challenge Flow состоит из сообщений CReq, CRes, RReq и RRes.

Если компонент ACS определяет, что требуется дальнейшее прямое взаимодействие с Держателем карты для завершения аутентификации, то информационный поток Frictionless flow переходит в информационный поток Challenge Flow. Например, Проверка (Challenge) может оказаться необходимой, если операция будет считаться высоко рискованной, то есть превышающей определенный порог, или требующей более надежного уровня аутентификации из-за требований законодательств определенных стран.

Компоненты 3DS Requestor решают, следует ли продолжить Проверку (Challenge) или следу-

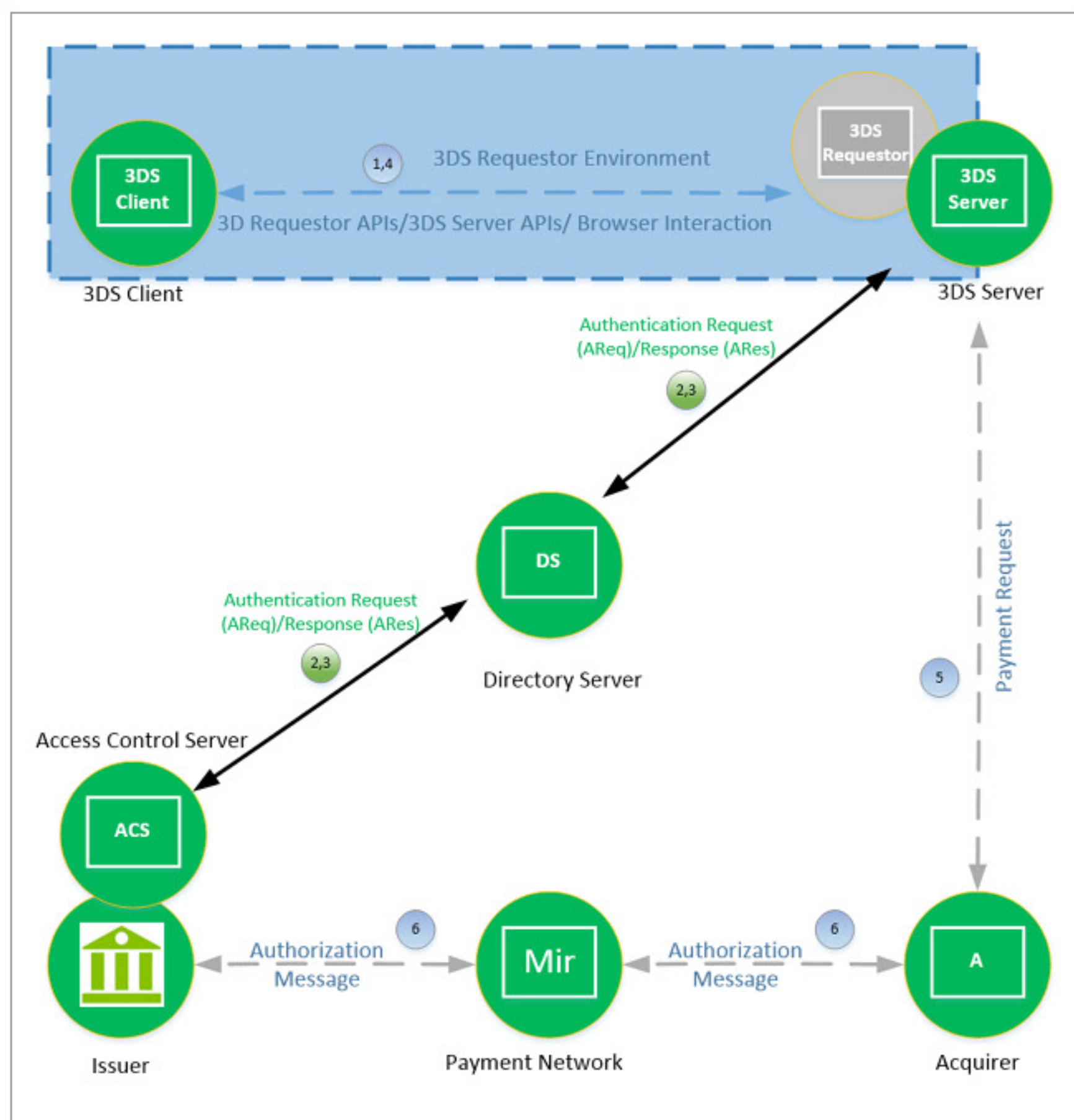


Рисунок 2. Frictionless Flow

ет прекратить процесс аутентификации MirAccept (EMV 3-D Secure).

Если проверка прекращается, то операция выходит из-под контроля MirAccept и продолжается как операция электронной коммерции с ответственностью на Эквайрере и магазине за ее финансовые и иные возможные последствия.

Если же проверка продолжается и выполняется успешно, то операция MirAccept, будучи успешно авторизованной, будет обеспечивать защиту Эквайреру и магазину.

ИНФОРМАЦИОННЫЙ ПОТОК FRICTIONLESS FLOW. ПОШАГОВОЕ ОПИСАНИЕ.

На рисунке 2 приведены шаги информационного потока.

Поток Frictionless Flow содержит следующие шаги:

Старт: держатель карты. Держатель карты «Мир» инициирует операцию на клиентском устройстве. Держатель карты «Мир» предоставляет информацию, необходимую для аутентификации (ее либо вводит держатель карты, либо она уже присутствует в файле в системе ТСП).

(1) 3DS Requestor Environment. Компонентами среды 3DS Requestor Environment собирается соответствующая необходимая MirAccept (EMV 3-D Secure) информация и предоставляется компоненту 3DS Server для включения в сообщение AReq.

Как предоставлена эта информация, и от какого компонента она поступила, зависит от следующего:

- ◆ Device Channel (канал) — App-based (на основе загружаемого приложения предприятия торговли/услуг) или Browser-based (на основе браузера в клиентском устройстве).

- ◆ Message Category (категория сообщения) — Payment (платежное) или Non-Payment (неплатежное).

- ◆ Реализации компонента 3DS Requestor.

(2) 3DS Server через DS к ACS. Используя информацию, предоставленную держателем карты «Мир» и данные, полученные в 3DS Requestor Environment, компонент 3DS Server создает и отправляет сообщение AReq компоненту DS, который затем направляет сообщение в соответствующий компонент ACS.

(3) ACS через DS к 3DS Server. В ответ на сообщение AReq компонент ACS возвращает сообщение ARes компоненту DS, который затем передает его инициирующему MirAccept (EMV 3-D Secure) операцию компоненту 3DS Server.

Перед возвращением ответа ARes компонент ACS оценивает данные, представленные в сообщении AReq. В информационном потоке Frictionless Flow компонент ACS определяет, что дополнительного взаимодействия с держателем карты не требуется, чтобы завершить аутентификацию.

(4) 3DS Requestor Environment. Компонент 3DS Server передает результат сообщения ARes компоненту 3DS Requestor Environment, который затем информирует держателя карты «Мир».

Компонент 3DS Requestor определяет, каким образом реализуется взаимодействие между этими компонентами.

Внимание! Обработка операции по стандарту MirAccept (EMV 3-D Secure) заканчивается на этом шаге. Для платежной авторизации должны быть выполнены последующие шаги:

(5) ТСП и его Эквайрер. ТСП направляет авторизационный запрос банку Эквайреру. ТСП, Эквайрер или Процессор может направить авторизационное сообщение в ОПКЦ ПС «Мир», если это необходимо.

(6) Авторизация. Эквайрер может обработать авторизацию, запросив об этом Эмитента и вернув после этого результат такой обработки в ТСП.

3DS REQUESTOR ENVIRONMENT НА ОСНОВЕ ПРИЛОЖЕНИЙ

Для модели, реализованной на основе приложений (App-based), информационный поток между компонентами 3DS SDK/3DS Requestor App и компонентами 3DS Server/3DS Requestor происходит с использованием API, которые доступны с компонентов 3DS Server/3DS Requestor.

Основные функциональные особенности для Шага 1 и Шага 4 являются такими, как определено в предыдущем разделе, со следующими пояснениями:

Старт. Держатель карты «Мир» и компонент 3DS Requestor App. Держатель карты «Мир» инициирует операцию с использованием компонента 3DS Requestor App на клиентском устройстве.

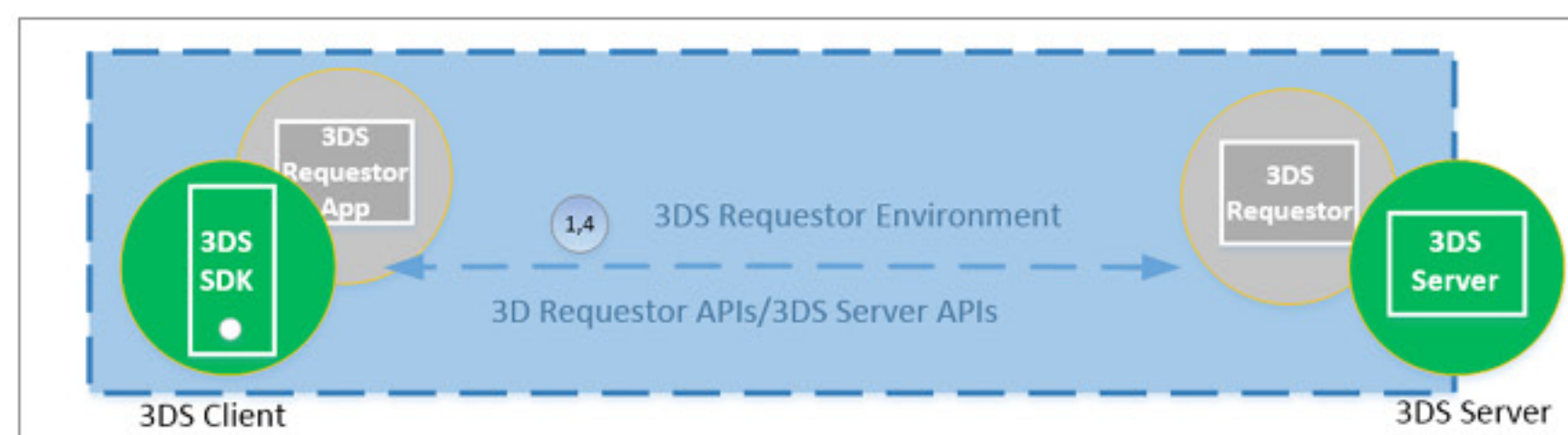


Рисунок 3. 3DS Requestor Environment-Frictionless Flow-реализация на основе приложений (App-based)

(1) **3DS SDK и 3DS Server.** Компонент 3DS SDK/3DS Requestor App связывается с компонентом 3DS Server/3DS Requestor. Чувствительная информация от клиентского устройства шифруется компонентом 3DS SDK перед отправкой в сообщении AReq компоненту DS.

(4) **3DS Server и 3DS SDK.** Компонент 3DS Server/3DS Requestor передает результат в сообщении ARes компоненту 3DS SDK/3DS Requestor App, который затем информирует держателя карты.

3DS REQUESTOR ENVIRONMENT НА ОСНОВЕ БРАУЗЕРА

Для модели, реализованной на основе браузера (browser-based), информационный обмен между клиентским устройством и компонентом 3DS Server/3DS Requestor использует стандартное браузерное TLS соединение. Рисунок 4 отображает среду 3DS Requestor Environment.

Функционально для шагов Шаг 1 и Шаг 4, описанных ранее, приводятся следующие пояснения:

Старт. Держатель карты. Держатель карты «Мир» инициирует операцию с помощью браузера, установленного на клиентское устройство, используя веб-сайт, который находится под управлением компонента 3DS Requestor.

(1.1) **3DS Requestor и 3DS Server.** Компонент 3DS Requestor взаимодействует с компонентом 3DS Server. Компонент 3DS Server определяет версию компонента ACS (ACS Version) и, если возможно (в случае присутствия), получает 3DS Method URL для запрошенного диапазона номеров карт «Мир» и передает эту информацию компоненту 3DS Requestor. Эти данные (ACS Version и 3DS Method URL) были получены ранее компонентом 3DS Server посредством сообщения PRes.

(1.2) **3DS Method на 3DS Requestor веб-странице чек-аута.** Страница чек-аута компонента 3DS Requestor загружает 3DS Method URL, если он присутствует, который позволяет компоненту ACS получить дополнительную браузерную информацию для принятия решения на основе анализа рисков.

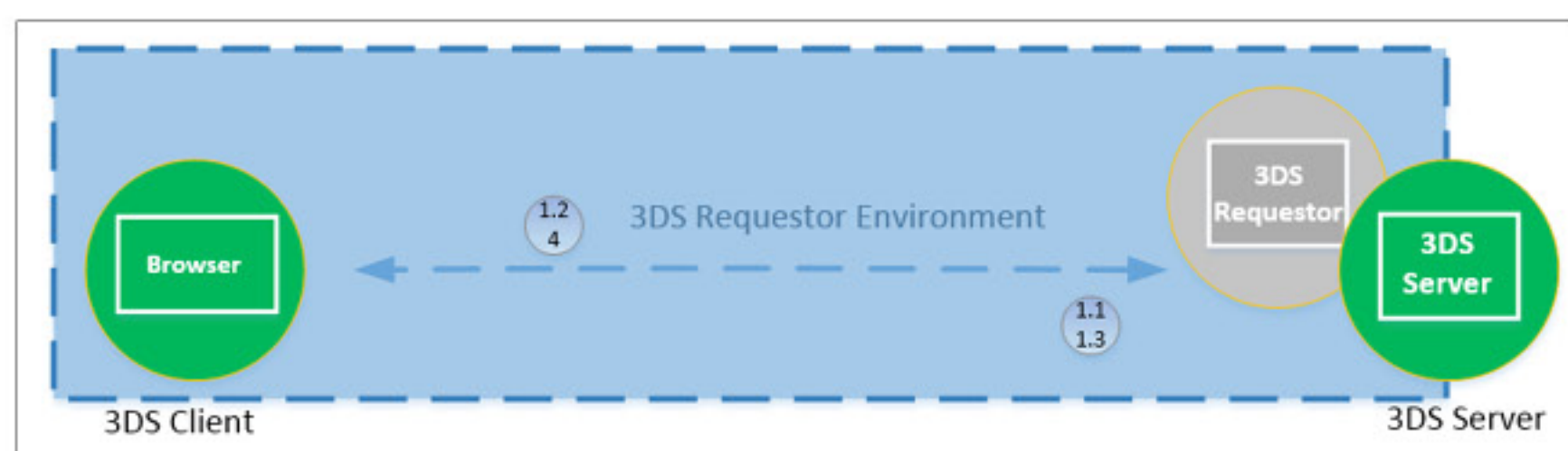


Рисунок 4. 3DS Requestor Environment-Frictionless Flow-реализация на основе браузера (browser-based)

(1.3) **3DS Requestor и 3DS Server.** Компонент 3DS Requestor обеспечивает передачу необходимой MirAccept (EMV 3-D Secure) информации, относящейся к операции, компоненту 3DS Server.

4. **3DS Server и 3DS Requestor.** Компонент 3DS Server передает результат сообщения ARes в компонент 3DS Requestor и завершает операцию. 3DS Integrator определяет, как реализовано взаимодействие между компонентами.

ИНФОРМАЦИОННЫЙ ПОТОК CHALLENGE FLOW. ПОШАГОВОЕ ОПИСАНИЕ

Рисунок 5 отображает шаги информационного потока Challenge Flow.

Поток стадии Challenge Flow содержит следующие шаги:

Старт. Держатель карты «Мир». Так же как и в случае Frictionless Flow.

(1.) **3DS Requestor Environment.** Так же как и в случае Frictionless Flow.

(2.) **от 3DS Server через DS к ACS.** Так же как и в случае Frictionless Flow.

(3.) **от ACS через DS на 3DS Server.** Так же как и в случае Frictionless Flow, за исключением сообщения ARes, которое указывает на то, что требуется дополнительное взаимодействие с держателем карты для завершения аутентификации.

(4.) **от 3DS Server к 3DS Requestor Environment.** Так же как и в случае Frictionless Flow, за исключением того, что требуется дополнительное взаимодействие с держателем карты для завершения аутентификации.

(5.) **от 3DS Client к ACS.** Компонент 3DS Client инициирует сообщение CReq используя информацию, которая была получена в сообщении ARes. Способ, при помощи которого это происходит, зависит от модели:

◆ Модель, ориентированная на приложение (app-based). Сообщение CReq формируется компонентом 3DS SDK и перенаправляется методом post по адресу ACS URL, полученному в сообщении ARes.

◆ Модель, ориентированная на браузер (browser-based). Сообщение CReq формируется компонентом 3DS Server и методом post через браузер держателя карты перенаправляется компонентом 3DS Requestor по адресу ACS URL, полученному в сообщении ARes.

(6.) **от ACS к 3DS Client** — компонент ACS принимает сообщение CReq и взаимодействует с компонентом 3DS Client, чтобы поддержать интерфейс с держателем карты. Способ, при помощи которого это происходит, зависит от модели:

♦ **Модель, ориентированная на приложение (app-based).** Компонент ACS использует пары сообщений CReq и CRes для выполнения Проверки (Challenge). В ответ на полученное сообщение CReq компонент ACS формирует сообщение CRes, которое запрашивает держателя карты ввести данные для аутентификации, и направляется в компонент 3DS SDK.

♦ **Модель, ориентированная на браузер (browser-based).** Компонент ACS отправляет пользовательский интерфейс для аутентификации держателя карты в браузер его клиентского устройства. Держатель карты «Мир» вводит данные для аутентификации через браузер, которые должны быть проверены компонентом ACS. В ответ на полученное сообщение CReq компонент ACS формирует сообщение CRes и отправляет компоненту 3DS Server, чтобы сообщить результат аутентификации.

Внимание! Для модели app-based шаги 5 и 6, описанные выше, будут повторяться до тех пор, пока в компоненте ACS не появится определенное решение в отношении результатов аутентификации.

(7.) **от ACS через DS к 3DS Server.** Компонент ACS отправляет сообщение RReq компоненту DS, которое может включать AV (Authentication Value), а компонент DS, в свою очередь, затем отправляет это сообщение соответствующему компоненту 3DS Server, используя адрес 3DS Server URL, полученный в сообщении AReq.

(8.) **от 3DS Server через DS к ACS.** Компонент 3DS Server получает сообщение RReq и отвечает на него сообщением RRes компоненту DS, который затем направляет это сообщение в соответствующий компонент ACS.

Примечание: MirАссерт (3-D Secure 2.0) обработка заканчивается здесь. Для оплаты товара, должны быть выполнены последующие шаги.

(9.) **ТСП и Эквайер.** Так же как и в случае Frictionless Flow.

(10.) **Авторизация.** Так же как и в случае Frictionless Flow.

ЗАКЛЮЧЕНИЕ

Надеемся, что авторам удалось познакомить читателей с основами и базовыми идеями MirАссерт (EMV 3-D Secure), дать стартовые знания для самостоятельного глубокого освоения этого предмета.

Пожалуйста, обращайтесь за подробностями к документам на сайте EMVCo по теме EMV 3-D Secure (<http://www.emvco.com/specifications.aspx?id=299>)

- ♦ Protocol and Core Functions Specification
- ♦ SDK Specification

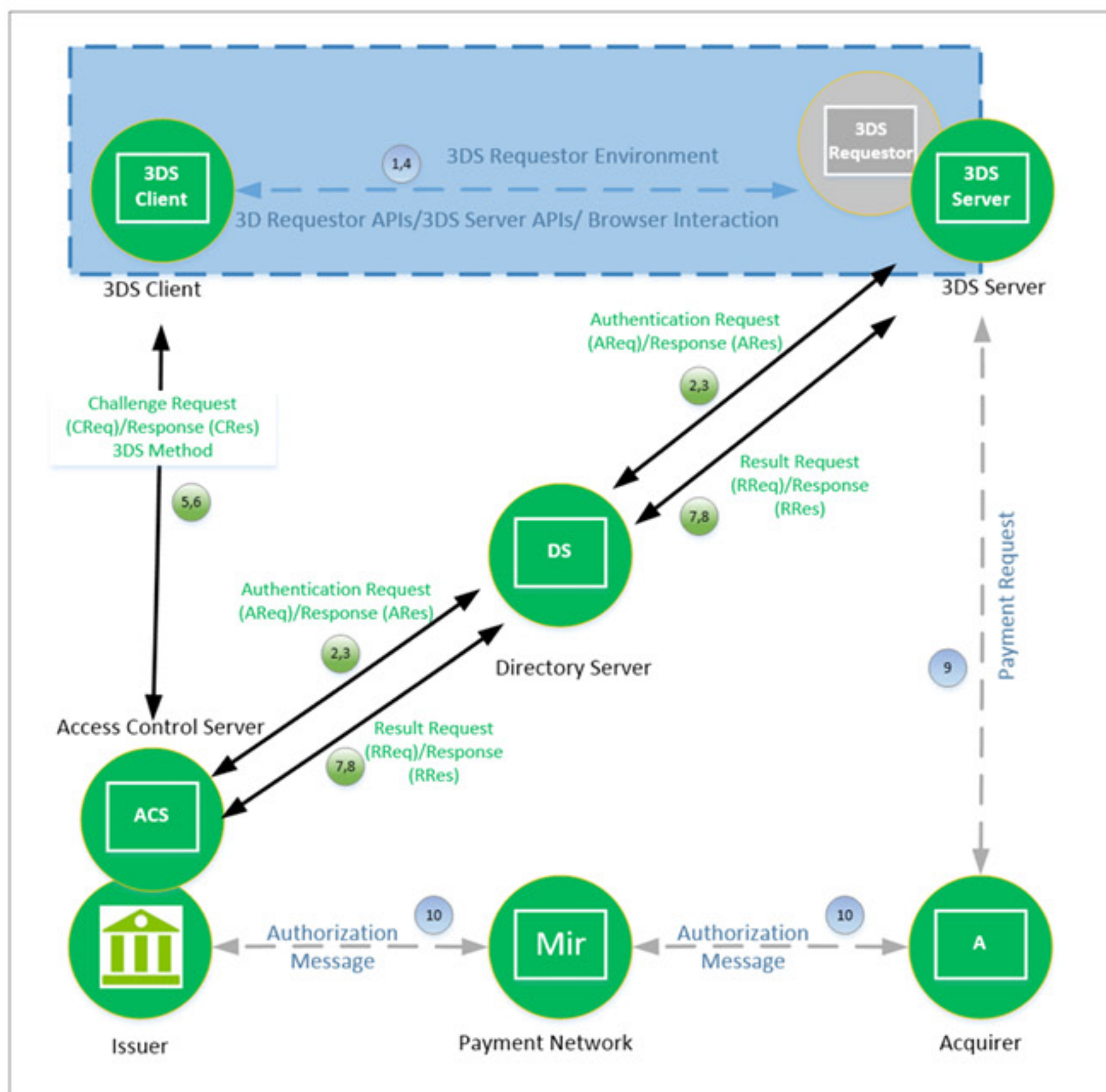


Рисунок 5. Информационный поток Challenge Flow

- ♦ SDK — Device Information
- ♦ SDK Technical Guide

Именно эти документы и были использованы автором для подготовки данного материала.

Уже очень скоро обновленный MirАссерт станет частью нашей повседневной жизни. Мы с вами в роли держателей карт будем пользоваться им для оплаты товаров и услуг в интернете, для денежных переводов с карты «Мир» и на карту «Мир», для управления содержанием электронных бумажников.

Это будет удобно, просто и безопасно. Гораздо лучше, чем это было раньше.

Заинтересованность в широком применении MirАссерт (EMV 3-D Secure) есть и у банков — участников платежной системы «Мир» и у предприятий торговли и услуг.

Именно поэтому всем участникам процесса важно понимать, как устроен MirАссерт, какие преимущества он несет, какие возможности он открывает, чтобы его применение приносило удовольствие и пользу держателям карт «Мир», предприятиям торговли/услуг и участникам платежной системы.

MirАссерт — чтобы покупать с удовольствием!

Использованы изображения с сайта www.mironline.ru



Евгений ЦАРЕВ
эксперт RTM Group

МНОГОЛИКАЯ ЭКСПЕРТИЗА

ТЕКУЩАЯ ПРАКТИКА СУДЕБНЫХ ДЕЛ ПО
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Когда речь заходит о судебных делах по информационной безопасности, необходимо сделать оговорку, что это не самостоятельные дела, а дела, в которых имеются существенные обстоятельства по тематике ИБ. Причем, на первый взгляд, такие дела не связаны с технологиями. К ним могут относиться трудовые споры, когда компания, например, увольняет сотрудника по статье, и в качестве обоснования своего решения использует записи систем видеонаблюдения, записи из журналов внутренних систем автоматизации и так далее. Таким образом компания пытается доказать, например, что сотрудник нарушил какие-то требования внутреннего распорядка, разгласил защищаемую информацию и нанес компании существенный ущерб.

ГРУППЫ СПОРОВ

Налоговые споры. В настоящий момент Федеральная налоговая служба очень часто использует цифровые доказательства в обоснование своей позиции в случае начисления недоимок по налогам и другим платежам.

УРОВЕНЬ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ НА ПРЕДПРИЯТИЯХ В НАСТОЯЩИЙ МОМЕНТ ЧРЕЗВЫЧАЙНО ВЫСОК, ОДНАКО, КОГДА ДЕЛО ДОХОДИТ ДО СПОРА, СТОРОНАМ ПО ДЕЛУ НЕОБХОДИМО ДОКАЗЫВАТЬ ДЕЙСТВИЕ ИЛИ БЕЗДЕЙСТВИЕ ТОГО ИЛИ ИНОГО СОТРУДНИКА

Споры, касающиеся банкротства того или иного предприятия. Здесь технических вариантов может быть очень много. Например, бывший генеральный директор не передал ключи электронной подписи, либо передал их с нарушениями, либо же параллельно после введения конкурсного производства распорядился деньгами на счете организации. Чтобы доказать это, необходимо привлечение технических специалистов, которые подтвердят или опровергнут этот факт.

Отдельная крупная группа — споры по качеству товаров или оказанных услуг. Когда одна организация поставляет другой технически сложный товар — программный продукт или компьютерное оборудование, и, соответственно, возникает спор по качеству, то есть оборудование работает «неправильно», не в соответствии с тем техническим заданием или проектом, который был определен изначально.

То же самое касается услуг. Тут вариантов еще больше. Наиболее популярный из них — это договоры подряда на разработку программного продукта. Нужно сказать, что при спорах, касающихся разработки того или иного

программного продукта, практически всегда привлекается экспертное учреждение, так как необходимо устанавливать и подтверждать объем разработанного программного продукта, время окончания разработки и так далее. Также к договорам подряда можно отнести договоры на проектирование тех или иных сложных технических систем, в том числе систем по информационной безопасности, дальнейшее внедрение по результатам проектирования и, возможно, предварительный или финальный аудит.

ПОПУЛЯРНЫЕ ЭКСПЕРТИЗЫ

В рамках работы в RTM Group можно выделить несколько вариантов наиболее популярных судебных и досудебных экспертиз по тематике ИТ и ИБ.

Первый вариант — это экспертиза существующей договорной работы с контрагентами в части обеспечения информационной безопасности и защиты информации. Что имеется в виду? Нередки случаи, когда хозяйствующие субъекты оказывают друг другу услуги и не желают, например, разглашать какие-то сведения касательно содержания работ и, может быть, даже самого факта заключения договора. Соответственно, чтобы предотвратить инциденты, необходимо тщательно прорабатывать договоры со своими контрагентами. Включать туда соответствующие разделы по неразглашению, разделы по защите информации, персональных данных и так далее.

Следующий вариант — экспертиза трудовых договоров по вопросам информационной безопасности. Примерно то же самое, что и предыдущий вариант, но он касается непосредственно



сотрудников, включая в том числе различные соглашения о неразглашении информации.

Очень популярный вариант — это экспертиза действий сотрудников в IT-системах. Не секрет, что уровень автоматизации бизнес-процессов на предприятиях в настоящий момент чрезвычайно высок, однако, когда дело доходит до спора, сторонам по делу необходимо доказывать действие или бездействие того или иного сотрудника.

Например, такой живописный случай. Сотрудник обладал значительными правами в ERP-системе и в определенный момент, при размещении крупного заказа, поставил отметку об оплате. Следствием этого стал факт отгрузки продукции, потому что продукция по системе числилась как оплаченная. В результате — хищение в особо крупном размере. Соответственно, для выяснения обстоятельств необходимо привлечение экспертов и проведение соответствующих процедур, которые могут проводиться в досудебном либо судебном порядке.

ЭКСПЕРТИЗЫ-ДВУХДНЕВКИ

Часто забываемый, но очень важный вариант экспертиз — это проведение предварительного расследования инцидентов. Мы их называем «экспертизы-двухдневки», они необходимы на самом раннем этапе, когда факт инцидента только установлен или имеются обоснованные подозрения, что инцидент произошел. «Двухдневки» необходимы для того, чтобы в дальнейшем цифровые доказательства не были оспорены в потенциальном судебном процессе.

В рамках «двухдневки» проводится предварительное расследование инцидента с целью подтверждения неизменности тех или иных данных. Всем известно, что большинство информационных систем делает записи в логах и журналах в изменяемом виде. То есть, чисто технически, данные журналов можно подделать. Чтобы в дальнейшем у суда не возникло сомнений в том, что сторона по делу, в нашем случае компания, внесла какие-то изменения, кото-

рые для нее были выгодны, необходимо проведение «экспертизы-двухдневки», которая подтвердит факт неизменности на самом раннем этапе расследования.

ПРИВЕТ ИЗ АФРИКИ!

По-своему экзотический вариант — это экспертиза телефонных соединений и вообще безопасности линии связи. В настоящий момент имеют место факты мошенничества, так называемого фрода, в телеком-сетях, когда организациям поступают счета за междугородные или международные телефонные соединения, при этом они этих телефонных переговоров не вели. Как правило, телефонные соединения происходят со странами Африки. В Европе такого рода фрод встречается даже чаще, чем в России.

ПРО ПО И СОБЫТИЯ

Следующий вариант — это экспертиза договоров на разработку или модернизацию программного обеспечения. Имеется в виду экспертиза именно

УСТАНАВЛИВАЕТСЯ, ЧТО БЫЛ ОБЯЗАН ДЕЛАТЬ БАНК, ЧТО ОБЯЗАН БЫЛ ДЕЛАТЬ КЛИЕНТ, КАКИЕ ТРЕБОВАНИЯ ЦЕНТРАЛЬНОГО БАНКА БЫЛИ ВЫПОЛНЕННЫ ИЛИ НЕ ВЫПОЛНЕННЫ И ТАК ДАЛЕЕ. ЭТО НАИБОЛЕЕ ПОПУЛЯРНАЯ ГРУППА ЭКСПЕРТИЗ

договорной работы, либо экспертиза в случае возникновения какого-то спора. Как мы уже говорили раньше — при разработке программного обеспечения возникает много нюансов, которые иногда не находят отражения в техническом задании или договоре, либо находят свое отражение, но в ходе работ выясняется, что выполнить те или иные требования либо невозможно либо слишком дорого. В этом случае, если дело доходит до судебного разбирательства, необходимо проведение соответствующей экспертизы с целью подтвердить или опровергнуть факт полного или частичного выполнения работ.

Интересный вариант — экспертиза событий в информационных системах организации. Тут имеются в виду не только действия сотрудников в этих информационных системах, но и действия внешних злоумышленников, которые каким-то образом получили доступ к внутренним IT-системам. Это чрезвычайно важно, так как в практике уже были случаи, когда после взлома компьютера бухгалтера и хищения денежных средств компании правоохранительные органы возбуждали уголовные дела на руководство компании в связи с подозрением в умышленном выводе денег на счета обналичных контор. Соответственно, точно так же собираются цифровые доказательства, которые в дальнейшем можно использовать и в уголовном процессе в рамках следственных действий и в судах общей юрисдикции или в арбитражных судах.

РЕГУЛЯТОРЫ И ЗАКОНЫ

Важный вариант — экспертиза соответствия обеспечения информационной безопасности требованиям российских

регуляторов. В России много регуляторов по вопросам информационной безопасности. Это и Федеральная служба по техническому экспортному контролю РФ, и Федеральная служба безопасности РФ, и Роскомнадзор, а в рамках банковской деятельности еще и Банк России. Все они выставляют свои официальные требования, и экспертиза может показать факт выполнения или невыполнения этих регуляторных требований.

Похожий вариант — экспертиза соответствия деятельности требованиям законодательства в области информационной безопасности в целом. То есть требования в России существуют не только на уровне регуляторов, но и на уровне законов и подзаконных актов. Соответственно, данная экспертиза помогает установить факт соответствия или несоответствия деятельности вопросам информационной безопасности в целом.

ИНЦИДЕНТЫ ДБО

Очень популярный вариант — экспертиза инцидентов в системах дистанционного банковского обслуживания. В первую очередь в рамках нашей компании мы занимаемся нормативными экспертизами по данным вопросам. То есть в случае хищения денежных средств со счетов клиентов единственным реальным способом получить возмещение ущерба является судебный процесс с банком. В такого рода процессах проводится и компьютерно-техническая экспертиза и нормативная экспертиза. В рамках нормативной экспертизы устанавливаются значимые детали договора между банком и клиентом по информационной безопасности. Устанавливается, что

был обязан делать банк, что обязан был делать клиент, какие требования Центрального банка были выполнены или не выполнены и так далее. Это наиболее популярная группа экспертиз.

НОВЫЕ ВАРИАНТЫ

Сравнительно новый вариант — экспертиза инвестиционного проекта, когда принимается решение об инвестициях в тот или иной технический проект, например, по разработке какого-то IT-сервиса. В таких случаях необходимо учитывать регулятивные вопросы по информационной безопасности в РФ, например, вопросы, связанные с криптографией. Такого рода экспертизы помогают инвестору понять, как обстоят дела по информационной безопасности в проекте и каковы его перспективы. Были случаи, когда отсутствие такой экспертизы приводило к банкротству организации, которая привлекла инвестиции только по той причине, что использовать решение оказывалось невозможным на территории РФ. Особую значимость данные экспертизы приобрели в связи с бумом ICO (Initial Coin Offering) — привлечением криптовалют в качестве инвестиций.

Другой вариант, стремительно набирающий популярность — это экспертиза в случае возникновения споров по закупкам. В данном случае происходит анализ соответствия конкурсной заявки требованиям законодательства в части защиты информации. Например, когда появляется объявление о закупках и там прописаны требования по защите информации, которые избыточны, неприменимы или осознанно искажены. Ни для суда, ни для Федеральной антимонопольной службы такие технические нюансы неочевидны и потому не рассматривались. И в практике бывали случаи, когда дополнительные требования по защите информации оказывались необоснованными, и торги отменялись. А иногда наоборот — более чем обоснованными. Соответственно, споры по закупкам — это отдельный вариант экспертиз.

(Окончание в следующем номере)

ЖИВАЯ ВОДА ДЛЯ SOC



Александр БОДРИК
заместитель
генерального
директора ANGARA
Professional Assistance



Евгений СОКОЛОВ
архитектор MSSP
ANGARA Professional
Assistance

КАК НЕ ДОПУСТИТЬ ЗОМБИ-АПОКАЛИПСИС В СФЕРЕ ИБ

Набравшая силу волна популярности SOC обнаруживает целый ряд зомби-SOC, которые существуют только формально. Несмотря на кипы процессных документов, полные наборы дорогостоящих технологий (SIEM, IDS, Service Desk) и вроде бы компетентных специалистов, компании с многомиллиардными оборотами годами безуспешно пытаются построить результативный, интересующийся всем новым, по-настоящему живой SOC.

Создавая для топ-5 российского MSSP свой SOC (естественно, итеративным путем, не минуя проб и ошибок), нам удалось найти практические рецепты — «живую воду», позволяющую возродить старый SIEM-ориентированный SOC и выстроить эффективную, гибкую, развивающуюся SOC-организацию.

ВИДЫ «ЖИВОЙ ВОДЫ»

Security Baseline. Перед началом реального мониторинга необходимо навести базовый порядок — разработать и утвердить политику ИБ, в частности базовый набор требований к ИТ-инфраструктуре (контрольной среде, в которой работают безопасники, ИТ-и бизнес-пользователи).

По факту это небольшой набор основных требований, предъявляемых к защищаемым объектам. Например, для хоста это могут быть: наличие антивируса, наличие Host IDS, настройка отправки логов в SOC, установка последних патчей, отсутствие учетных

записей пользователей без паролей или с паролями «по умолчанию».

Отсутствие таких базовых мер позволяет взламывать хосты в сети практически мгновенно. Так в одном из тестов на проникновение взлом непропатченного хоста занял 15 минут, а уже через 20 минут доменный контроллер был захвачен. Хотя до этого пентестеры молили — пустите в сеть, отключите Port Security и т.д.

А уж если хост доступен из Интернета, необходимо понимать, что, помимо вашего SOC, существуют еще десятки тысяч чужих систем (ботов), которые постоянно осуществляют мониторинг сети в надежде чем-нибудь поживиться. Боты реализуют простые, но эффективные сценарии поиска объектов атаки. Какой бы скромной и незаметной ни была ваша компания, за сутки к ее интернет-ресурсу обратятся два-три десятка ботов. Информация об обнаруженной уязвимости будет направлена хозяевам бота, после чего последует очень быстрая, хорошо автоматизированная атака по заранее подготовленному для найденной уязвимости сценарию.

Операторы SOC должны иметь под рукой Security Baseline предприятия, а также инструменты для его оперативной проверки. SOC должен отслеживать события изменения конфигурации наблюдаемой среды, в частности появление новых хостов, и немедленно выяснять, не нарушен ли Security Baseline. Это жизненно необходимо, так как ошибки в действиях ИТ-персонала мо-

гут привести к тому, что под огонь попадет незащищенная критичная для бизнеса система предприятия.

Базовые контроли. Основная (но не единственная) задача SOC — обнаружить факт того, что имеющиеся на предприятии средства защиты не работают. SOC может это обнаружить, анализируя данные, получаемые от специальных технических и программных устройств, которые далее мы будем называть «контролями». Без минимального набора контролей шансов найти сколько-нибудь профессионального злоумышленника просто нет — если он будет понимать, что есть системы защиты, то, например, вместо хищения данных он оставит в сети шифровальщика и уйдет из нее в надежде получить свой выкуп.

Существуют 6 базовых контролей без которых никакой эффективности SOC не будет:

♦ **Host IDS** умеет обнаруживать признаки атаки на хостах, такие как изменение системных файлов, создание новых учетных записей или изменение членства в группах безопасности, открытие новых портов и т.п. Желательно иметь Host IDS на всех без исключения компьютерах в сети, что не всегда возможно (например, в схеме с использованием BYOD). Основная рекомендация следующая: если вы можете установить Host IDS на компьютер — сделайте это.

♦ **Network IDS** умеет «просматривать» сетевой трафик и находить в нем признаки атак, например, работу се-

тевого сканера или попытку использовать эксплойт (программу для эксплуатации известной уязвимости в системе). Желательно направить на Network IDS весь трафик вашей сети, а не только трафик сегментов, которые вы считаете критически важными. Маловероятно, что атака начнется внутри критически важного сегмента, обычно до него не просто добраться. Лучше иметь возможность обнаружить атаку на ранней стадии. Коммерческие IDS могут оказаться слишком дороги для «неважных сегментов», в этом случае можно использовать продукты Open Source.

♦ **Антивирус.** Если антивирус что-то обнаружил на хосте, то как оно туда попало? Значит средства защиты «на периметре» не сработали. Кроме того, некоторые антивирусы содержат Host IDS в качестве одного из своих модулей.

♦ **Почтовый фильтр** умеет обнаруживать исполняемый код во вложенных файлах и задерживать такие письма в карантине. Задерживать надо все, что может исполняться, не следует полагаться на такие вещи, как почтовый антивирус. Вот практическая статистика по одной из компаний: почти 100% задержанных писем действительно содержали трояны или загрузчики троянов, менее 10% из этих писем детектировались популярными антивирусами, как содержащие вредоносный код. Почему так? Прежде чем послать трояна по почте, любой злоумышленник сначала проанализирует его на одном из ресурсов, осуществляющих анализ подозрительных файлов и ссылок (например, Virustotal), чтобы убедиться в том, что файл проходит сигнатурный анализ всех известных антивирусов. Задержка в карантине нужна для того, чтобы ваш SOC смог сначала выполнить исполняемый код в так называемой «песочнице» и убедиться в том, что он безопасен.

♦ **Next Generation** или **UTM Firewall**. Для простоты будем считать, что

это разные названия одного и того же — межсетевого экрана. Что мы от него хотим? Он должен иметь встроенную IPS, обновляемую базу категорий известных сайтов, средства «разрыва» SSL-соединений. Мы хотим разрывать зашифрованные соединения SSL и, с помощью IPS, анализировать, нет ли внутри вредоносных объектов. При этом мы не хотим разрывать все соединения, но только те, которые устанавливаются с неизвестными сайтами категории Unrated.

♦ **Сбор системных журналов:** отовсюду, со всех компьютеров, сетевых коммутаторов, маршрутизаторов, веб-серверов, серверов баз данных. Наш SOC должен уметь принимать и хранить огромные объемы данных и, кроме того, выполнять в них очень быстрый поиск и агрегировать данные по различным параметрам. Больше всего «следов атаки» мы можем найти именно здесь, главное — знать, что искать.

МОНИТОРИНГ

Мониторинг традиционно является основным процессом SOC. Операторы SOC непрерывно пытаются увидеть что-то, что может быть квалифицировано как нарушение безопасного состояния системы: признаки намеренных атак, ошибки персонала, сбои в работе оборудования. В этом им помогают «контроли» и Security Baseline. Интересно, что у широкой общественности сложилось мнение, что SOC — это, прежде всего, SIEM. Однако это — заблуждение. Заблуждение, возникшее благодаря многолетним усилиям продавцов SIEM.

SOC в первую очередь — это люди. А SIEM — это всего лишь средство автоматизации труда, позволяющее сократить трудозатраты персонала SOC (и то — в развитом SOC SIEM составляет до 10% в технологическом стеке).

Главный ресурс — опыт, знания и компетенции. Главная ценность SOC — его команда. И эта команда должна постоянно учиться — учиться выделять признаки атак из всей массы анализируемых событий. Это является основой концепции RedTeam, о которой мы поговорим далее.

Непрерывное противоборство и совершенствование. Но есть и еще кое-что. Даже самая обученная команда не должна «спать на боевом дежурстве». В этом нам могут помочь те самые десятки тысяч ботов, которые непрерывно работают в Интернете. Их роботизированные атаки на нашу инфраструктуру бессмысленны и неопасны, если, конечно, у нас все в порядке с Security Baseline. Но SOC должен фиксировать факты атак, пусть и не открывая инцидент.

Пример из армейской жизни. Фраза «This is the CENPAC command center with the communication flash test call» знакома многим, кто служил в военной разведке — это всего лишь проверка связи типа «молния» у бывшего вероятного противника. Но боец на посту должен ее зафиксировать. Ваша проверка — это и наша проверка. А еще за проверкой связи может последовать что-то более важное, поэтому особо упорные роботизированные атаки тоже следует брать на заметку: возможно, это прелюдия, и следует ждать чего-то еще, например, фишинговых писем. Это сигнал о том, что нужно быть начеку.

Не только «на периметре», но и внутри сети возникают такие «бодрящие» события. Например, создание учетных записей пользователей или изменение членства в группах безопасности. Это обычные действия администраторов, но их тоже следует фиксировать и, как минимум, отправлять администраторам, чтобы они могли посмотреть и подтвердить, что это была их работа.

Иногда «бодрящие события» относят к классу False Positive и стараются избавиться от них SOC. Это ошибка. False Positive — это совсем другое, это когда некое автоматическое правило анализа событий выявляет индикатор «опасного» события, а на самом деле событие штатное. Кстати, такие события тоже

SOC В ПЕРВУЮ ОЧЕРЕДЬ — ЭТО ЛЮДИ. А SIEM — ЭТО ВСЕГО ЛИШЬ СРЕДСТВО АВТОМАТИЗАЦИИ ТРУДА, ПОЗВОЛЯЮЩЕЕ СОКРАТИТЬ ТРУДОЗАТРАТЫ ПЕРСОНАЛА SOC

не следует сразу отбрасывать, так как это вопрос точности индикаторов. Вместо того, чтобы «выбросить» False Positive, надо подумать над тем, как уточнить индикаторы.

RedTeam. Аналитики SOC всегда должны иметь некоторое количество инцидентов в работе независимо от того, происходят в настоящий момент реальные атаки на активы организации или нет — быть «на страже». Чтобы обеспечить поток атак, реализуется концепция RedTeam (непрерывного внутреннего теста на проникновение) — практические навыки аналитиков совершенствуются непрерывно, а сама RedTeam совершенствует свои навыки скрытной эксплуатации уязвимостей и изучения корпоративной сети.

Чтобы не получилось как в известной истории про «Волки! Волки!», RedTeam должна быть не одна и постоянно перемещаться по сети — источники атак обязаны различаться. Время от времени RedTeam должна появляться в принципиально другом сегменте инфраструктуры, чтобы уже изученная первая команда не становилась преимуществом аналитиков SOC. Развитые компетенции RedTeam можно использовать уже в ходе независимых аудитов безопасности клиентов, поставщиков или дочерних предприятий.

Управление конфигурациями. Критично важен процесс управления конфигурациями. Ваша CMDB — большое подспорье для SOC. Очень трудно защищать что-то, о чем не имеешь ни малейшего представления. Но хороший процесс управления конфигурациями и актуальная CMDB — очень большая редкость. Однако есть минимум, без которого «каши не сварить».

Прежде всего нужно выделить в вашей системе критические сегменты. Как правило, они связаны с важнейшими бизнес-процессами: платежи, каналы продаж, CRM и т.п. В них попадают критические элементы инфраструктуры: серверы, сетевые коммутаторы и маршрутизаторы, АРМы операторов и АРМы управления (администрирования). Для критических сегментов у вас, скорее всего, будет более строгий Security Baseline, но главное не в этом. Как правило, в этих сегментах реже проис-

В КОМПАНИИ С РАЗМЕРОМ ИНФРАСТРУКТУРЫ ДО 500 УЗЛОВ ПРАКТИКИ НЕ БУДЕТ ПОЧТИ СОВСЕМ, ОТ 500 ДО 2000 УЗЛОВ — ОПЫТА ПРИДЕТСЯ НАБИРАТЬСЯ ДОЛГО, БОЛЕЕ 2000 — ТУТ, ПОЖАЛУЙ, МОЖНО НАУЧИТЬСЯ В ТЕЧЕНИИ ГОДА-ДВУХ

ходят события изменения конфигурации и характер потоков данных относительно стабилен. Любое отклонение от стабильного состояния здесь является более подозрительным событием, чем в общем потоке событий. Можно определить несколько категорий активов, включая производственный, тестовый и девелоперский сегменты.

Также необходимо определить, какие свойства актива приоритетны: доступность или безопасность. Это важно для разработки разумных сценариев реагирования. Самая безопасная реакция при подозрении на успешную атаку, например, на какой-нибудь сервер, — отключить его, но вряд ли это разумно в отношении сервиса online-продаж. Или разумно? Это не очень простой вопрос.

Ваш SOC должен обладать указанной выше информацией о вашей системе, иначе он будет вынужден всего лишь дублировать «лай караульной собаки».

Маленьким нельзя. Почему трудно создать эффективный SOC в рамках небольшой компании?

Как мы уже говорили, главная ценность SOC — люди, обладающие необходимым опытом и знаниями. Главная проблема в том, что эти люди должны постоянно учиться, приобретая не только знания, что просто, но и навыки. Если вы отлично знаете устройство токарного станка, это не значит, что вы токарь 8-го разряда. Навыки приобретаются только на практике. А где взять практику? Грубо говоря, в компании с размером инфраструктуры до 500 узлов практики не будет почти совсем, от 500 до 2000 узлов — опыта придется набираться долго, более 2000 — тут, пожалуй, можно научиться в течении года-двух.

Большим тоже. Почему трудно создать эффективный SOC в рамках большой компании?

В большой компании трудно навести и поддерживать порядок на том уровне, который необходим для эффективной работы SOC. Трудно описать конфигурации и Security Baseline, трудно расставить контроли. Трудно, но можно.

«ЗДОРОВЫЙ И БОГАТЫЙ»

К сожалению, очень часто процесс построения SOC состоит из трех этапов, длительностью по полгода каждый:

1. Мы решили сделать SOC и выбираем самый лучший SIEM.
2. Консультант внедрил нам самый лучший SIEM, и он классно работает.
3. Кто-нибудь помнит пароль от консоли SIEM?

И не надо думать, что это преувеличение «для красного словца». Когда видишь такую картину первый раз в жизни — удивляешься, второй раз — не веришь своим глазам, третий — понимаешь, что это судьба. Причем, судьба очень многих.

С другой стороны, стоимость коммерческих сетевых IDS даже для средней компании для мониторинга всех сегментов сети составит десятки и сотни миллионов рублей, и, как правило, таких денег у бизнеса нет. Остается лишь по старинке брать SIEM. Но без мониторинга сети нельзя быть уверенным, что злоумышленник будет найден, поэтому нужно искать другие варианты. Например, использовать решения Open Source или аутсорсинг.

* * *

Не бывает безвыходных ситуаций, бывают лишь нелегкие решения, но без таковых в нашей профессии не состояться.



Евгений АФОНИН
архитектор решений информационной безопасности Micro Focus



Виктор СЕРДЮК
генеральный директор
АО «ДиалогНаука»

SOC НЕ РАВЕН SIEM

ОПЫТ КОМПАНИИ MICRO FOCUS В ПОСТРОЕНИИ СИТУАЦИОННЫХ ЦЕНТРОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В 2017 году исполнилось 10 лет, как первые решения Micro Focus ArcSight¹ были внедрены в российских компаниях. За эти годы более 400 компаний доверили сбор и анализ информации о событиях безопасности этой платформе.

УНИКАЛЬНЫЙ ОПЫТ

Одна из важнейших задач, стоящих перед Micro Focus и отечественными компаниями-интеграторами — перенос лучших практик зарубежного опыта. И тут простого технологического лидерства недостаточно, поскольку успех в данном случае зависит, в том числе, от зрелости и мастерства людей, которые занимаются установкой, настройкой и последующей эксплуатацией продукта Micro Focus ArcSight. За 10 лет был накоплен уникальный опыт в установке и эксплуатации продукта, его проектировании, а самое важное — понимании того, как на базе Micro Focus ArcSight построить процессы управления инцидентами информационной безопасности.

НЕТРИВИАЛЬНАЯ ЗАДАЧА

Сегодня одним из наиболее эффективных средств мониторинга и реагирования на инциденты ИБ является создание SOC (Security Operations Center). Общепринятого определения SOC все еще нет, но мы будем понимать под ним выделенную организационно-штатную структуру, ответственную за обработку инцидентов ИБ и располагающую необходимым техническим обеспечением. Деятельность SOC должна быть строго регламентирована внутренними нормативными документами, описывающими все этапы процесса управления инцидентами — от их регистрации до устранения их последствий и последующего расследования.

Эффективность работы SOC обеспечивается конвейерным подходом в организации работы, строгой специализацией ответственных сотрудников, автоматизацией рутинных задач и тесным взаимодействием с остальными подразделениями предприятия — как в части реагирования на инциденты, так и в части определения актуальных задач информационной безопасности. Такая организация позволяет обеспечить стабильное качество работы сотрудников по выявлению и реагированию на инциденты ИБ, четко понимать

структуру инвестиционных и операционных затрат с учетом заданного уровня качества, а также иметь возможность их обоснования перед руководством организации. В качестве базовой платформы для организации SOC, как правило, выступает система мониторинга событий ИБ (SIEM), при этом необходимо понимать, что SOC не равен SIEM.

Организация эффективного SOC является нетривиальной задачей, которая к тому же находится на пересечении трех различных составляющих: кадры, технологии и регламенты взаимодействия-эксплуатации. Как поставщик платформы ArcSight, Hewlett Packard Enterprise, ныне Micro Focus, сталкивался с задачами построения SOC достаточно часто, чтобы создать в 2007 году выделенное подразделение по созданию SOC с нуля или аудиту уже существующих SOC. За время работы созданного подразделения Security Intelligence & Operations Consulting (ранее HPE SIOC, ныне Micro Focus SIOC) силами этой международной команды из 50 специалистов было создано более 50 SOC и проведено более 120 аудитов по всему миру.

САМЫЙ БОЛЬШОЙ SOC

Три года назад Micro Focus SIOC (ранее HPE SIOC) создал внутренний SOC

¹ 1 сентября 2017 г. компания Hewlett Packard Enterprise выделила подразделение HPE Software и объединила его с компанией Micro Focus.

компании Hewlett Packard, который обрабатывает события аудита, поступающие со всей ИТ-инфраструктуры, обеспечивающей повседневную работу более 300 тыс. сотрудников компании по всему миру. С целью своевременного выявления инцидентов ИБ каждую секунду в реальном времени коррелируется более 3 млрд событий ежедневно. Команда Micro Focus SOC состоит из трех смен аналитиков первичного реагирования, которые обеспечивают мониторинг выявленных инцидентов круглосуточно, отдельной команды по выполнению расследований подтвержденных инцидентов ИБ, двух инженеров Micro Focus ArcSight и, самое важное, руководителя SOC, отвечающего за вопросы контроля качества, управления персоналом, развития SOC и взаимодействия с остальными подразделениями Micro Focus.

Проектирование и создание Micro Focus SOC заняло порядка 8–10 месяцев и включало в себя создание и развертывание отказоустойчивой инфраструктуры по автоматическому сбору, хранению и корреляции событий аудита на базе платформы Micro Focus ArcSight, формулирование требований и прием персонала с привязкой к специфике но-

ПРОЦЕСС СОЗДАНИЯ SOC БЫЛ РАЗДЕЛЕН НА ТРИ ЭТАПА: ЗАЩИТА ПЕРИМЕТРА, ЗАЩИТА ВНУТРЕННИХ ПРИЛОЖЕНИЙ И ЗАЩИТА БИЗНЕС-ПРОЦЕССОВ, ЧТО ПОЗВОЛИЛО СУЩЕСТВЕННО ПРИБЛИЗИТЬ ДАТУ НАЧАЛА РАБОТЫ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

менклатуры инцидентов ИБ Micro Focus, создания необходимых правил корреляции событий, инструментальных панелей мониторинга и отчетов по показателям повседневной работы команды SOC, а также регламентов реагирования на инциденты и взаимодействия с остальными подразделениями Micro Focus. Процесс создания SOC был разделен на три этапа: защита периметра, защита внутренних приложений и защита бизнес-процессов, что позволило существенно приблизить дату начала работы в режиме реального времени.

Из наиболее важных выводов по итогам данного проекта стоит выделить следующие: костяк группы аналитиков

SOC должен обладать опытом выявления и реагирования на инциденты; необходимый опыт инженера по обслуживанию ИТ-инфраструктуры должен быть не менее двух лет; в целях снижения текучки персонала в SOC необходимо предусмотреть план развития сотрудников; при организации круглосуточного мониторинга обязательно необходимо обеспечивать передачу опыта между сменами; карта компетенций каждой функциональной группы специалистов должна быть актуализирована относительно утвержденной номенклатуры инцидентов и учитывать неизбежную ротацию специалистов SOC.

Метрики работы SOC						
Идентификатор	Метрика	Текущий период			Динамика	Статус
		За день, среднее	За день, максимальное	За день, минимальное		
TM-002	Инциденты, содержащие достаточное количество исходной информации	86%	100%	75%	↑	2
	Дополнительные затраты (чч), связанные с недостатком исходной информации	8.2	9.1	0	↓	2
TM-003	Количество событий на аналитика в час	11.1	132.1	2.1	↑	1
TM-004	Инциденты с уникальным текстом описания	83%	95%	76%	—	2
TM-005	Инциденты, потребовавшие изменения уровня влияния аналитиком	17%	19%	7%	↓	3
TM-006	Ошибки 2 рода с группировкой по сценариям	11%	15%	0%	↓	3
TM-007	Уведомления с эскалацией до 2го уровня	15%	30%	10%	↓	1
	Уведомления с эскалацией до 3го уровня	7%	10%	0%	↓	2

Рисунок 1. Пример внутренних метрик работы SOC

СОГЛАСНО ОТЧЕТУ «STATE OF SECURITY OPERATIONS 2016: REPORT OF CAPABILITIES AND MATURITY OF CYBER DEFENSE ORGANIZATIONS», КОТОРЫЙ БЫЛ ОПУБЛИКОВАН НРЕ SIOC, СРЕДНИЙ УРОВЕНЬ ЗРЕЛОСТИ SOC ПО МИРУ НЕ ПОДНИМАЛСЯ ВЫШЕ 1.5, ПРИ МИНИМАЛЬНОМ ПОКАЗАТЕЛЕ 0.59 И МАКСИМАЛЬНОМ 3.34

Более подробную информацию о работе SOC Micro Focus можно узнать из публикаций на профильных конференциях и тематических печатных изданиях. Сам SOC территориально расположен в Пало-Альто и является хорошей площадкой для демонстрации возможностей технологий безопасности Micro Focus.

ДАЛЬНЕЙШЕЕ РАЗВИТИЕ

Дальнейшее развитие SOC на предприятии является не менее ответственной и комплексной задачей, чем его развертывание. Команда Micro Focus Security Intelligence & Operations Consulting

при формировании оценки зрелости SOC и рекомендаций по его развитию использует модель CMMI с разделением на следующие уровни: Incomplete, Performed, Managed, Defined, Measured. Более того, используя статистику предыдущих аудитов, индексная оценка зрелости SOC по шкале от 0 до 5 по каждому из показателей разделов Business, People, Process, Technology может быть оценена относительно среднего наблюдаемого уровня зрелости заказчика в его вертикали — телеком, банки, ритейл и пр. Такой подход позволяет сформировать долгосрочные

цели развития SOC на 2–3 года вперед и подготовить календарный план мероприятий для их достижения, как в части технологий, так и в части персонала и процессов их организующих.

ЧТО ПОЧИТАТЬ?

Ежегодно Micro Focus SIOC публикует на своей странице <https://software.microfocus.com/en-us/software/security-operations-center> аналитические материалы по различным актуальным проблемам построения SOC.

Наиболее интересной для отечественного рынка, на наш взгляд, может являться информация об управлении персоналом SOC, начиная от определения ролей и обязанностей, оценки уровня компетенций, подготовки плана развития сотрудников и организации сменной работы до преодоления проблем, связанных с ротацией специалистов. Полезные рекомендации, полученные из реального опыта, также можно найти в документе «Growing the Security Analyst: Hiring, training, and retention» (Как вырастить аналитика по безопасности: Найм, обучение и удержание).

Согласно отчету «State of Security Operations 2016: report of capabilities and

Описание	Отдел архитектуры и стратегического развития	Руководитель SOC	Аналитик уровня 2	Аналитик уровня 1	Аналитика угроз	Отдел сервисов SOC	Отдел сопровождения	Владелец системы	Отдел системного администрирования	Отдел реагирования на инциденты	Отдел персонала	Отдел связей с общественностью	Юридический отдел	Отдел соответствия и аудита
Обнаружение угроз с помощью мониторинга и анализа событий	C	A	R	R	R	I	C	C	R	C	C	C	C	I
Постоянный мониторинг исторических данных для выявления подозрительной активности	C	A	C	C	R	I	C	C	C	C	C	C	C	I
Предоставление отчетов для аудита	C	I	R	R		I	R	Y	R	R				A
Создание правил/отчетов SIEM	C	I	I	I	I	I	A	C	I	I	I	I	I	I

Рисунок 2. Пример матрицы распределения ответственности по модели RACI

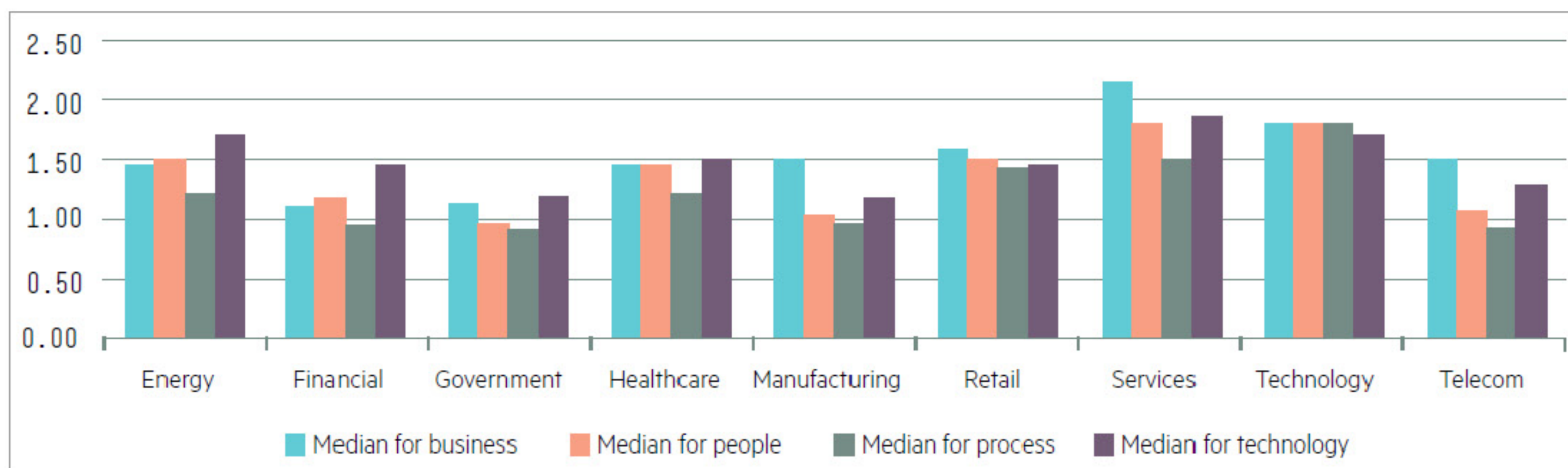


Рисунок 3. Распределение среднего уровня зрелости SOC по вертикалям за последние 5 лет

maturity of cyber defense organizations», который был опубликован Micro Focus SIOC, средний уровень зрелости SOC по миру не поднимался выше 1.5, при минимальном показателе 0.59 и максимальном 3.34. Повышение уровня зрелости SOC не должно быть самоцелью, а его границы, как правило, определяются бюджетом, согласованным в рамках бизнес-кейса, привязанного к актуальным задачам обеспечения ИБ организации. Ключевыми трендами прошлого года стали более широкое использование аутсорсинга для замещения — масштабирования аналитиков первичного реагирования, появление новой роли data scientist для работы с большими данными и поведенческими профилями, а также растущая популярность средств автоматизации реагирования на инциденты ИБ.

ПЯТЬ ОШИБОК

Интересна и статистика из прошлых отчетов Micro Focus SIOC, которая показывает, что только 25% проектов создания SOC добились выполнения поставленных целей. При этом, если привести пять наиболее часто встречающихся ошибок, то можно увидеть следующее: а) недостаток поддержки. SOC не подвешен в вакууме. Его сотрудникам приходится каждый день взаимодействовать с большинством подразделений организации. Без поддержки руководства и четко определенной цели обеспечить эффективную работу по расследованию инцидентов невозможно; б) упор на технические решения. Наиболее частой причиной проблем является перекос бюджетов в сторону внедрений технических ре-

шений, что приводит к недостаточной квалификации и количеству специалистов. Большинство современных угроз требует серьезной квалификации аналитика, а также высокого уровня организации работы по расследованию инцидентов; в) нарушение принципа «от простого к сложному». Проблемы с решением базовых задач ИБ обязательно приводят к затруднениям при решении задач более высокого уровня. Управление информационными активами, корреляция кадровой информации, категоризация информационных активов — вся эта информация является ключевой при расследовании инцидентов; г) отсутствие фокуса. Решение несвойственных, второстепенных задач оказывает существенное негативное влияние на результаты работы ситуационного центра; д) работа «ради галочки». К сожалению, решение задач по обеспечению формального соответствия требованиям регуляторов или стандартам не всегда приводит к существенному повышению уровня защищенности; е) отсутствие процессного подхода. Финансирование ситуационных центров зачастую заканчивается на этапе внедрения. Обеспечение ресурсами их повседневной работы зачастую крайне недостаточно, однако совершенно необходимо для их эффективной работы.

НЕМНОГО РЕКЛАМЫ

В заключение хотелось бы сказать, что на отечественном рынке ИБ находятся все составляющие успеха для построения эффективного SOC: 1) проверенные технологии — на российском рынке представлено много промышленных

систем класса SIEM, одной из которых является Micro Focus ArcSight. Пользователями Micro Focus ArcSight в РФ являются все основные провайдеры мобильной связи, один из крупнейших телекоммуникационных операторов проводной связи, один из крупнейших поставщиков услуг по железнодорожным перевозкам в РФ, крупнейшие российские банки, а также многие другие организации, имеющие подразделения по всей территории нашей страны; 2) необходимые компетенции — за эти годы появилось множество специалистов по продуктам SIEM, которые обладают многолетним опытом работы по реагированию и расследованию инцидентов ИБ, администрированию, проектированию, внедрению и развитию данной платформы; 3) понимание процессов и задач SOC — активная работа Micro Focus Enterprise Security, отечественных интеграторов по обобщению отечественного и зарубежного опыта и организации процессов SOC, проведение регулярных тематических конференций по профилю SOC, наличие отечественных компаний, предлагающих услуги аутсорсинга по мониторингу и расследованию инцидентов ИБ.

* * *

Все перечисленное позволяет нам с уверенностью сказать, что те компании и предприятия, которые выбирают организацию собственного SOC, принимают правильное решение, позволяющее существенно повысить уровень защищенности предприятия как от внешних, так и внутренних угроз.



Максим ФИЛИПОВ
директор по развитию бизнеса
Positive Technologies в России

МОЖЕТ ЛИ ЭФФЕКТИВНАЯ SIEM-СИСТЕМА СТОИТЬ ДЕШЕВЛЕ?

Технология SIEM (Security information and event management) существует уже более 15 лет и за это время де-факто стала мировой практикой при организации управления инцидентами информационной безопасности. В России бум на внедрение SIEM-систем пришелся на 2011–2013 годы. Но и сегодня российский рынок еще далек от насыщения и, по нашим оценкам, продолжает расти в среднем на 20–25% в год.

Первыми SIEM-системы внедрили компании финансового и телекоммуникационного секторов, традиционно стоящие на передовой борьбы с киберпреступниками и, как следствие, нововведений в области ИБ. Сегодня же интерес к решениям данного класса проявляют представители самых различных отраслей. Например, в число наших клиентов входят компании различных сфер: госучреждения, промышленные предприятия и ТЭК. Впрочем, многие компании пока только осознают необходимость использовать системы данного класса и пытаются сформировать свои требования к ним.

Однако более половины (52%) организаций не удовлетворены эффективностью выявления ИБ-инциден-

тов с помощью SIEM. Большинство существующих на данный момент систем не выявляют целенаправленные и быстрые массовые атаки. Еще один недостаток — высокие затраты на внедрение процессов реагирования и экспертизу специалистов эксплуатации. Так, по статистике Ponemon Institute LLC, для анализа и реагирования на инциденты 68% компаний вынуждены нанимать дополнительный персонал, а расходы на поддержку SIEM составляют четверть всего ИБ-бюджета!

Возникают закономерные вопросы: возможно ли сократить стоимость эксплуатации SIEM? И при этом повысить эффективность выявления инцидентов? Попробуем разобраться.

КАК ПОВЫСИТЬ ЭФФЕКТИВНОСТЬ SIEM

Основные причины низкой эффективности традиционных SIEM-систем в том, что необходимо постоянно изменять настройки системы — для того чтобы она продолжала собирать актуальные данные из источников и выявлять инциденты, а также отсутствие специалистов с опытом по расследованию инцидентов, аудиту и тестам на проникновение. Чтобы изменить сложившуюся ситуацию

на рынке SIEM, нужны новые подходы для эффективного выявления инцидентов ИБ. SIEM должна быть инструментом оперативного реагирования на инциденты и выявлять широкий круг угроз, что возможно при адаптации системы к изменениям ИТ-инфраструктуры, ее полном понимании, работающих правилах корреляции и знаниях об актуальных угрозах. Все эти подходы мы реализовали в системе MaxPatrol SIEM.

Контроль ИТ-инфраструктуры. ИТ-инфраструктура крупных компаний разнообразна и состоит из большого количества элементов. Специалисты по информационной безопасности каждой компании должны контролировать изменения в ИТ-инфраструктуре для решения своих повседневных задач. Зачастую компании для контроля ИТ-инфраструктуры приобретают дополнительные решения, которые также требуют интеграции с другими системами, что влечет за собой двойную нагрузку. Поэтому, как правило, специалисты по безопасности имеют устаревшую «картину мира».

В отличие от классических решений, MaxPatrol SIEM поддерживает актуальную модель ИТ-инфраструктуры и механизмы Asset Management. Топология сети строится автоматически и так же автоматически изменения сразу отображаются в модели инфраструктуры. В условиях массовых атак с моментальным распространением, таких как WannaCry или NotPetya, только актуальные знания о топологии сети позволяют выявлять заражение до его масштабного распространения в сети. Таким образом, MaxPatrol SIEM обладает актуальной информацией о состоянии каждого актива и выполняет сразу две задачи: анализирует сеть в режиме реального времени, обеспе-



* Challenges to Achieving SIEM Optimization, Ponemon Institute LLC, March 2017

** SIEM Efficiency Survey (Netwrix, 2016)

чивая тем самым моментальное реагирование на инциденты, и контролирует текущее состояние ИТ-инфраструктуры. Решение этих задач с помощью SIEM позволяет ИТ- и ИБ-службам сэкономить на внедрении дополнительного решения.

Работающие правила нормализации, корреляции и агрегации. Еще одна проблема, из-за которой компании снова и снова вливают деньги в поддержку SIEM-системы, — неработающие правила. Каждый день в инфраструктуре происходят конфигурационные изменения, что приводят к «поломке» правил, ложным срабатываниям или пропуску множества событий. Существующие средства ИБ адаптируются к изменениям с большой задержкой — приходится добавлять новые правила нормализации, корреляции и агрегации и тут у заказчика есть выбор: делать это самостоятельно или с помощью интегратора. Процесс этот бесконечен, так как правила теряют жизнеспособность с подключением новых источников логов и обновлением продуктов. В результате SIEM работают только в тех компаниях, где есть десятки специалистов по безопасности. В остальных случаях SIEM используется как дорогой лог-коллектор.

Очевидно, что необходимо изменить парадигму SIEM: система по архитектуре должна быть не просто доработанным лог-менеджером (что лежит в основе большинства традиционных SIEM) и строить правила корреляции на основе логов, а должна работать с более высокоуровневыми динамическими данными для создания правил корреляции, которые автоматически адаптируются к изменениям ИТ-инфраструктуры и не требуют постоянной перенастройки, а значит, позволяют снизить затраты на эксплуатацию SIEM.

Расследование инцидентов. Традиционные SIEM-системы не могут увидеть историю актива за все время его жизни, что затрудняет проведение ретроспективного анализа при расследовании инцидентов. Как следствие, экспертам приходится вручную изучать «сырые» данные и искать в них закономерности. Чтобы решить эту задачу требуется несколько специалистов, которые смогут анализировать логи нескольких систем-источников. Как следствие —

увеличивается экспертозависимость системы и стоимость ее эксплуатации.

В MaxPatrol SIEM присутствуют механизмы точной идентификации ИТ-активов. Например, если один или несколько компьютеров изменили IP-адрес, то система контроля ИТ-инфраструктуры узнает его и будет продолжать видеть историю изменения актива. Вся история изменений сохраняется в паспорте ИТ-актива, который можно просмотреть во времени за всю историю жизни актива, а значит, для расследования инцидентов уже не требуется глубоких знаний в анализе логов различных систем, следовательно, снижается зависимость от экспертов.

Знания об актуальных угрозах. Пожалуй, наиболее ресурсозатратное условие для эффективной работы SIEM — необходимость выявлять новые угрозы, которые появляются каждый день. Как правило, компания настраивает правила корреляции на выявление инцидентов, которые однажды уже произошли в компании, при этом понимая, что не защитит себя таким образом от атак, в основе которых новые методики проникновения в ИТ-инфраструктуру. Производитель SIEM-системы в свою очередь может поделиться своими знаниями только в ручном режиме — через специализированные форумы или рассылку бюллетеней, в то время как массовые атаки типа WannaCry и NotPetya происходят молниеносно.

Чтобы выявлять новые угрозы, группа эксплуатации SIEM должна включать экспертов, специализирующихся на тестировании на проникновение, исследовании уязвимостей и расследовании инцидентов. Но таких специалистов на рынке крайне мало. Так, по данным Cybersecurity Skills Gap, нехватка ИБ-специалистов к 2019 году в мире составит 2 млн человек. В России уже сейчас нехватка достигает 60 тысяч человек. Современный бизнес (например, Сбербанк, QIWI, «Тинькофф Банк») вкладывает большие деньги в кибербезопасность и образует новые структуры с лучшими специалистами на рынке. Остальные компании могут попытаться перекупить специалистов, но в условиях ограниченного ИБ-бюджета чаще всего вынуждены обходиться 1–2 специалистами поддержки SIEM-системы.

Однако есть и альтернативный подход. Мы вложили наш пятнадцатилетний опыт проведения тестов на проникновение и аудитов защищенности, реверс-инжиниринга, анализа уязвимостей и расследования инцидентов в облачную базу знаний Positive Technologies Knowledge Base (PT KB). Она автоматически наполняет MaxPatrol SIEM новыми способами обнаружения компрометации в виде правил корреляции, агрегации, нормализации, а также информации о способах расследования инцидентов. Таким образом, с помощью PT KB мы предоставляем заказчикам возможность выявлять актуальные угрозы сразу, как только нашим экспертам становится о них известно. Такой подход позволяет снизить требования к экспертизе и числу персонала внутри заказчика.

SIEM-СИСТЕМА МОЖЕТ СТОИТЬ ДЕШЕВЛЕ

Мы считаем, что затраты на эксплуатацию SIEM могут быть в разы меньше. Однако для снижения стоимости и повышения эффективности в архитектуре SIEM должны быть заложены новые принципы, которые позволят сократить издержки на эксплуатацию (актуализацию правил и оперативность реагирования), что невозможно при традиционном подходе к построению SIEM-систем. SIEM должна выполнять несколько функций и решать задачи контроля ИТ-инфраструктуры, тем самым убрав необходимость в дополнительном решении.

Решения класса SIEM должны стать не только инструментом для работы экспертов, но и снизить нагрузку на них за счет предоставления актуальной информации о новейших угрозах от экспертных и исследовательских команд. Это обеспечит SIEM-систему уникальной базой знаний, аккумулирующей актуальные данные об угрозах в формате уже готовых работающих правил корреляции, которые помогут выявлять современные атаки на информационные системы организации. Все эти новые подходы получили свое применение в системе MaxPatrol SIEM, которая учла недостатки существующих систем и уже сейчас выявляет новые угрозы, а также знает, как расследовать инциденты.



**Станислав
МЕРЗЛЯКОВ**
ведущий инженер
департамента
информационной
безопасности
АМТ-ГРУП

НУЖЕН ЛИ SOC? РЕШАТЬ ВАМ!

А СПЕЦИАЛИСТЫ ПО ФОРЕНЗИКЕ —
НЕ ВОЛШЕБНИКИ

Совсем недавно я участвовал в расследовании инцидента в одной компании. Этот инцидент мне понравился своей наглядностью. Предлагаю свое видение ситуации: первичное обследование и выводы.

Вкратце — на одном из компьютеров специалиста ИТ-отдела стали происходить странные вещи с буфером обмена. Периодически, при работе с буфером, из него вставлялись то куски документов, то команды, которые, по его словам, он никогда не вводил. В наш SOC для расследования компания обратилась только спустя месяц после обнаружения такого поведения.

ПРЕДЫСТОРИЯ

До данного инцидента АМТ-ГРУП уже работала с этим заказчиком. Некоторое время назад был реализован проект, в рамках которого мы внедряли, в том числе, пограничный NGFW. Также на АРМ работников и Windows-серверах было установлено антивирусное ПО — вот и все, что было из технических средств защиты в данной компании. Выделенного отдела ИБ тоже нет, часть

задач возложена на ИТ-отдел, который периодически смотрит логи упомянутого NGFW. Следует отметить, что еще во время проекта по интеграции мы предлагали подключить услугу экспертного мониторинга SOC или помочь с разработкой собственного, но, из-за недостаточного финансирования направления ИБ, заказчик отказался.

ОБСЛЕДОВАНИЕ

Услышав описание инцидента, к заказчику я ехал, честно говоря, без особой надежды на успех расследования. По симптомам это, с большой вероятностью, могло быть либо плохо написанное шпионское ПО, либо так совпали звезды, что пользователю это просто показалось (поскольку документальных подтверждений инцидента не было). К тому же прошло около месяца с появления симптомов, а компьютер продолжал использоваться. Шпионское ПО могло уже удалиться, особенно в случае присутствия внутреннего злоумышленника. А косвенные признаки — кэши, физически не удаленные файлы и т.д., которые могли остаться, — уже бы перезаписались. После стандартных процедур снятия дампа

памяти и копии диска, я решил просто бегло осмотреть систему. Вскоре на компьютере были обнаружены интересные артефакты, которые и натолкнули меня на мысль написать статью:

1. На АРМ обновления не ставились уже два года! Т.е. в компании был настроен WSUS, но по непонятным причинам, уже два года был сбой установки. В логах обновления — «отказ» и невнятная ошибка.

2. Логирование событий остановлено и все файлы логов удалены. Служба логирования не перезапускается, выдается ошибка.

3. Последняя запись журнала антивируса — логи удалены пользователем несколько дней назад. Больше ничего. Пользователь говорит, что ничего не удалял.

4. В Windows директории был найден сервис PsExec для удаленного доступа к системе. Как выяснилось, пользователь когда-то сам изучал утилиты из Sysinternals пакета, но, разумеется, он его ставил или злоумышленник — непонятно.

5. IP-адреса DNS-серверов в сетевом подключении подменены на внешние, зарегистрированные в Америке IP-адреса.

6. На АРМ присутствуют учетные записи, назначение которых пользователь не знает.

В принципе, такой букет сюрпризов уже крайне подозрителен. Стоит отметить, что при внедрении SOC даже в минимальном наборе «SIEM + инженер мониторинга» в компании обо всех этих событиях можно было бы узнать через несколько минут, а не лет!

**ПРИ ВНЕДРЕНИИ SOC ДАЖЕ
В МИНИМАЛЬНОМ НАБОРЕ
«SIEM + ИНЖЕНЕР МОНИТОРИНГА»
В КОМПАНИИ ОБО ВСЕХ ЭТИХ
СОБЫТИЯХ МОЖНО БЫЛО БЫ УЗНАТЬ
ЧЕРЕЗ НЕСКОЛЬКО МИНУТ, А НЕ ЛЕТ!**

Дальнейшее расследование — тема отдельной статьи, ниже давайте на основе приведенного случая разберем каждый найденный артефакт в срезе того, как можно было бы ускорить и повысить эффективность расследования, если бы был внедрен SOC. Основная идея тут в важности наличия процесса мониторинга и журналирования событий, позволяющих, по аналогии с традиционным расследованием преступления, сохранять улики и доказательства до того, как они будут затоптаны ногами, смыты дождем, сожжены пожаром и т.д.

Начнем с остановки журналирования. Любой провайдер SOC первым делом настраивает правила, позволяющие выявить сбой службы журналирования. Это можно сделать как сбором некоторых типов событий о неудачной записи в журнал, так и установки таймеров на приемниках событий, которые срабатывают, если от узла не получены события за определенный промежуток времени. Также можно через групповые политики разослать разработанные задачи, отправляющие в журнал события через определенный промежуток времени.

Сбор событий со средств антивирусной защиты (помимо других источников) также является обязательным, как и отслеживание запуска и остановки самого процесса антивируса.

Ошибки обновления компонентов обязательно должны журналироваться и SIEM должна оперативно оповещать об этом инженера мониторинга. Также собираются события об успешно установленных обновлениях, так что, в экстренном случае, например, при эпидемии вируса, использующего незакрытые патчами уязвимости, можно быстро узнать, на каких компьютерах определенный патч отсутствует. Кроме того, при услуге управления уязвимостями выполняется периодическое сканирование внутренней сети на предмет уязвимостей и не установленных обновлений.

Все легитимные средства удаленного управления и другие утилиты, которые могут быть использованы хакерами, но при этом проходить проверку антивирусом, обязательно должны отслеживаться. Их использование можно обнаруживать как по имени файла,

ОКОЛО ДВУХ ТРЕТЕЙ ВСЕХ ИНЦИДЕНТОВ ИБ ПРОИСХОДЯТ СО СТОРОНЫ ВНУТРЕННЕГО ЗЛОУМЫШЛЕННИКА. РЕАЛЬНОЕ РАССЛЕДОВАНИЕ НЕВОЗМОЖНО БЕЗ ПРОАКТИВНОГО МОНИТОРИНГА И ПОЛНОЦЕННОГО ЖУРНАЛИРОВАНИЯ

обращению на известный пул адресов, так и с помощью поведенческого анализа по категории запускаемого средства, если на хостах используется HIPS (например, есть в АВ Касперского — KES). При установке агентов на хост возможности журналирования также расширяются. Если пользователю необходимо использование подобных утилит — настраиваются исключения, но логирование по-прежнему выполняется, и инциденты для инженера мониторинга уже не создаются. К примеру, запуск tcpdump для бухгалтера является инцидентом, а для сетевого инженера нет.

Смену DNS-сервера можно обнаружить по обращению на DNS-порты внешних IP-адресов из внутреннего сегмента сети. Кстати, в данном конкретном случае в смене DNS виноват поставленный для альтернативной проверки антивирус Comodo с опцией по умолчанию Comodo Secure DNS. Но, во-первых, сменой DNS часто промышляет вредоносное ПО, а во-вторых, для некоторых государственных структур такой инцидент фактически отслеживания DNS запросов уже является серьезным нарушением политики безопасности.

Ну и, разумеется, отслеживание изменения списка или прав пользователей — базовая задача любого SOC.

ПОЧЕМУ МОГ ПРОИЗОЙТИ ИНЦИДЕНТ

Чем же плоха описанная ИБ-система и как мог произойти инцидент? Пограничные NGFW решения не видят внутрисетевого трафика, да и от целенаправленных APT атак не спасут. Для того, чтобы убедиться, что обойти такие средства можно без специальных навыков, достаточно ввести в поисковике название вашего средства защиты + bypass, и вы найдете различные

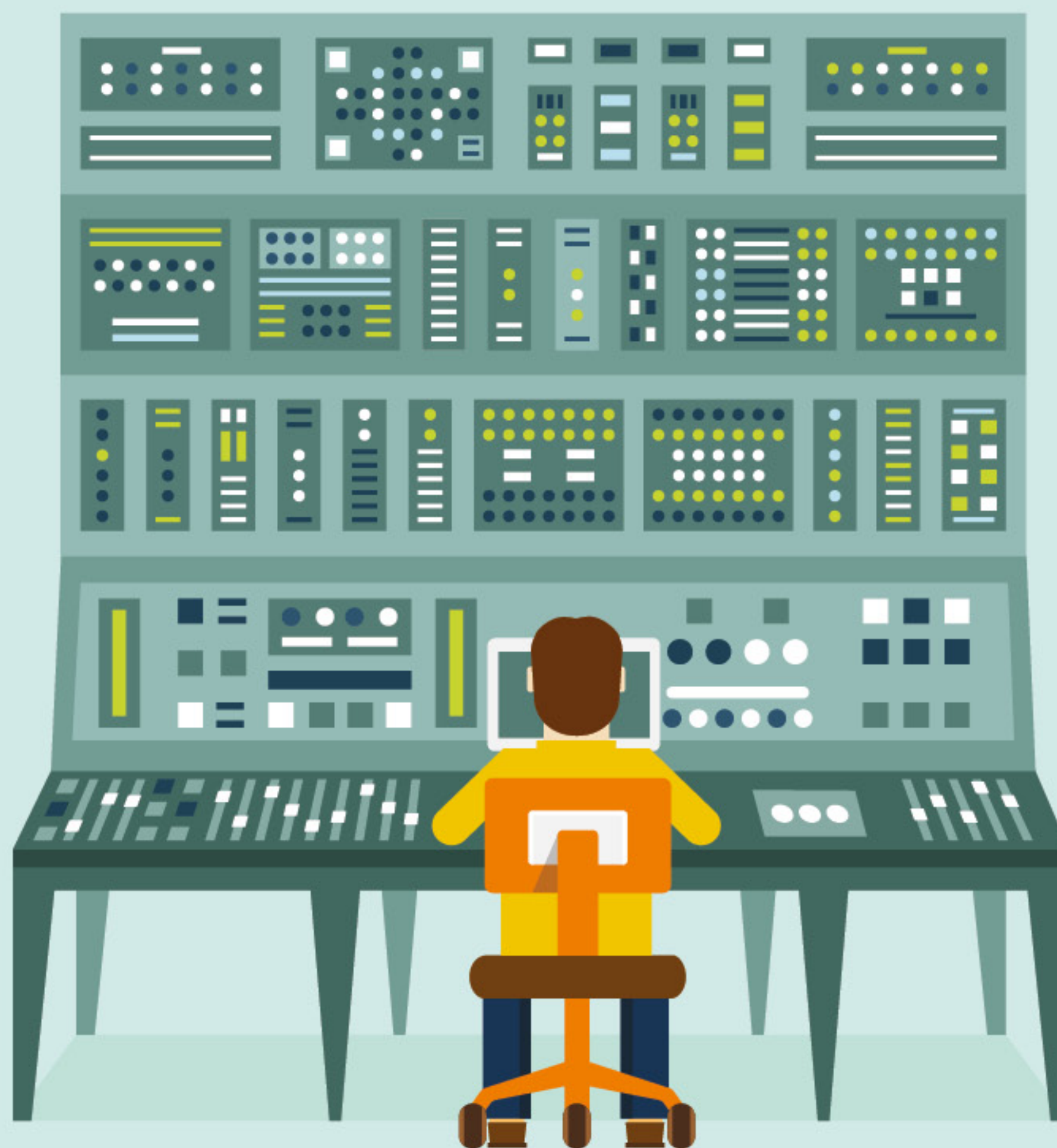
способы, вплоть до использования стандартных msf утилит, чтобы обойти блокировку. Обход современных антивирусов с эвристикой сложнее, но способы также существуют. К примеру, еще недавно вредоносные powershell скрипты не определялись ни одним антивирусом, да и сейчас не все антивирусы это отслеживают. На профильных форумах всегда можно увидеть свежие обсуждения обхода антивирусных движков, не говоря уже о закрытых обсуждениях, которые мы не можем увидеть. К тому же около двух третей всех инцидентов ИБ происходят со стороны внутреннего злоумышленника. Реальное расследование невозможно без проактивного мониторинга и полноценного журналирования.

* * *

Часто можно услышать слова: «Ну вы же специалисты, разбирайтесь, найдите что-нибудь». И не всегда ИТ-или ИБ-специалистам компании удастся объяснить руководителям, не знакомым со спецификой форензики, что, чтобы было в чем разбираться, нужно заранее об этом позаботиться. Специалисты по форензике не волшебники, и доказательства не появляются из ниоткуда. Если нет инструмента, собирающего эти самые доказательства, а злоумышленник постарается и почистит за собой следы, то расследование только затянется, очень дорого обойдется, но не всегда приведет к результату. Кто-то это понимает и объясняет важность развития ИБ в своей компании, кто-то нет. Ждать первого инцидента внутри компании для того, чтобы получить толчок к созданию своего SOC, или позаботиться об этом заранее — решать вам.

НИКАК ИНАЧЕ

О ПРАКТИКЕ КОНТРОЛЯ АДМИНИСТРАТОРОВ



Дмитрий МИХЕЕВ
технический
директор компании
«АйТи БАСТИОН»

Говоря о примерах применения средств контроля администраторов в банковских организациях, стоит помнить, что банк — это сложная распределенная информационная система. Система, которая строилась не в один день, выполняет массу задач, многие из которых тре-

буют как соблюдения значительных требований в части информационной безопасности, так и соблюдения серьезных обязательств по качеству и надежности сервисов.

МАСШТАБ И РИСКИ

Довольно часто выполнение этих задач связано со сложностями масштаба — размер внутренней инфраструктуры, необходимость присутствия во множестве географических расположений и соблюдение положений регу-

лирующих документов накладывают существенные особенности при эксплуатации. На практике это приводит, с одной стороны, к достаточно жесткой централизации предоставляемых услуг, с другой стороны — к высоким требованиям SLA для обеспечения непрерывного функционирования систем связи, вычислительных средств и пользовательских рабочих мест.

Банки эксплуатируют много специализированного ПО, содержат значительные объемы аппаратных ресурсов

и выстраивают жесткие практики эксплуатации в рамках ограниченных бюджетов. На практике это приводит к необходимости обслуживать собственные ресурсы ограниченным штатом персонала, привлекать для обслуживания специализированных средств внешних специалистов — из интеграторов, сервисных служб поддержки оборудования, производителей специально адаптированного ПО. В конечном счете, это неизбежно приводит к необходимости допускать внешних исполнителей с административными правами через периметры безопасности — как внутренних, так и юридически внешних.

Эта ситуация не уникальна и так происходит во многих областях, но в банковской сфере риски порой достигают уровней, с которыми нельзя мириться. Необходимость выполнять требования SLA ограничивается рисками нарушений, которые могут непосредственно нарушить функционирование бизнеса, привести к нарушениям требований регулирующих документов, с достаточной серьезными последствиями.

МОГУТ ПОМОЧЬ

Системы контроля действий администраторов могут помочь упорядочить сложившуюся практику предоставления доступа, поэтому такие решения интересны как ответственным за безопасность, так и ответственным за эксплуатацию. По нашему опыту, наиболее значительные результаты могут быть достигнуты при совместном проекте, где от внедренной системы контроля выигрывают и отдел ИБ, и ИТ службы.

ПРО ДВУХ ЗАЙЦЕВ

Например, в одном из пилотных проектов, инициированном со стороны службы ИБ, уже на этапе аудита и начального запуска удалось перестроить порядок и инфраструктуру узла внешнего доступа таким образом, что вместо нескольких исторически сложившихся вариантов удаленного входа остался только один, что безусловно облегчило нагрузку в части безопасности. Но и ИТ отдел оказался в выигрыше. Мало того, что об одном из старых доступов было практически неизвестно (он не фигурировал в документах и представлял собой потенциальную дыру в зоне от-

НАИБОЛЕЕ ЗНАЧИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ МОГУТ БЫТЬ ДОСТИГНУТЫ ПРИ СОВМЕСТНОМ ПРОЕКТЕ, ГДЕ ОТ ВНЕДРЕННОЙ СИСТЕМЫ КОНТРОЛЯ ВЫИГРЫВАЮТ И ОТДЕЛ ИБ, И ИТ СЛУЖБЫ

ветственности службы ИТ), так получилось применить ту же систему и для записи действий собственных специалистов при обслуживании систем, с отказами которых приходилось регулярно сталкиваться. Имея на руках документальный журнал работы администраторов, удалось защитить собственных исполнителей от обвинений в ошибках администрирования, приводящих к отказам и нарушениям SLA.

НИКАК ИНАЧЕ

Система контроля администраторов предоставляет информацию, которую сложно получить другими способами. Практически все современные протоколы удаленного управления закрыты криптографически, что не позволяет фиксировать происходящее в рамках сессий с необходимой тщательностью пассивными средствами. Очень часто на защищаемых информационных объектах мы ограничены в допустимых средствах безопасности, т.к. их или нельзя установить совсем (например, на маршрутизатор), или применение таких средств повлечет заметную деградацию производительности целевой системы, что неприемлемо. Подробное журналирование со стороны серверов также часто не применяется, т.к. добавляет нагрузки на систему и требует серьезных усилий по обработке потока событий и выделения из него необходимых.

ИСТОЧНИК СОБЫТИЙ

Система контроля действий администраторов выдает события, непосредственно связанные с активностью людей и выполнения ими изменений в настройках. Это исключительно удобно, т.к. это позволяет фиксировать эти действия с необходимыми подробностями на случай будущих расследова-

ний, а также анализировать действия в момент их выполнения. В том числе и с теми или иными вариантами автоматизированного противодействия нежелательным действиям. Даже если просто фиксировать действия администраторов в масштабе информационной системы банка, это является весьма удобным источником событий, который можно использовать как непосредственно, так и подключить в общую систему анализа событий.

ИНТЕРЕСНЫЙ ПРОЕКТ

В нашей практике есть интересный проект, который начался со стороны ИТ службы, с одного очень компактного узла доступа — по результатам внешнего аудита потребовалось усилить контроль за доступом к системе, содержащей персональные данные. Очень быстро, еще на первом этапе знакомства, этот проект вырос до нескольких узлов доступа в разных городах — для обеспечения доступа к оборудованию в ЦОДах для дежурных смен. Узлы контроля удалось интегрировать с SIEM системой и завести на централизованный мониторинг банка, с разработкой необходимых регламентов и диспетчеризацией заявок как на ИТ подразделения, так и с выходом на реагирование по линии ИБ.

* * *

Нельзя сказать, что системы контроля действий администраторов — это «серебряная пуля». Но практика показывает, что задачи для них есть и они приносят пользу, конкретную и измеримую, не требуя при этом устраивать революционных изменений как в техническом плане, так и со стороны регламентов и процедур применения.



Алексей ЦВЕТКОВ
менеджер по продвижению
решений компании
«Информзащита»

ФИНАНСЫ В ПОРЯДОК!

ПРО ВЫПОЛНЕНИЕ СХОЖИХ ТРЕБОВАНИЙ РАЗНЫХ СТАНДАРТОВ ИБ В ФИНАНСОВОМ СЕКТОРЕ

Есть ряд очевидных тенденций на рынке информационной безопасности, отрицать которые нельзя. Они заключаются в том, что вектор движения в ИБ меняется: от «бумажной безопасности», в основном предполагающей формальное соответствие требованиям регуляторов, он движется в сторону технической защищенности, соответствующей уровню рисков организации, и зачастую превосходящей формальные требования. В настоящей статье мы рассмотрим эти тенденции, чтобы понять, как их использовать в процессе обеспечения максимального уровня защищенности.

ТРЕБОВАНИЙ МНОГО...

Требования регуляторов (ЦБ, Роскомнадзор, МПС, SWIFT и т.д.) к защите информации постоянно ужесточаются. Это связано, прежде всего, с непрерывно возрастающим количеством киберугроз и внушительным техническим арсеналом злоумышленников. Последний включает в себя средства автоматизации создания вредоносного кода, не обнаруживаемого классической защитой (антивирусные решения, системы обнаружения и предотвращения вторжений и др.). Также укрепление арсенала нарушителей связано с использованием ими инструментов социальной инженерии, эксплуатацией как публично известных уязвимостей, так и уязвимостей нулевого дня.

Общий перечень требований регуляторов, актуальных на сегодняшний день, приведен в Таблице 1.

...НО ОНИ ПОХОЖИ

При этом, несмотря на большое количество разрозненных требований регуляторов, во многом они очень схожи. Так, например, практически все эти требования включают в себя следующее:

- ♦ уточнение и, по возможности, отделение критической инфраструктуры от менее ценных информационных ресурсов, обеспечение защиты на сетевом уровне;
- ♦ безопасное конфигурирование информационных систем;
- ♦ внедрение дополнительных технических средств защиты информации, включая антивирусную защиту, средства обеспечения контроля целостности;
- ♦ управление доступом пользователей и администраторов;

♦ управление техническими уязвимостями и установка обновлений;

♦ проверка защищенности (путем проведения внутренних или внешних аудитов, тестирования возможности проникновения в защищаемую среду и пр.);

♦ обеспечение регистрации и мониторинга событий информационной безопасности;

♦ выявление инцидентов информационной безопасности и реагирование на них, расследование инцидентов и извлечение уроков из инцидентов;

♦ обеспечение физической безопасности;

♦ обучение и повышение осведомленности в области информационной безопасности;

Норматив	Область регулирования	Регулятор
382-П	Безопасность безналичных платежей	ЦБ РФ
552-П	Подключение к ЦБ РФ АРМ КБР, АРМ ПУР	ЦБ РФ
152-ФЗ (ПДн)	Безопасность обработки персональных данных (ПДн)	Роскомнадзор
PCI DSS	Безопасность данных платежных карт	МПС (Visa, Mastercard)
СТО БР	Обеспечение ИБ технологических процессов обработки платежной и неплатежной информации	ЦБ РФ
SWIFT Customer Security Framework. Supplementary Guide	Обеспечение безопасности выполнения переводов через SWIFT	SWIFT
ГОСТ (проект)	Обеспечение ИБ технологических процессов обработки платежной и неплатежной информации	ЦБ РФ

Таблица 1. Требования регуляторов по защите информации в финансовом секторе

- ♦ моделирование угроз и/или оценка рисков информационной безопасности;
- ♦ данный список может быть продолжен.

НЕТ ЛОСКУТНОМУ ОДЕЯЛУ!

Безусловно, у каждого из внешних требований есть своя отраслевая специфика, которую необходимо учитывать. Но строить систему обеспечения информационной безопасности изначально стоит с учетом всех применимых требований регуляторов, также принимая во внимание корпоративную систему управления организации. В противном случае, система обеспечения информационной безопасности становится похожей на лоскутное одеяло, и для получения общей картины о текущем состоянии защищенности информации и об уровне соответствия внешним требованиям необходимо прикладывать дополнительные усилия со стороны специалистов по безопасности.

Стоит также отметить, что адекватное исполнение требований регуляторов помогает также обеспечить и реальную защищенность, а возникающие инциденты информационной безопасности практически всегда являются следствием невыполнения или неполного выполнения какого-либо из требований или группы требований стандартов.

ДЛЯ ПРИМЕРА

Для примера рассмотрим два применяемых к некоторым организациям финансовой сферы западных стандарта. Первый и давно известный — Payment Card Industry Data Security Standard (PCI DSS), и относительно новый SWIFT Customer Security Framework. У данных стандартов совершенно разные области оценки, которые в идеале не пересекаются. Именно поэтому на данном примере хочется показать, на каком участке можно добиться оптимизации ресурсов, необходимых для соблюдения требований стандартов, и по какому вектору можно направлять усилия для дополнительно повышения уровня защищенности.

Если не подходить к решению каждой из задач разрозненно, а изначально выстраивать работающие процессы, охватывающие всю организацию, либо наиболее ее критичные сегменты, то можно существенно упростить про-

цесс одновременного соблюдения нескольких стандартов. Можно говорить о технической унификации, применении средств автоматизации и, как следствие, снижении затрат на обеспечение безопасности отдельного объекта инфраструктуры. Например, требования по безопасному конфигурированию систем применить и на компоненты в области действия PCI DSS и на серверы, реализующие подключение к SWIFT.

Хороший пример — процесс управления уязвимостями. Данное требование есть в обоих рассматриваемых стандартах. Если расширить область сканирования и установки обновлений на дополнительные серверы, рабочие станции, сетевое оборудование и т.д., то это не сильно увеличит как фактические финансовые расходы, так и трудозатраты системных администраторов и специалистов по защите информации. При этом будут соблюдаться требования сразу двух стандартов. По такому же принципу можно добиться оптимизации затрат по требованиям сетевой безопасности, физической защиты компонентов, мониторингу.

ОТ МИНИМУМА К МАКСИМУМУ

При этом стоит понимать, что должное выполнение требований регуляторов обеспечит только минимально необходимый уровень безопасности, останавливаться на котором нельзя, если организация действительно планирует защититься от актуальных киберугроз. Поэтому, помимо внедрения требуемых регуляторами мер и средств защиты надо проанализировать и сфокусировано защищать критически важные бизнес-процессы организации, а также наиболее уязвимые элементы инфраструктуры.

Определить проблемные и слабые места позволит анализ защищенности или так называемые пентесты. Этот метод оценки уровня безопасности позволяет моделировать атаку злоумышленника. Процесс включает в себя активный анализ инфраструктуры на наличие потенциальных уязвимостей, которые могут спровоцировать некорректную работу, либо полный отказ в обслуживании. Результатом такого анализа или аудита может служить отчет, который содержит в себе все найденные уязвимости системы безопас-

ности, а также рекомендации по их устранению. На основании полученной реальной картины и достоверных данных необходимо корректировать набор используемых инструментов защиты. Но это дополнительные финансовые затраты. Что делать?

ОБ АУТСОРСИНГЕ

В ближайшее время должен выйти новый стандарт ЦБ, который регламентирует использование аутсорсинговой модели ИБ в организациях финансового сектора. Но передача функций на аутсорсинг не освобождает от обязанности и не снимает ответственности с банков как в вопросах обеспечения ИБ, так и в обязательности соответствовать требованиям законодательства. Однако аутсорсинговая модель позволит решить многие задачи в области защиты информации и оптимизировать затраты, передать непрофильную деятельность внешнему подрядчику и сократить эксплуатационные издержки.

Это выход для многих компаний, т.к. не каждая организация имеет ресурсы для киберразведки (threat intelligence); не все оперативно получают информацию о новых угрозах, идентификаторы компрометаций и т.д. Не у всех выстроены и автоматизированы процессы по реагированию на инциденты, процессы проведения расследований (forensics). Аутсорсинговая модель ИБ позволит большему числу компаний повысить уровень информационной безопасности, защитить ценную информацию, финансы и репутацию.

* * *

Возвращаясь же к требованиям стандартов, нужно также помнить, что вслед за изменением ландшафта угроз любые стандарты имеют свойство периодически обновляться. И для того, чтобы организации могли избежать рисков, связанных с возможными архитектурными или иными ошибками, стоит выстраивать свои процессы изначально в соответствии с глобальными тенденциями в сфере обеспечения информационной безопасности, за которыми регуляторные требования, как правило, следуют с некоторым запозданием.



**Владимир
ГЕРАСИМЕНКО**
советник директора
ООО «САФИБ»,
кандидат технических
наук, эксперт ABISS



Иван ГРИГОРЬЕВ
заместитель директора
по управлению проектами
ООО «САФИБ», кандидат
технических наук

РУКА ПОМОЩИ

СИСТЕМА ЗАЩИЩЕННОГО УДАЛЕННОГО МОНИТОРИНГА И УПРАВЛЕНИЯ «АССИСТЕНТ»

В статье рассматривается вопрос минимизации рисков информационной безопасности клиентов банков в процессе устранения сбоев, возникающих при предоставлении дистанционных банковских услуг, и предлагается использование системы защищенного удаленного мониторинга и управления «Ассистент» в качестве соответствующего вспомогательного инструмента.

ПРОБЛЕМА КАК ОНА ЕСТЬ

Для малых и средних организаций банковской системы РФ характерна ситуация, когда в удаленном филиале ИТ-подразделение состоит из 2–3 человек, и кроме того, оно заранее уведомляет клиентов о перерывах в приеме их обращений, мотивируя это занятостью или обслуживанием поступивших электронных транзакций.

От сбоев и ошибок в процессе предоставления дистанционных банковских услуг с использованием интернет-сервисов никто не застрахован. Но что происходит, когда, например, входной фильтр сервиса интернет-клиента не пропускает на подпись платежное поручение, указывая на ошибку, которой клиент в нем не находит? При этом ни операционисты, ни ИТ-подразделение банка не видят этого платежного поручения, так как оно клиентом еще не подписано и не отправлено в банк. Как сегодня на практике разрешается подобная «конфликтная» ситуация?

Клиенту, дозвонившемуся по телефону в банк и перенаправленному в ИТ-подразделение (в случае, если он звонит в рабочее время), предлагается несколько вариантов оказания помощи:

♦ вывод платежного поручения на экран монитора, создание скриншота

и отправка его на электронную почту в ИТ-подразделение;

♦ воспользоваться приложением удаленного доступа для предоставления специалисту ИТ-подразделения банка возможности удаленно подключиться к рабочему столу компьютера клиента. При этом используются широко распространенные системы удаленного управления, построенные по клиент-серверной технологии, и серверная часть которых зачастую расположена или за пределами РФ или на серверных мощностях, неподконтрольных банку.

Предметом статьи не является обсуждение правомочности таких предложений. Мы полагаем, что банк дорожит доверием клиента и стремится помочь ему — в данном случае отправить платежное поручение, разрешив как можно быстрее «конфликтную» ситуацию.

Однако негативные стороны таких предложений заключаются в том, что в указанных сценариях оказания помощи клиенту риски информационной безопасности при устранении сбоев в процессе предоставления дистанционных банковских услуг полностью переносятся на самого клиента: именно он добровольно отправляет скриншот в банк через Интернет, именно он добровольно предоставляет удаленный доступ к своему рабочему столу, зачастую не задумываясь о безопасности (например, рабочий стол компьютера клиента может оказаться доступен третьим лицам, а не только сотрудникам банка).

РЕШЕНИЕ СУЩЕСТВУЕТ

Специалистами нашей компании, имеющей большой опыт разработки высоконагруженного программного обеспечения и технического сопровождения автоматизированных информационных систем в финансовой сфере, разработана система защищенного удаленного мониторинга и управления «Ассистент». Это программное обеспечение может быть использовано в организациях банковской сферы в качестве инструмента для устранения сбоев, возникающих при предоставлении дистанционных банковских услуг, при этом существенно минимизируются риски информационной безопасности клиента, связанные с удаленным доступом.

«Ассистент» представляет собой полнофункциональную систему защищенного удаленного доступа, управления и администрирования компьютерной техники и серверного оборудования и внесен в Единый реестр российских программ для электронных вычислительных машин и баз данных. Может применяться для решения различных задач, возникающих при осуществлении технической поддержки пользователей, например, в вопросах использования и настройки информационных систем, а также для проведения обучения пользователей ПО.

Уже сейчас для работы с «Ассистент» доступно использование серверной компоненты, размещенной в ЦОДе на территории РФ через сеть Интернет. При этом клиентское приложение для

пользователей доступно на официальном сайте системы.

В случае необходимости подобная структура может быть развернута локально внутри закрытой ИТ-инфраструктуры организаций банковской системы.

Понимая, что подобные инструменты должны удовлетворять серьезным требованиям по обеспечению безопасности, в том числе требованиям регуляторов в области защиты персональных данных, в систему было встроено средство защиты удаленного доступа, реализующее следующие функции безопасности:

- ♦ идентификация и аутентификация;
- ♦ управление доступом;
- ♦ регистрация событий безопасности;
- ♦ контроль целостности программного обеспечения.

Программное средство защиты информации от несанкционированного доступа прошло сертификацию в ФСТЭК России на отсутствие недеklarированных возможностей (по 4 уровню контроля) и соответствие техническим условиям, что позволяет использовать его в составе систем защиты информации государственных информационных систем высшего класса защищенности и информационных систем персональных данных высшего уровня защищенности.

Помимо указанного встроенного средства защиты в программном комплексе «Ассистент» реализованы дополнительные меры для обеспечения безопасности удаленного доступа, которые обеспечивают выполнение следующих функций:

- ♦ авторизация пользователей;
- ♦ настройка прав и политик доступа, в том числе разрешение на установление соединения по расписанию и ограничение доступного функционала;
- ♦ ведение журналов действий операторов при использовании инструментов удаленного доступа;
- ♦ ведение видеозаписи действий операторов при осуществлении удаленного доступа;
- ♦ отслеживание работоспособности компонентов программного комплекса;

- ♦ проверка на отсутствие несанкционированных изменений в исполняемых файлах;

- ♦ оповещение ответственных лиц об обнаруженных сбоях или фактах вторжения в работу программного комплекса и его подсистем;

- ♦ шифрование (криптографическая защита) канала удаленного управления с использованием криптографического пакета OpenSSL. При этом в настоящее время ведется разработка модуля, реализующего криптографию по ГОСТ с последующей сертификацией его в качестве средства криптографической защиты информации.

ДОПОЛНИТЕЛЬНЫЕ БОНУСЫ

Таким образом, использование программного комплекса «Ассистент» позволяет обеспечивать высокий уровень доверия при осуществлении удаленного управления и доступа к удаленному рабочему столу компьютера пользователя, в том числе при оказании технической поддержки в процессе предоставления дистанционных банковских услуг и тем самым минимизировать риски информационной безопасности клиентов банков.

На наш взгляд, применение системы защищенного удаленного мониторинга и управления «Ассистент» в качестве вспомогательного инструмента в организациях банковской системы также позволит:

- ♦ осуществлять удаленную поддержку пользователей, удаленных подразделений в вопросах использования и настройки компьютерной техники, программного обеспечения;
- ♦ реализовать дистанционное обучение удаленных пользователей использованию компьютерной техники и программного обеспечения (по принципу «делай как я») и тем самым повысить уровень квалификации специалистов;
- ♦ организовать службу технической поддержки с функциями HelpDesk для собственных нужд внутри филиальной сети банка;
- ♦ предоставлять контролируемый удаленный доступ сторонним ИТ-сервисным компаниям к техническим и информационным ресурсам банка для проведения разовых и периодических работ по настройке и сопровождению.



Евгений АКИМОВ
директор по развитию
кибербезопасности
ГК Softline

ПОБЕДА НАД ВРЕМЕНЕМ

ПОЧЕМУ КИБЕРБЕЗОПАСНОСТЬ КАК
СЕРВИС ЧЕРЕЗ 2–3 ГОДА СТАНЕТ
ОСНОВНОЙ МОДЕЛЬЮ ОБЕСПЕЧЕНИЯ ИБ

С момента обнаружения киберугрозы до её закрытия обычно проходит около года. Но ни один департамент информационной безопасности уже сегодня не может позволить себе потратить на решение проблемы столько времени — интервалы между схожими массовыми атаками сократились до нескольких недель. Именно поэтому одна из приоритетных задач сегодня — найти новую модель защиты от угроз, которая могла бы обеспечить защиту бизнеса в приемлемые сроки.

ПРОДУКТОВЫЙ ПОДХОД

Производители решений для киберзащиты стараются использовать любой информационный повод для продвижения своих продуктов. После Wanna-Cry и Not.Petya в короткие сроки появилось множество статей и инструкций, в которых содержатся рекомендации, как защитить бизнес от атаки вирусов-шифровальщиков. Поставщики защиты от целенаправленных атак напо-

минают про риск zero day и наличие неизвестных уязвимостей, от которых можно спастись, используя песочницы. Поставщики систем резервного копирования призывают копировать данные, чтобы в случае атаки иметь возможность их восстановить и снизить ущерб для бизнеса. Компании, занимающиеся проверками наличия уязвимостей, версионности ПО и др. убеждают, что своевременная установка обновлений способна защитить от атак, что в какой-то степени соответствует действительности, ведь информация о наличии уязвимостей появилась задолго до самих атак. И сейчас уже все знают, что Microsoft достаточно оперативно выпустил патчи, но мало кто их установил. Поставщики SIEM призывают «мониторить» события, происходящие в вашей сети — обнаружение атаки на ранней стадии может вовсе предотвратить её.

Несмотря на преимущества такого подхода (бить чётко в цель), очевидно, что он сложен в реализации, поскольку требует от заказчика самостоятель-

ного анализа эффективности использования каждого продукта.

ИНТЕГРАТОРСКИЙ ПОДХОД

Привлечение интегратора избавляет от необходимости досконально знать возможности того или иного продукта, поскольку предполагается, что вместе с услугами интегратора вы покупаете его экспертизу в этом вопросе. Данный подход определённо можно назвать более зрелым, поскольку он основан на понимании необходимости комплексного подхода к безопасности.

Интеграторы дают рекомендации — как лучше строить систему защиты от угроз, какие продукты использовать. Однако при всём удобстве такого подхода ответственность за эффективность всё равно лежит на заказчике.

SECURITY AS A SERVICE (SECaaS)

К сожалению, ни интеграторский, ни продуктовый подходы не соответствуют требованиям, которые предъявляют текущие реалии: чтобы привести вашу систему безопасности к необходимому уровню, нужно затратить непозволительно много времени. Посмотрим, из чего складывается время на ликвидацию проблемы. После атак вирусов-шифровальщиков весной-летом 2017 года многие компании задумались о внедрении системы резервного копирования. Стартует длительный многоэтапный процесс: выбор продукта (встречи с поставщиками, сравнение и составление списка продуктов, отобранных для пилотирования — 2–3 месяца) > реализация пилотов и выбор поставщика

**ИНТЕГРАТОРЫ ДАЮТ РЕКОМЕНДАЦИИ —
КАК ЛУЧШЕ СТРОИТЬ СИСТЕМУ
ЗАЩИТЫ ОТ УГРОЗ, КАКИЕ
ПРОДУКТЫ ИСПОЛЬЗОВАТЬ. ОДНАКО
ПРИ ВСЁМ УДОБСТВЕ ТАКОГО
ПОДХОДА ОТВЕТСТВЕННОСТЬ
ЗА ЭФФЕКТИВНОСТЬ ВСЁ РАВНО
ЛЕЖИТ НА ЗАКАЗЧИКЕ**

(2–3 месяца) > согласование бюджета (сумма будет существенна, поэтому бюджет будет заложен только на следующий год — ещё полгода ожидания) > конкурс (будет проводиться в новом году — 2 месяца) > внедрение (2–3 месяца).

Получаем целый календарный год. Мы помним, что Not.Petya случился всего лишь через 1,5 месяца после Wanna-Cry. Думаю, что к приходу Not.Petya состоялись бы только первые 2–3 встречи с вендорами, что, конечно, никак не отразилось бы на степени защищённости организации.

В редких случаях департаменту информационной безопасности могут выделить бюджет уже в текущем году (если компания стала жертвой вируса), но даже в ускоренном темпе система резервного копирования была бы построена только к концу года. С другими системами ситуация была бы аналогична, а в некоторых случаях процесс занял бы ещё больше времени.

Интеграторский подход, возможно, более распространён, но и он не способен сократить этот немалый срок. Таким образом, очередной вирус нанесёт вам ущерб, возможно, даже больший, чем его предшественники, просто потому, что невозможно подготавливаться к атаке, используя старые подходы. Риск от таких атак нельзя недооценивать — многие заказчики, вынужденные приостановить работу некоторых своих бизнес-процессов, пришли к нам именно после инцидента с Not.Petya.

Хорошо всем известный подход аутсорсинга кибербезопасности, заключающийся в привлечении сервис-провайдеров (MSSP), способен существенно сократить сроки построения системы защиты. Например, в ситуации с созданием системы резервного копирования провайдер изучает архитектуру, смотрит, какой объём данных необходимо копировать. Затем предлагает решение, которое базируется на полученных данных и его опыте. Через неделю озвучивает цену услуги. Учитывая время на выбор провайдера (2 недели) и время на подключение услуги (2 недели), получается примерно 1–1,5 месяца с момента

БИЗНЕС-ЗАКАЗЧИКУ НЕВАЖНО, КАКИЕ СЕРВИСЫ КИБЕРБЕЗОПАСНОСТИ ВЫ ИСПОЛЬЗУЕТЕ — ОБЕСПЕЧЬТЕ БЕЗОПАСНОСТЬ ЕГО БИЗНЕС-ПРОЦЕССОВ

обнаружения проблемы до её закрытия. Поэтому механизм аутсорсинга MSSP-провайдера — вероятно, самый быстрый и эффективный способ действительно защитить бизнес от киберугроз и сохранить репутацию ИТ-директора.

А ЧТО ДАЛЬШЕ?

Впрочем, радоваться рано. Через некоторое время даже такой формат будет неэффективен для заказчика, поскольку сложность угроз возрастает. Специалистам по кибербезопасности со стороны клиента придётся быть экспертами высшего класса в умении определить, при помощи каких сервисов можно решить проблему. Но даже быть суперэкспертом — недостаточно. Такой специалист должен обладать достаточным авторитетом среди собственного бизнес-руководства, чтобы уметь обосновать и убедить их в том, что им нужен именно такой набор сервисов, потому что только такой набор решит их проблемы. Бизнес-заказчик не понимает, зачем ему нужна песочница как сервис, например. Если даже понимает, что нужна, то надо объяснить, почему именно эта. Почему мы должны платить в год такую-то сумму, а не в два раза меньшую.

Бизнес-заказчику неважно, какие сервисы кибербезопасности вы используете — обеспечьте безопасность его бизнес-процессов.

Представителям бизнеса сложно ориентироваться в параметрах сервисов кибербезопасности, они не обязаны разбираться в них, в отличие от параметров работоспособности бизнес-процессов и технологических процессов. Если провайдер обеспечивает этот бизнес-SLA и несёт финансовую ответственность в случае отклонения от него — это наиболее предпочтительная ситуация для бизнес-заказчика.

Бизнес может высказывать требования, что время простоя его ИТ-сервисов не должно превышать, например, 4-х часов единоразово. За такое время простоя он готов заплатить, например, миллион рублей. Если простой больше, то появляется заранее определённый штраф. Чем больше время простоя, тем этот штраф больше. Это понятные бизнесу категории. Более того — в такие же категории можно уложить даже утечку конфиденциальных данных.

Аналогично, например, строится обеспечение физической безопасности в банке. Банк не требует ту или иную экипировку сотрудников охранной фирмы, не диктует, как они должны быть вооружены. Это дело ЧОПа. Через некоторое время этот же подход будет актуален и для кибербезопасности.

Суть такого подхода заключается в том, что экспертиза подбора механизмов кибербезопасности выносится на сторону провайдера, который будет определять список сервисов и их технических SLA, чтобы обеспечить допустимое время простоя, требуемое время восстановления и др.

Конечно, такая модель применима не ко всем организациям. Некоторые компании федерального и транснационального масштаба предпочтут иметь высококлассного специалиста в штате. Однако для многих будет эффективнее передать экспертизу по выбору решений внешней компании, которая будет нести финансовую ответственность, в отличие от штатного сотрудника.

* * *

Можно прогнозировать, что такая модель потребления услуг кибербезопасности станет массовой года через 2–3. Сейчас же это только начинает обсуждаться профессиональным сообществом.



Дарья ОРЕШКИНА
директор по развитию
бизнеса Web Control

ЗАЩИТА САМОГО ЦЕННОГО

ИТ-БЕЗОПАСНОСТЬ СО СКОРОСТЬЮ БИЗНЕСА

Конец года — весьма подходящее время, чтобы отметить важные тенденции, которые наметились в деятельности киберпреступников и сфокусировать внимание на наиболее актуальных в отношении своей компании. Мегатрендами, по мнению исполнительного директора INTERPOL IGCI Нобору Накатани, остаются вирусы-вымогатели, атаки на финансовые учреждения и DDoS-атаки. Конечно, в фокусе злоумышленников остается получение денег. Не прекратятся и целенаправленные атаки, осложненные сокрытием следов. Компаниям потребуется надежно защищать критичные ИТ-активы.

Согласно отчету Group-IB — ведущей международной компании, которая занимается предотвращением и расследованием киберпреступлений и мошенничеств, в прошедшем году наиболее ярко отметились и имеют предпосылки повториться события:

1. Вирусы-вымогатели (шифровальщики) приводили к масштабным эпидемиям и также использовались для отвлечения внимания от основного инцидента и маскирования следов целенаправленных атак.

2. Атаки на критическую инфраструктуру, включая банки, производились уже не только для получения денег, но еще и с целью шпионажа или диверсий.

3. Новой целью атакующих стал процессинг производителей терминалов самообслуживания. Также атаковались банкоматы и карточный процессинг.

4. Злоумышленники регулярно использовали вредоносные программы, которые работают только в опе-

ративной памяти и исчезают после перезагрузки системы, что позволяет преступникам долго оставаться незамеченными.

5. Весьма актуален был почтовый фишинг.

6. Были атакованы оборудование клиентов банков и криптовалютные сервисы.

7. Вредоносный код активно выкладывался в открытый доступ, инструментарий для взлома существенно развивался.

Как выглядит критичный ИТ-актив для финансовой организации, ритейл, производственной, телеком компании или любой другой? Для каждой отрасли и организации он выглядит по-разному. Это может быть система, обрабатывающая важные данные в ЦОДе, автоматизированная/IoT-система, например, корпоративный транспорт с дистанционным мониторингом и контролем, подключенный к Интернету, это может быть точка продаж, банкомат или даже пользовательская рабочая станция. Все эти системы объединяет то, что стабильность их работы очень важна для жизнедеятельности компании и эти системы необходимо надежно защищать. Снижение производительности и простой business- или mission-critical систем, конечно же, должен сводиться к минимуму, а развитие вычислительных сред, позволяющих получать прибыль, требуется делать «со скоростью бизнеса».

Таким образом, подходящее средство защиты для наиболее критичных систем должно обеспечивать максимальную защиту от угроз, в том числе от новых уязвимостей и угроз нулевого дня. Оно должно быть гибким по архитектуре и покрывать потребности в защите для множества типов систем, легко раз-

вертываться и управляться. Безусловно, такое средство защиты должно оказывать минимальное влияние на производительность защищаемого объекта и должно давать возможность защищать как высоконагруженные кластеры, так и системы с ограниченными вычислительными ресурсами, с учетом, что зачастую такие системы не имеют подключения в общую сеть и тем более Интернет. И такое решение есть...

SYMANTEC DATA CENTER SECURITY AND CRITICAL SYSTEM PROTECTION

В аспекте защиты критичных ИТ-активов, решения Symantec Data Center Security: Server Advanced (SDCS: SA) и Symantec Critical System Protection (SCSP) различаются между собой преимущественно набором защищаемых платформ: SDCS: SA фокусируется на типовых для ЦОДов системах, а SCSP — на критичных IoT-системах (таких, как транспорт) и отдельно стоящих устройствах.

Как это работает? Принцип защиты основан на микросегментации, деэскалации административных привилегий, снижения критичности уязвимостей и очень важный момент — обеспечивается защита от угроз нулевого дня. Для сохранения целостности системы выполняется контроль приложений, служб/процессов и сетевых подключений, обращений к оперативной памяти и важным пользовательским файлам, блокируется состояние настроек системы и приложений. Главное отличие продуктов SDCS: SA и SCSP от антивируса заключается в том, что контентная проверка на основе сигнатур не выполняется, вся защита происходит

НА СОРЕВНОВАНИЯХ ХАКЕРОВ «CAPTURE THE FLAG» НА ЕЖЕГОДНОЙ КОНФЕРЕНЦИИ BLACK HAT В США SYMANTEC УЖЕ БОЛЕЕ 6 ЛЕТ ДЕМОНСТРИРУЕТ НАДЕЖНОСТЬ ЗАЩИТЫ СИСТЕМ ОТ ВЗЛОМА ПРИ ПОМОЩИ ТЕХНОЛОГИИ DATA CENTER SECURITY И CRITICAL SYSTEM PROTECTION

на основе детализированных политик доступа для каждого процесса, не нагружая сервер или embedded систему. Соответственно, регулярные апдейты сигнатурных баз не нужны, как и подключение к Интернету (рис. 1).

На соревнованиях хакеров «Capture the Flag» на ежегодной конференции Black Hat в США Symantec уже более 6 лет демонстрирует надежность защиты систем от взлома при помощи технологии Data Center Security и Critical System Protection. Каким же образом достигается успех? Разберем критичную систему на основные группы объектов защиты (рис. 2).

Для защиты в SDSC: SA и SCSP применяется целый ряд технологий. Для упрощения восприятия при знакомстве с этими решениями, мы сведем основные технологии в три группы и рассмотрим их.

Изолированная среда исполнения для системных служб и прикладных программ, контроль доступа к процессам и к оперативной памяти. Большинство известных системных приложений и служб имеют профиль поведения, который определен в шаблоне политик защиты. Для пользовательских приложений и служб можно создать свой собственный профиль поведения или использовать готовый из шаблона. Работает функционал создания пользовательского профиля по элементарному алгоритму:

- 1) запускается профилирование поведения пользовательского приложения/службы;

- 2) запускается пользовательское приложение/служба и производится сбор событий активности всех его процессов;

- 3) завершается профилирование, создается пользовательский профиль поведения и используется в политике.

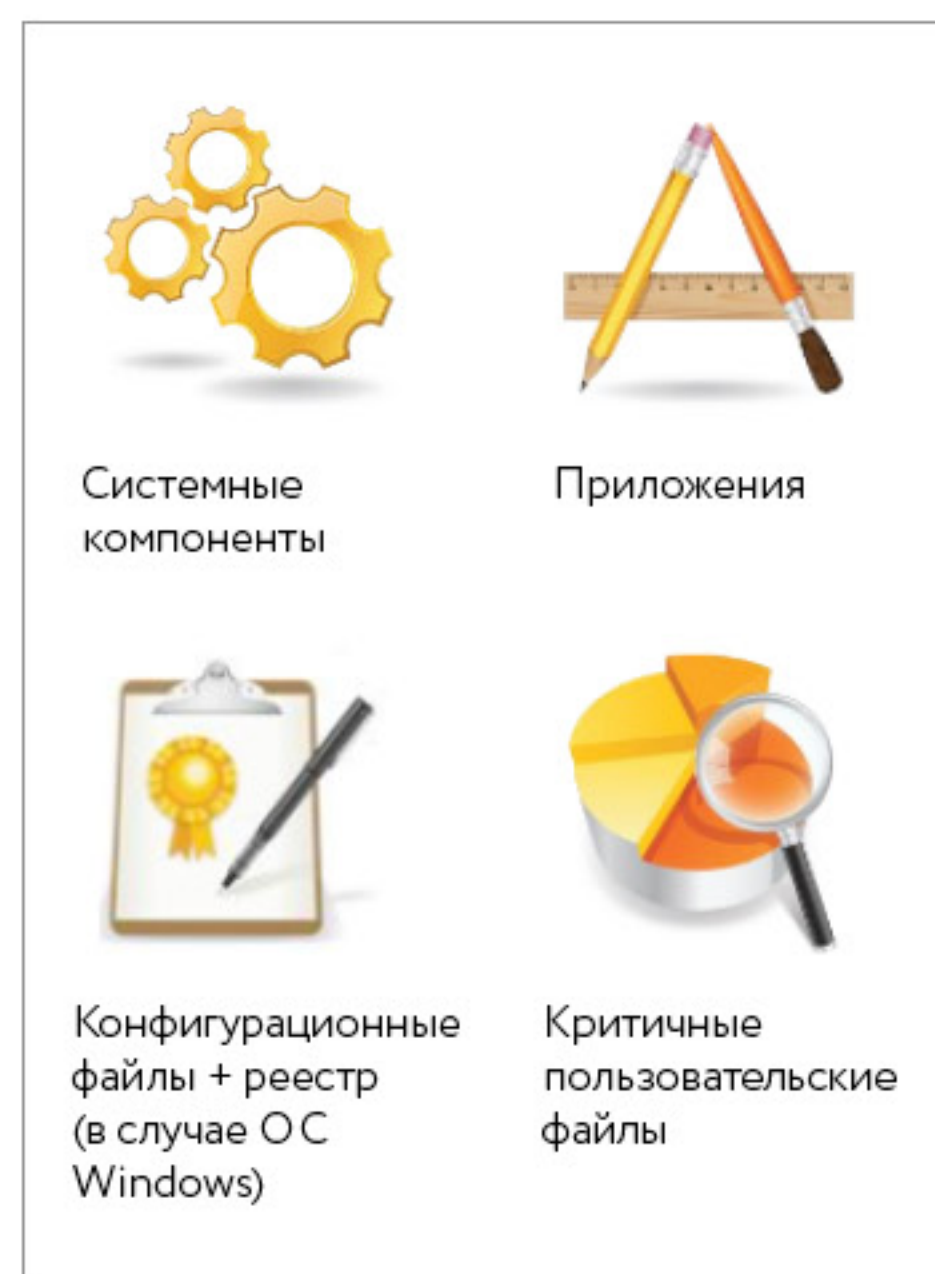


Рисунок 2

В будущем отклонения поведения пользовательского процесса/службы будут классифицироваться как вредоносная активность и блокироваться. Что немаловажно — все процессы получают лишь необходимые привилегии. Эта технология является ключевой, позволяет наиболее эффективно защищать любые системы и не требует регулярных обновлений и подключения к сети Интернет. Она позволяет защитить важную для бизнеса систему от новых угроз и снижает критичность установки патчей. Поскольку принцип работы изолированной среды и контроля доступа не подразумевает анализ контента, то потребность в ресурсах значительно ниже, чем для антивируса, что позволяет защищать высоконагруженные и ограниченные в вычислительных ресурсах системы. Именно благодаря этой технологии решения SDSC: SA и SCSP стабильно демонстрируют свою эффективность уже много лет.

Блокировка настроек и файлов конфигурации. Настраивается запрет на изменение файлов и реестра, а также подключение устройств. Даже если злоумышленник получит доступ к системе — изменить настройки он не сможет.

Хостовый фаерволл и IPS. Очистка сетевого трафика эффективно отсекает вредоносный код. Для сред Windows доступны готовые политики IDS и IPS «из коробки», которые отслежи-

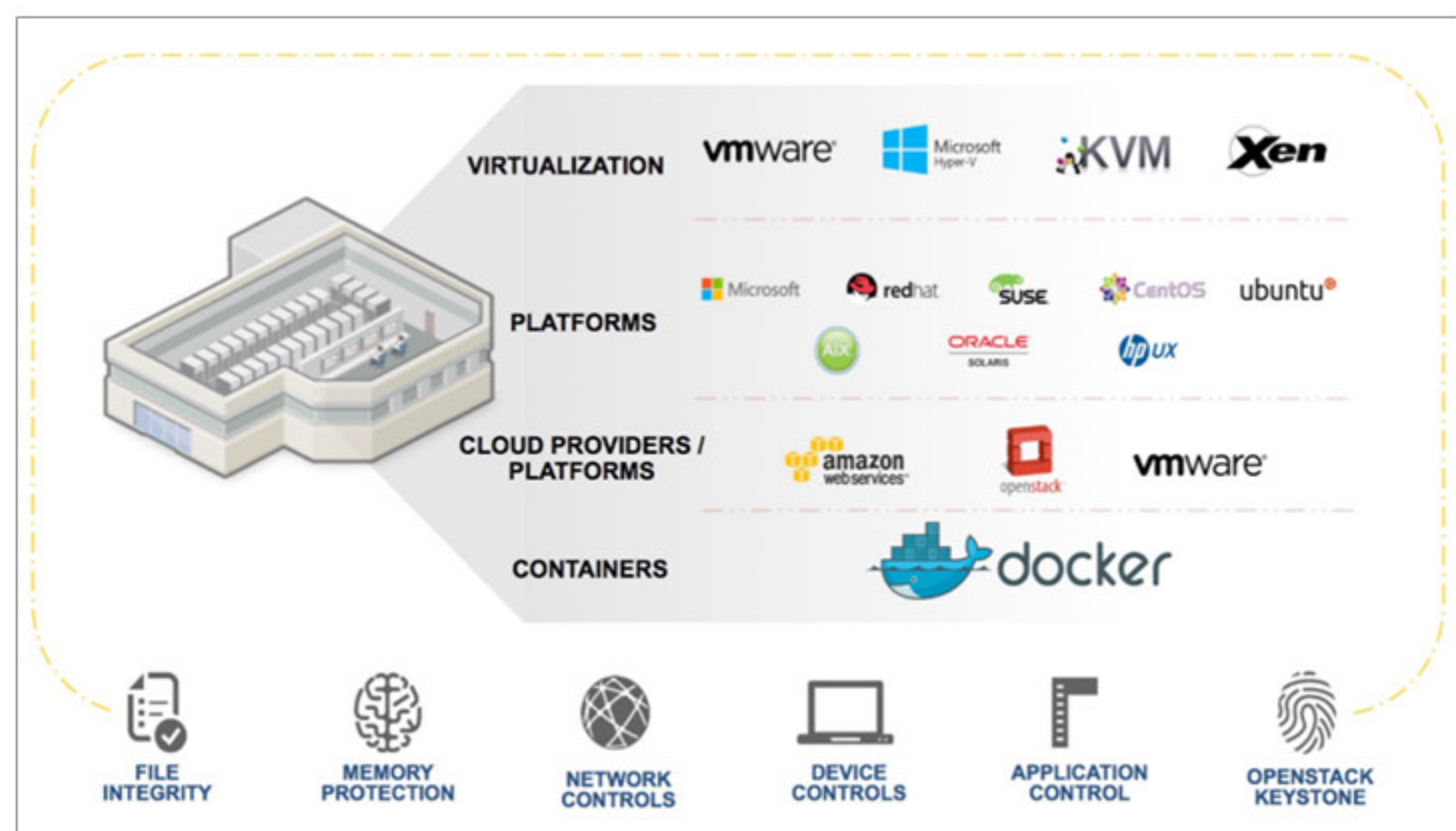


Рисунок 1

вают и предотвращают подозрительную активность.

Для виртуальных сред Windows при интеграции с VMware NSX, новые виртуальные машины становятся защищены уже сразу после создания, что существенно повышает скорость обеспечения безопасности систем.

С помощью SDSC: SA и SCSP вы сможете защитить подавляющее большинство платформ: физические и виртуальные сервера Windows, Linux, Unix-подобные системы, QNX RTOS, контейнеры Docker и embedded-системы.

ПРИМЕР ИСПОЛЬЗОВАНИЯ SYMANTEC CSP ДЛЯ БАНКОМАТОВ

Банкоматы являются важнейшим оборудованием и лакомым кусочком для киберпреступников. Эти системы предназначены для одной задачи, поэтому установка ПО и изменение настроек происходит редко, набор приложений заранее известен, системные ресурсы ограничены, а также необходимо обеспечивать требования стандарта PCI DSS. Представим в виде таблицы потребности в IT-защите для банкоматов и методы защиты (табл. 1).

* * *

Успехи в защите систем от взлома, которые демонстрирует ПО Symantec Data Center Security: Server Advanced и Symantec Critical System Protection на хакерских соревнованиях, вселяют оптимизм — эту группу решений уверенно можно назвать качественным звеном в экосистеме защиты, существенно поднимающим стоимость атак киберпреступников. На российском рынке это ПО успешно прижилось, однако, пока не имеет широкой известности. Эту несправедливость исправляет компания Web Control.

Угрозы и потребности в защите для банкомата	Метод защиты с помощью Symantec CSP
Заражение вредоносным кодом через сетевой трафик	Определение сетевой активности для приложений, запущенных в системе и защита от вредоносного трафика
Несанкционированная эскалация привилегий	Реализация принципа наименьших привилегий и блокировка внешних интерфейсов
Запуск вредоносного ПО	Блокировка запуска несанкционированных программ и разрешение исполнения только необходимых действий в системе
Заражение системы через память, хищение чувствительных данных через память	Защита от вредоносного кода, который вставляется в память или выполняется из памяти, защита от несанкционированного доступа к памяти
Реализация вредоносных сценариев путем переконфигурирования системы	Непрерывный мониторинг файлов настроек и реестра
Подделка файлов и системных компонентов	Мониторинг и контроль поведения приложений, блокировка настроек, белые и черные списки возможных действий
Несанкционированное копирование данных на подключаемые внешние устройства	Ограничение возможности подключения нежелательного оборудования (USB, DVD, SD)
Поддержка различных платформ, включая устаревшие версии ОС	Широчайший список поддерживаемых платформ: Windows, Linux, QNX, Unix-подобные, интеграция с VMware NSX для безагентской защиты
Централизованное управление профилем безопасности	Централизованное развертывание агентов и применение политик
Защита должна быть надежной, даже в условиях отсутствия периодических обновлений для системы защиты	В отличие от традиционного антивируса, базы сигнатур отсутствуют, система защиты не требует периодических обновлений
Ограниченные вычислительные ресурсы	В основе защиты не анализ контента, как в случае традиционных антивирусов, поэтому не создается повышенная нагрузка на систему; эффективная защита без применения сигнатурного анализа может применяться даже на ограниченных в ресурсах embedded системах

Таблица 1. Потребности в IT-защите для банкоматов и методы защиты

КАК МАРТЫН ИНФОРМАЦИЮ ЗАЩИЩАЛ



Мария ЛУРЬЕ
руководитель отдела маркетинга
ООО «С-Терра СиЭсПи»

СКАЗКА С ПОДСКАЗКОЙ ОТ С-ТЕРРА

Жил-был на свете инженер по информационной безопасности. В обычной жизни-то он был веселым, компанейским парнем, Мартышкой друзья называли, а на работе — серьезным и ответственным специалистом отдела ИБ крупного банка. Коллеги обращались к нему уважительно, Мартын Петрович.

Вызывает его однажды начальник и говорит:

— Придумай-ка, Мартын, как нам защитить информацию нашу, которой мы с филиалами обмениваемся. Только учти, с 1 января начнет действовать новый ГОСТ, что стандарты обеспечения безопасности банковских операций устанавливает. Так вот, требования его учесть надо. Да про импортозамещение не забудь — нынче все наше должно быть, российское, сертифицированное. Ну и цена важна, конечно — банк хоть деньгами и распоряжается, но попусту тратить их не любит. А структуру нашей сети ты и без меня знаешь — сам сможешь разные ситуации предусмотреть, где защита необходима. Да, чуть не забыл, ты предложения свои завтра к вечеру подготовь, иначе не видать премии в этом квартале ни тебе, ни всему отделу.

Вышел Мартын от начальника задумчивый. Впору, как в сказке про конька-горбунка, сесть, закручиниться и заплакать. Вот только конек не прискачет, волшебством дело не решит. Думал Мартын целый рабочий день, весь Интернет перевернул, на сайты разных производителей сходил, десятки решений

изучил. Особо пристально предложения российских вендоров рассматривал. К вечеру повеселел немного — нашлись несколько вариантов, как наказ начальника выполнить. Решил, что утром придет и подробно всё рассчитает, запросы в компании те отправит.

Пришел Мартын домой, поужинал, чайку крепкого заварил, да за компьютер снова сел — посмотреть перед сном новости, с друзьями пообщаться. И не заметил он, как задремал — устал ведь за день, понервничал, а дома тепло, спокойно, кот Баська на коленях мурлычет, пес Журка хвостом виляет — рад хозяина видеть. А на экране так и осталась картинка висеть — новость, которую Мартын читал. В новости той рассказывалось про то, как одно уникальное устройство канал супербыстрый защитило, да еще и между мощными ЦО Дами на огромном рас-

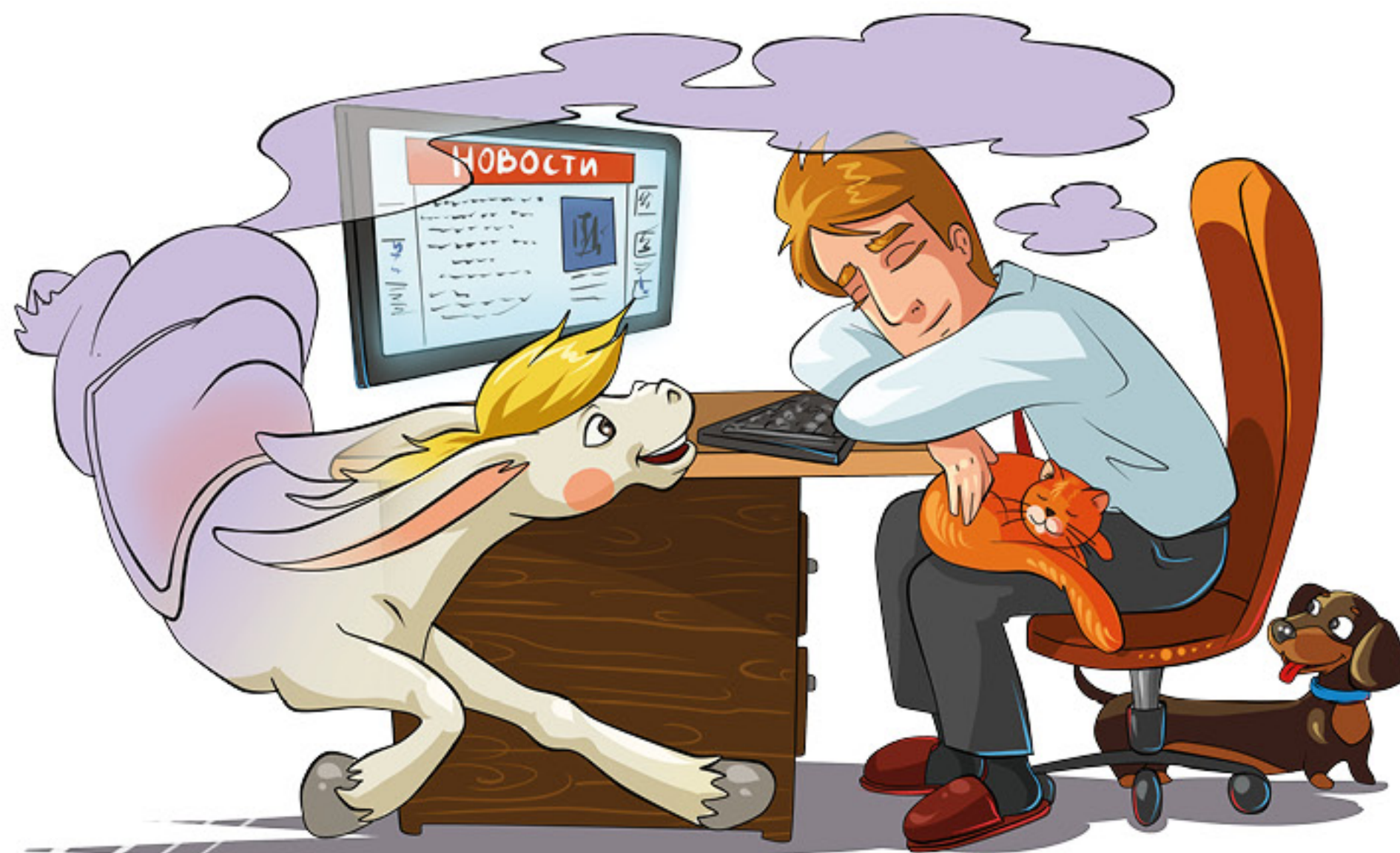
стоянии друг от друга. И так вдохновило его это событие, что задумался он, как можно для своего дела это решение применить... Думал-думал, да и уснул...

Спит Мартын и видит сон волшебный. Прискакал к нему во сне конек-горбунок и говорит:

— Не кручинься, Мартын, расскажи лучше, что тебя беспокоит?

— Ох, конёк, да как ты можешь мне помочь? — запричитал Мартын — Ведь нужно мне дело великое сделать — банковскую сеть компьютерную защитить, да надежно, да по стандартам, да еще и по цене разумно, да...

— Постой, Мартынка! Я понял, что ты в полной тоске и безысходности, но твоя задача — дело разрешимое. Садись верхом, и я отвезу тебя в такое место, где все тайны открываются, голова проясняется и любое решение находится.





Взобрался Мартын на конька-горбунка и поскакал. Не очень долго, но и не коротко ехали, и добрались они до небольшого, зеленого городка. Дома в том городке красивые, улицы широкие, люди улыбаются, а главное — лес кругом, даже дома среди деревьев стоят, будто прячутся. Остановился конек на небольшой полянке, спешился Мартын, огляделся. А конек как сквозь землю провалился — исчез.

От полянки две тропинки в лес убегают: одна в бор еловый, другая — в рощу березовую. Выбрал Мартын ту, что ближе всего ему показалась, будто сама под ноги стелилась. Идет, а ёлки вокруг всё плотнее, лес всё гуще, даже странно, что в городке такой лес оказался, но наш герой не придавал этому значения. Вдруг появляется перед ним девица лесная красоты неописуемой, в парчу и шелка заграничные одетая. За собой зовет, манит, улыбается, угощает яствами необыкновенными, обещает решение всех проблем и богатство в придачу. Не устоял перед её чарами Мартын (да и кто бы удержался?), и пошел за ней, позабыв и про свой отдел, и про премию квартальную, и про задание свое важное. Вдруг всё вокруг потемнело, жутковато стало, запах странный появился. Понял Мартын, что Кикимора перед ним, что заманила она его в ловушку, в болото, и что теперь ему обратный путь никогда не найти...

Вдруг из-за огромной ели два зверя выскакивают. Пригляделся, да это же

его кот Баська и пес Журка! Бросаются к нему, повизгивают радостно и галдят наперебой:

— Мартын, Мартын, мы нашли!!

— Что вы нашли? — спрашивает Мартын, а про себя отмечает, что даже не удивился как пес и кот человеческим голосом разговаривают, и как они вообще тут оказались.

— Решение нашли, — отвечает Журка, — для твоей задачи. Тут оно, рядом, через лесок только перейти.

Чудесным образом рассеялись чары, расступились суровые ели, стало светло и оптимистично. Вывели мохнатые друзья Мартына из чащи, повели по тропе в ближайшую березовую рощу.

А за рощей той большой терем виднелся, высокий, расписной. Зашли наши герои всей компанией в тот терем и увидели диво дивное: повсюду стойки серверные стоят, экраны светятся, провода змеями сворачиваются — и никого. Восхитился Мартын, кинулся всё рассматривать. То в один монитор заглянет — там система мониторинга строчками подмигивает, то в другой — там какой-то добрый молодец издали сведениями делится. На серверы поглядел и заметил надпись знакомую с красной точкой между букв (запомнил особый признак). Внимание обратил, что часть серверов как виртуальные машины работает, и подумал: «Ну всё, как у нас в банке! Чудо!». А на виртуальных машинах тех тоже защита стоит, шлюзы безопасности трудятся.

В радостном волнении поднялся Мартын на второй этаж терема. А там...! Диво пуще прежнего. Сплошной стеной экраны огромные стоят, да на каждом из них страны чужеземные — дальние и ближние. В каждой стране — по терему похожему, размером только чуть меньше. В каждом тереме экраны светятся, сервера жужжат, люди работают. А на каждом экране слова в уголке мерцают: «Защищенное VPN соединение. Стандарт». Аж зажмурился Мартын от такой невероятности!

А Баська уже тянет за полу кафтана (да-да, Мартын и сам не заметил, что в русское платье обряжен), зовет дальше идти. Последовал Мартын за своими верными друзьями на третий, самый верхний этаж терема. Комнатка там оказалась совсем небольшая, но светлая, тихая и уютная. За крепким деревянным столом человек сидит, чай пьет из блюдца, конфетами да баранками лакомится. К Мартыну ласково обращается:

— Присаживайся, Мартын, к столу, угощайся. Знаю, наш терем чудесный поразил тебя, спросить многое хочешь. Так вот, выпей чайку, отдохни, да и начинай расспросы. Но учти, прямо тебе ничего не скажу, только подсказку дам. А дальше — сам смекай.

Поблагодарил Мартын незнакомца за добрые слова, к столу подсел, чаю себе налил. Угощается, а сам хозяина рассматривает — кого-то тот ему напоминает. И только когда собеседник бороду свою теребить начал — понял, заулыбался — Хоттабыч перед ним, прав-



да, не старик совсем, а солидный такой мужчина.

Наконец, настало время вопросы задавать. Рассказал Мартын, что заинтересовало его в техническом оснащении терема, особо на разнообразие устройств безопасности внимание обратил, на защищенную связь с заморскими странами. Спросил про способ удаленного подключения, про систему управления чудную, про стандарты используемые.

Ответ Хоттабыча смутил Мартына. Сказал ему мудрый человек, что знает Мартын ответ на свои вопросы, видел он и решение готовое и средства подходящие, вот только уставший был — не запомнил. И дал Мартыну листок, пополам сложенный. Развернул его Мартын, хотел прочесть, ...

И проснулся.

Открыл глаза, а за окном рассвет уже, пора на работу собираться. Потянулся Мартынка — шутка ли, всю ночь проспал, сидя на стуле. Глядь, а перед ним на столе лист лежит, точь-в-точь, как Хоттабыч ему вручил. А на листке знакомым почерком (его собственным, потому и знакомым) написано: «Подсказка от С-Терра».

Успел Мартын решение в срок представить. Понравилось оно начальнику, он премию Мартыну Петровичу выписал, и весь отдел не обидел, все довольными остались.

ПОДСКАЗКА ОТ С-ТЕРРА

Не стоит далеко ходить, дорогой наш специалист по ИБ! Всё, что нужно для счастья и безопасности каналов связи твоей организации, ты сможешь найти в С-Терра.

Все решения проверены, надежны, стоят умеренно, а продукты сертифицированы и в Реестр Российского ПО включены. Инженеры и менеджеры любезные, расскажут всё и научат, если чего не умеешь.

Протоколы используем стандартные, IPsec (знаешь, конечно), интерфейс — cisco like (ты же знаток Cisco, признайся). Криптобиблиотеку — собственную, дополнительных лицензий не требующую, требованиям ГОСТ соответствующую.

А вот и конкретная подсказка, ассортиментная, нить путеводная по продуктам С-Терра, можно сказать:

- ◆ С-Терра Шлюз — для защиты сети банковской, причем любой топологии.
- ◆ С-Терра Клиент — для устройств пользователя предназначен. Можно удаленный доступ защитить, а можно и в офисе сотрудникам поставить. А если мобильную модификацию взять, так и смартфон по защищенному каналу письма слать будет.
- ◆ С-Терра Виртуальный Шлюз — тут гипервизор нужен. Любой. Потому и называется продукт так, что в виртуальной среде трафик защищает.
- ◆ Экспортные исполнения — да-да, есть и такие! Причем, и клиент, и шлюз, и виртуальный шлюз — все специально для экспорта предназначены.
- ◆ Российские универсальные устройства: ESR-ST и Zelax-ST — в одном небольшом криптомаршрутизаторе сразу 4 устройства спрятаны: маршрутизатор, коммутатор, VPN-шлюз и межсетевой экран.
- ◆ VPN-Модули к маршрутизаторам иностранным: Cisco и Huawei — и тоже с ГОСТ-криптографией, сертификаты имеются!
- ◆ С-Терра Шлюз 10G — специализированный VPN-шлюз для защиты высокопроизводительных каналов. Именно о нем был рассказ в том пресс-релизе, который Мартына в сказку увел. Уникальное устройство, новейшая разработка, тестирование прошедшая. Как раз для ЦОДов подойдет.

Решение есть! Действуй, звони и пиши: +7 (499) 940-90-61, sales@s-terra.ru



САЛЮТ НАД НЕВОЙ

PKI-ФОРУМУ РОССИЯ – ПЯТНАДЦАТЬ ЛЕТ!

В Санкт-Петербурге с 12 по 14 сентября прошла юбилейная — пятнадцатая — международная научно-практическая конференция — PKI-Форум Россия 2017. На нее съехались более 300 российских и зарубежных специалистов, чтобы обсудить актуальные проблемы, обменяться опытом и сопоставить точки зрения на основные вопросы развития инфраструктуры открытых ключей и электронной подписи.

Приподнятое — юбилейное — настроение позволило участникам оставаться активными все три дня, пропуская через себя несравнимо более плотный, чем в прошлые годы, поток информации. Этот феномен отметил

один из основателей PKI-Форума председатель его программного комитета Владимир Матюхин: «За пятнадцать лет сфера PKI выросла и возмужала, превратившись в самостоятельную отрасль. Поднимаемые сегодня проблемы по своему многообразию, сложности и остроте на порядок значительнее тех вопросов, ответы на которые мы искали на первых конференциях. Соответственно выросло и влияние PKI-Форума, его масштаб, наукоемкость и продуктивность. Сегодня это мощный и очень эффективный инструмент совершенствования отрасли. А дней в нем по-прежнему всего три».

Участники форума по заслугам оценили работу программного комитета, который на протяжении пятнадцат

ати лет самоотверженно трудился, год от года расширяя и совершенствуя программу конференции, поднимая ее на все более высокий уровень. Тепло и с уважением прошло чествование ветеранов отрасли, стоявших у истоков конференции: руководителя секции информационного права Института государства и права РАН И. Л. Бачило, представителя ФСБ И. В. Аристархова, советника Департамента проектов по информатизации Минкомсвязи А. А. Домрачева, заместителя генерального директора компании «Крипто-Про» И. А. Курепкина, члена-корреспондента Академии криптографии РФ, члена совета АЗИ Г. В. Емельянова, государственного советника РФ 1-го класса А. П. Курило.

Основная работа РКІ-Форума в этот раз велась по четырем направлениям: организационные вопросы, нормативное регулирование, международное сотрудничество и новые технологии. Активность представителей регуляторов — Минкомсвязи и ФСБ — позволила осуществить плодотворный диалог по каждому из направлений, не оставляя насущные вопросы «висеть в воздухе».

Одним из лейтмотивов конференции стала активность Минкомсвязи России, направленная на сокращении числа удостоверяющих центров. Выступлений по этому поводу было много. С одной стороны, в качестве аргументов приводились примеры европейских стран, где 3–5 УЦ вполне справляются со своими функциями, а также опасения по поводу роста числа мошенничеств с электронными подписями. С другой, речь шла об уничтожении масштабной работающей системы общегосударственного значения, последствия которого трудно представить. Немаловажным социальным аспектом в этом свете является угроза сокращения значительного числа рабочих мест квалифицированных сотрудников УЦ. Особое мнение выразил заместитель



В.Г. Матюхин, И.В. Аристархов и Р.В. Кузнецов

генерального директора АО ГНИВЦ А.П. Баранов. Он убедительно доказал, что такое сокращение числа УЦ в России в ближайшее время невозможно по организационным и технологическим причинам.

Позицию регуляторов со стороны Минкомсвязи России представили директор Правового департамента Р.В. Кузнецов и заместитель директора Правового департамента А.Ю. Кузне-

цов, со стороны ФСБ — И.В. Аристархов. Они подробно рассказали о текущей деятельности и планах регуляторов и успокоили представителей удостоверяющих центров: в ближайшее время сокращения не планируются, но тем не менее Минкомсвязь и ФСБ России продолжают работу по проверкам деятельности УЦ.

Вопросы нормативного регулирования отрасли были освещены с разных



АНДРЕЙ КУРИЛО, ГЛАВНЫЙ ЭКСПЕРТ КОМПАНИИ РНТ

— Я очень рад, что РКІ-Форум развивается и уже не ограничивается прикладной тематикой РКІ, а отслеживает, осмысляет более широкие тенденции, явления. С введением в массовый обиход электронного документа, заверенного цифровой подписью, возникают гражданско-правовые отношения, необходимость хранения таких документов, особенно много вопросов вызывает длительное хранение — и все это становится новой реальностью, с которой приходится иметь дело и государственным институтам, и миллионам обычных граждан.

Форум — это зеркало, в котором можно увидеть будущее и вовремя о нем подумать, определиться, принять своевременные решения. Например, слушая выступления коллег, в том числе из Европейского союза, вижу, как аккуратно, постепенно, но очевидно намечается тенденция отхода от тяжелых решений на уровне клиента в направлении хранения подписей в облаке. Или ФЗ-63. Явственно ощущается, что время требует пересмотреть наше отношение к нему, потому что изменилось наше мировоззрение, изменился окружающий мир. Этот закон был хорош для своего времени. Критиковать его нельзя, надо просто вносить коррективы, дорабатывать...

И вот это ощущение движения времени вызывает потребность переосмысливать ключевые сущности нашей отрасли. Не относиться к вопросу использования инструментария подписей как к решенному, стандартному, вполне понятному процессу, а видеть его в развитии, в контексте эволюционных жизненных процессов. Я буду рад и счастлив, если РКІ-Форум продолжит развиваться в этом направлении. Мне он интересен именно этим.

сторон. А. Ю. Кузнецов представил новые законопроекты от Минкомсвязи, старший научный сотрудник Института государства и права РАН Н. И. Соловьяненко выступила по теме «Законодательство об электронном документе как фактор актуализации правового пространства для цифровой экономики», главный специалист юридического отдела Федеральной нотариальной палаты Е. К. Волчинская подняла проблему многолетнего хранения электронных документов.

Темы международного сотрудничества и трансграничного пространства доверия РКІ были развернуто отражены в выступлениях коллег из Польши, Беларуси, Азербайджана и Эстонии. Выступили основатель Европейского форума по электронной подписи (ЕФРЕ) Анджей Бендиг-Веловейски, начальник отдела ИБ Департамента информационных технологий Евразийской экономической комиссии Ю. В. Хархордин, представитель Главного управления информационных технологий Федеральной таможенной службы РФ К. О. Романов, директор Департамента инфраструктурных решений Министерства информации Республики Казахстан Айрат Хайруллин, директор Центра сертифицированных услуг Министерства транспорта, связи и высоких технологий Азербайджанской республики Майылов Ариф Алескер оглы, учредитель компании BEST Solutions Яна Кримпе, руководитель НТК технологий информационного общества ОАО НИИАС А. А. Галдин, представитель АО «Грина-том» Н. И. Беленький и другие.

Новым опытом в истории РКІ-Форумов стал круглый стол «РКІ в блокчейн технологиях». Обсуждение про-



шло бурно, но в результате серьезных, продуктивных точек соприкосновения между РКІ и технологией распределенных реестров на данный момент выявлено не было. Заместитель председателя программного комитета РКІ-Форума С. А. Кирюшкин прокомментировал это так: «Блокчейн — технология новая, непредсказуемая, и тут очень важно держать руку на пульсе. В любом случае, теперь мы можем быть уверенными, что за этой темой мы следим, и как бы ни развивались события, мы ее не упустим. В этом собственно и состоит еще одна, наряду с другими, миссия РКІ-Форума».

Не менее полезными и содержательными были тематические заседания, дискуссионные панели и круглые столы, посвященные другим актуальным аспектам и проблемам отрасли. Особый интерес вызвало заседание «Доверенные сервисы на базе РКІ: нормативное, правовое и техническое обеспечение», которое тщательно подготовил и бле-

стяще провел академик Международной академии связи А. Г. Сабанов.

Стоит отметить, что статус юбилейного создал на форуме приподнятое настроение, которому организаторы — Медиа Группа «Авангард» — сумели придать завершенную яркую форму. Торжественный проход по Неве флотилии из семи кораблей с участниками конференции на борту, невероятный по своему размаху, разнообразию и продолжительности салют, юбилейный банкет с потрясающей программой... Каждый день форума завершался великолепным праздником.

Партнерами Форума выступили: АО «НИИАС», компании Кripto-про, Актив, ИнфоТеКС, ISBC, Газинформсервис, Gemalto и Линфо, Фонд содействия развитию безопасных информационных технологий, Ассоциация защиты информации и Ассоциация предприятий компьютерных и информационных технологий.





**АНДРЕЙ ГАЛДИН, РУКОВОДИТЕЛЬ НТК
ТЕХНОЛОГИЙ ИНФОРМАЦИОННОГО
ОБЩЕСТВА ОАО НИИС**

— Да, юбилейный РКИ-Форум получился выдающимся. Не говорю о праздничных мероприятиях, которые безусловно всем понравились, но рабочая часть тоже произвела впечатление. Масштабная, хорошо спланированная и организованная конференция. Полноценное представительство и по регуляторам, и по науке, и по производителям, разработчикам...

Что бросилось в глаза? Минкомсвязи стало серьезно закручивать гайки, повысило требования к удостоверяющим центрам и, конечно, комментарии регуляторов были очень востребованы. Напряжение зала чувствовалось — большинство дискуссий, круглых столов, где участвовали представители Минкомсвязи и ФСБ, так или иначе поворачивали обсуждение в сторону проверок и регулирования деятельности УЦ. И мне очень понравилось, что конфронтации не возникло, регуляторы очень терпеливо и довольно конкретно ответили почти на все — очень многочисленные — вопросы. Надо признать, на предыдущих форумах так было не всегда.

Также произвел впечатление необыкновенный, неподдельный интерес к новым технологиям. Обсуждались и мобильные технологии, и облачные, и даже блокчейн... Это означает, что отрасль не стоит на месте, идет в ногу со временем.

Мне лично был полезен доклад Евразийской Экономической комиссии, который впервые полно представил процесс межгосударственного взаимодействия в нашей сфере. Процесс этот очень непростой. Когда мы разрабатывали трансграничное взаимодействие для РЖД — в рамках одного бизнеса, где все партнеры заинтересованы в результате — проблем было очень много. Что касается межгосударственного взаимодействия, сложностей будет еще больше. Предстоит пересмотреть нормативную базу разных стран, предусмотреть массу юридических тонкостей, свести концы с концами... Но главное, картина, понимание уже имеется, созидательный процесс, будто железнодорожный состав от станции, уже двинулся и набирает ход.

**ТАТЬЯНА СТАНКЕВИЧ,
МЕНЕДЖЕР ПО
ПРОДУКТУ КОМПАНИИ
«ГАЗИНФОРМСЕРВИС»**

— Хочется сказать большое спасибо организаторам форума и пожелать его развивать. Собирать лучших экспертов, как в этом году, и много-много молодежи. Чтобы побольше новых идей, новых мыслей. А участникам желаю по максимуму использовать такую уникальную возможность общаться, учиться, взаимодействовать, придумывать и продвигать новое в нашей одновременно и такой сложной, и такой интересной отрасли.

Новые идеи — это не обязательно революция, разрушение старого. Некоторые считают РКИ устаревающей технологией, но это не так. Чем ее можно заменить? Блокчейном? Но обсуждение этой темы на форуме показало, что блокчейн — даже не альтернатива РКИ, не то что замена. А РКИ работает и совершенствуется больше 15 лет, на ее стороне опыт, сложнейшая юридическая база... Это технология с очень большим потенциалом, которая раскрывает свои возможности постепенно. И на форуме прозвучали выступления, которые показали, какие области РКИ еще совсем не охвачены.



**ВЛАДИМИР КУСТОВ,
ГЕНЕРАЛЬНЫЙ
ДИРЕКТОР «УЦ ГИС»**

— Было время, когда мне казалось, что у нас у каждого по семь жизней. Они как дни недели. Я прожил шесть из них и думал, что воскресенье наступило, а на самом деле еще работать и работать. И я пожелал бы нашему Форуму, чтобы в его истории не было воскресенья. Только работа.

Время течет неравномерно, и в жизни запоминаются именно те моменты, когда информация, события концентрируются, накапливаются, и время летит с огромной скоростью. Наш Форум — это ровно тот самый момент. И я благодарен тому, что эти три дня моей жизни пролетели как одно мгновение, и надеюсь, что через год это чудо повторится. И еще меня порадовало очень доброжелательное, заинтересованное отношение коллег друг к другу. Форум нас сплачивает, дает ощущение одного большого дела, одной команды. Спасибо.



INFOSECURITY RUSSIA 2017

ЕДИНСТВЕННАЯ В РОССИИ ВЫСТАВКА
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРЕВРАТИЛАСЬ В ПРОФЕССИОНАЛЬНЫЙ КЛУБ

В Москве в выставочном центре «Крокус Экспо» состоялась XIV Международная выставка по информационной и кибербезопасности InfoSecurity Russia. Она в очередной раз подтвердила свой статус авторитетного и масштабного события в жизни отрасли. Более сотни экспонентов продемонстрировали свои новые решения, актуальные внедренные проекты, поделились опытом разработчиков и пользователей, полученным за прошедший год.

Практически все компании-участники проводили на своих стендах презентации продуктов, семинары, мастер-классы, розыгрыши и викторины. Ведущие отечественные производители представили новейшие решения в коллективной экспозиции «Сделано в России», которая традиционно привлекла внимание государственных заказчиков и регуляторов отрасли.



Сенсацией выставки стали стенды ведущих производителей из Китая, которые демонстрировали инновационные решения и радостно делились опытом азиатских брендов. Китайцы участвовали в InfoSecurity Russia впервые, поэтому отбоя от посетителей не было.

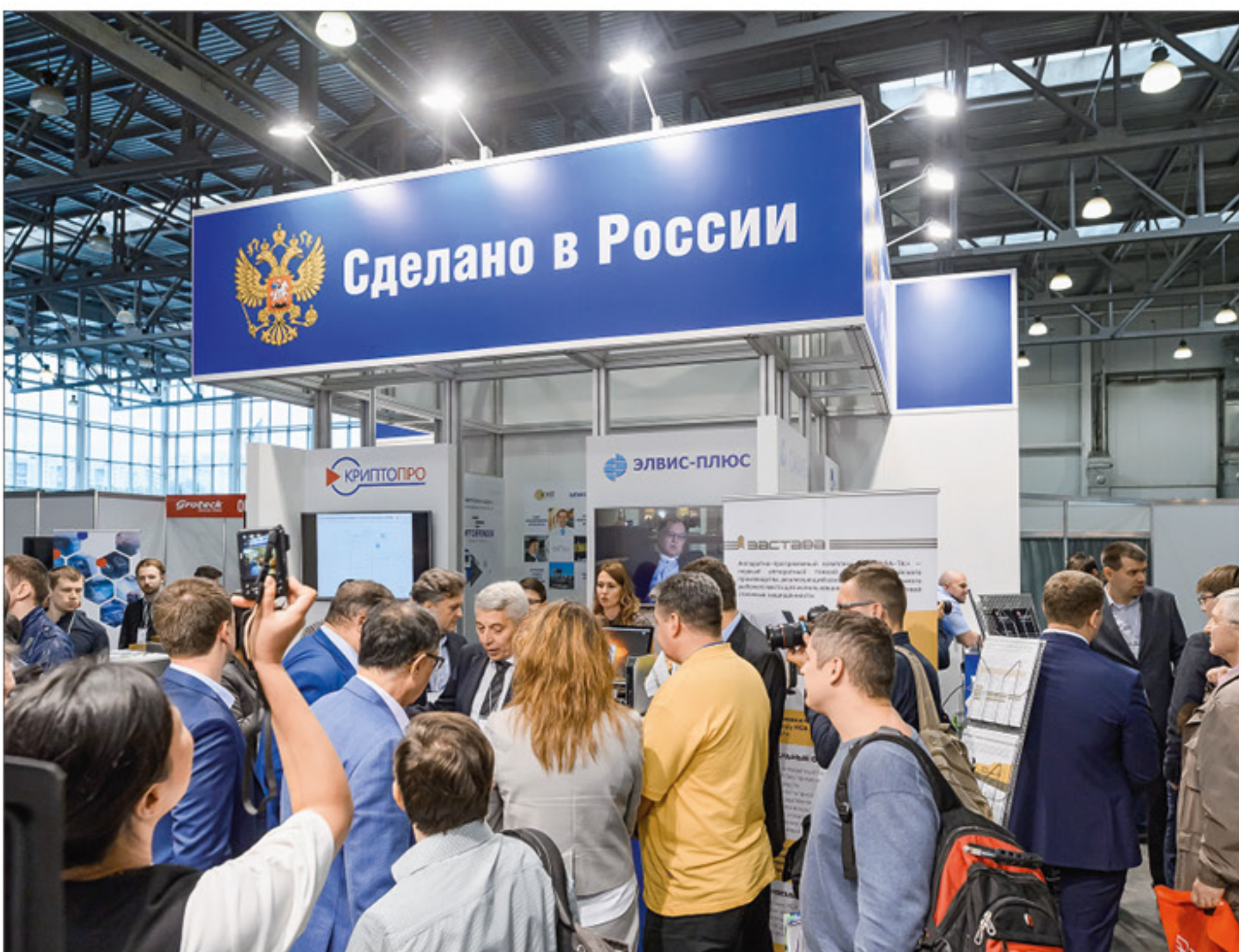
Традиционно богатой была конференц-часть выставки. Три дня в режиме нон-стоп проходили промышленные конференции, тематические секции, семинары, круглые столы, доклады и дискуссии. Выставка больше походила на профессиональный клуб, объединяющий руководителей и технических специалистов, производителей профильной продукции и разработчиков уникального ПО, представителей органов госрегулирования и ведущих предприятий страны.

Что обсуждалось? Солидный практический опыт, понимание тенденций рынка и знание продуктов и решений — далеко не полный перечень того, чем эксперты по информационной безопасности делились в своих выступлениях, на стендах и в кулуарных беседах.

День промышленного сектора провели Норникель, Вымпелком, Cisco, Газинформсервис, ЕВРАЗ, УЦСБ, Positive Technologies, АРСИБ. Говорили о защите инфраструктуры КВО, промышленном Интернете вещей, современных инфраструктурах обработки и защите данных, безопасности критической информационной инфраструктуры.

День финансовой безопасности объединил мероприятия Банка России, Ростелекома, Гознака, Wildberries, Газпромбанк. Среди обсуждавшихся животрепещущих тем: пресечение и расследование инцидентов в кредитно-финансовой сфере, противодействие DDoS-атакам. Особенное внимание привлекли следующие темы: «Эволюция безопасности: от натурального обмена к блокчейну», «Интернет вещей на финансовых рынках», «ИБ на предприятиях ритейла», «Пароль = Я: биометрические технологии».

День технологий поддержали СО ЕЭС, Cisco, Газпромбанк, WayRay, Anti-malware.ru, ANGARA Professional Assistance, R-Vision, Сбербанк. Зажигательные дискуссии, сравнения, оценки и реальные кейсы не оставили никого



равнодушными. Инвестиции в технологии: маркетинг и реальность. SOC против SIEM. Межсетевые экраны: защита приложений и защита от приложений... Захватывающим темам не было конца.

Не остались незамеченными и мастер-классы зарубежных экспертов. Одни только названия стали для них отличной рекламой: «Соблюдения законов о персональных данных в России» (Саймон Китс, THALES); «Стратегии

успешного участия бизнеса в кибербезопасности» (Allan Boardman); «Аналитика киберпреступности: алгоритмы» (Manjula Sridhar, ArgByte); «Возможность кибертеррористического нападения в Западно-Балканском регионе» (Зоран Живкович, Сербская ассоциация кибербезопасности); «Live Hacking: как хакеры взламывают ваши системы» (Sebastian Schreiber, SySS); «Про DDoS-атаки и киберпреступления» (Allan Guillen, Level 3 Communications).

ТАБУН ТРОЯНСКИХ КОНЕЙ



Валерий КУЛИКОВ
эксперт BIS Journal,
доктор технических
наук

BIS SUMMIT 2017 – О ТОМ, КАК НАМ РЕОРГАНИЗОВАТЬ
ИТ И ОБУСТРОИТЬ «ЦИФРОВУЮ ЭКОНОМИКУ»

Не все айтишники одинаковы. Такой вывод можно сделать после посещения X конференции BIS Summit. Его докладчики и модераторы дискуссий в выступлениях, комментариях и репликах, как правило, разделяли понятия «айтишник» и «безопасник» или «ибэшник». И это отличие не только внешнее, когда для первых характерны джинсы и свитера, а для дресс-кода «безопасников», по шутливому наблюдению Рустэма Хайретдинова

(представленного на форуме в качестве президента ассоциации BISA), до недавнего времени были характерны пиджаки и деловые костюмы. Глубинная разница между ИТ и ИБ в том, что философия ИТ до сих пор лучше всего передаётся содержанием анекдота, финальная фраза которого звучит приблизительно так: «С таким настроением ты слона не продашь!», а подход ИБ к внедрению ИТ сродни врачебному принципу «Не навреди».

Спикеры многих деловых публичных мероприятий сегодня напоминают гамельнского дудочника, влекущего бизнес-обывателя в опасную пучину того, что принято называть современными ИТ-технологиями. Слова «принято называть» написаны не случайно. Ибо многое из того, что превозносится, технологиями не является, представляя собой продукт, который с точки зрения нормальной инженерии не тянет и на результат НИР.

А вот трезвые и разумно консервативные взгляды докладчиков, мо-





дераторов и участников дискуссий BISS 2017 на сущность ИТ и их роль в экономике и обществе вселяют надежду на то, что рано или поздно разработка и внедрение ИТ перестанут быть бизнес-проектами и превратятся в системную деятельность по устройству рабочего пространства предприятий и организаций удобной безопасной рабочей средой и инструментами. При этом, по мнению Натальи Касперской, старые технологии не должны быть забыты. Это более чем разумное замечание да в уши бы тем, кто с энтузиазмом, достойным лучшего применения, тянет общество к электронным биометрическим паспортам, тотальным безличным денежным расчётам. В этом же ряду не слишком продуманных футуристических инициатив следует упомянуть и тягу к всеобщей «бимизации» строительства (от аббревиатуры BIM или Building Information Model (ling?)), при том, что в этой сфере (BIM) ещё горячи споры даже о терминах, а уж до нормальных стандартов представления данных и структуры моделей сто вёрст, да всё лесом.

На BISS пока не было слышно представителей строительной отрасли, однако, что касается биометрических ИТ и ИТ в медицине, участники пленарной дискуссии Михаил Петров и Илья Массух обратили внимание слушателей на возможные угрозы как для отдельных граждан, так и для страны в целом

в связи с несанкционированным доступом к упомянутым выше данным со стороны «частных» злоумышленников и заклятых партнёров. Речь шла в том числе и о том, что утрата медицинских данных может способствовать разработке этнического оружия.

Отрадным фактом является то обстоятельство, что, как отметила в ходе дискуссии Наталья Касперская, государство стало активно привлекать экспертов по информационной безопасности для выработки политики в сфере ИТ. При этом обращает на себя внимание то, что в терминологии экспертов по ИБ присутствуют как понятие «государство», так и «регулятор». Это, вкупе с уже упомянутым фактом обращения государства лицом к экспертам рынка ИБ, позволяет надеяться на наличие или, по крайней мере, на возникновение плодотворной конкуренции мнений, подходов и требований ИТ-бизнеса, государства, регуляторов и «безопасников».

ОТРАДНЫМ ФАКТОМ ЯВЛЯЕТСЯ ТО ОБСТОЯТЕЛЬСТВО, ЧТО, КАК ОТМЕТИЛА В ХОДЕ ДИСКУССИИ НАТАЛЬЯ КАСПЕРСКАЯ, ГОСУДАРСТВО СТАЛО АКТИВНО ПРИВЛЕКАТЬ ЭКСПЕРТОВ ПО ИБ ДЛЯ ВЫРАБОТКИ ПОЛИТИКИ В СФЕРЕ ИТ

Такое четырёхстороннее сотрудничество позволит перейти от этапа созревания ИТ к этапу их зрелого тотального внедрения. При этом слова «тотальное внедрение» в данном случае является не синонимом словосочетания «агрессивное административное внедрение», а синонимом термина «цифровая экономика».

Что же касается термина «зрелый», то это антипод понятия agile в разработке приложений. Манифест agile — это троянский конь анархии в ИТ. Практически официально закрепляемое этим манифестом пренебрежение документированностью программного кода вкупе с подвижностью рабочей силы и дистанционным аутсорсингом не позволяют гарантировать качество программного кода. То, к чему это приводит на уровне «цифровой экономики», наблюдалось при параличе фондовой биржи после обновления ПО, прекращении работы систем продаж авиабилетов.

СИТУАЦИЯ В СОВРЕМЕННОМ ПРОГРАММИРОВАНИИ НЕ УПРАВЛЯЕТСЯ ПО БОЛЬШЕЙ ЧАСТИ ЧЕМ-ТО ПОДОБНЫМ ISO 9000. БАЛОМ ЗДЕСЬ ПРАВИТ ИНТЕРНЕТ-БУМ И БУМ ПОТРЕБИТЕЛЬСКОЙ МУЛЬТИМЕДИЙНОЙ ЭЛЕКТРОНИКИ

Атмосфера разработки ПО в небольших компаниях неплохо иллюстрируется цитатой из статьи Владимира Татарчевского «Некоторые мысли по поводу программирования встроенных систем»: «...каждый программист работает фактически на тех инструментальных средствах, на которых хочет работать. ...Программисты в фирме не взаимозаменяемы. Мало того, что каждый программирует, на чем хочет, они еще ведут проекты в одиночку, и все нюансы проекта находятся у разработчика в голове...». Но и большие компании не безгрешны. Достаточно запастись попкорном, подождать очередного обновления Windows и почитать CNews.

Ситуация в современном программировании не управляется по большей части чем-то подобным ISO 9000. Балом здесь правит Интернет-бум и бум потребительской мультимедийной электроники. А это приводит к тому, что анализ текстов программ, если таковой оказывается возможным провести, не позволяет достоверно определить, является ли данный фрагмент кода «багом» или «фичей» (как образно подметил Рустэм Хайретдинов).

Приёмы и средства создания качественных безопасных программ должны быть тесно связаны с обеспечением для разработчика полного, прямого и неограниченного доступа ко всем возможностям аппаратной платформы. Тогда как многие современные языки, платформы и средства разработки абстрагированы от аппаратного обеспечения. Это хорошо для agile-программирования, но плохо для ИБ.

Стало быть, намереваясь создавать «цифровую экономику», для ИТ-платформ которой понятие информационной безопасности — это не надстройка или внешняя броня, а органично встроенная в них «иммунная система», следует сначала создать адекватные вызовам ИБ базовые аппаратно-программные средства для построения «цифровой экономики». И в связи с этим нельзя согласиться с мнением Ильи Массуха о том, что мы уже не успели «вскочить на поезд» в том, что касается разработки «железа». Нет, мы успели сделать это в своё время, но, к сожалению, лет 20 простояли на запасном пути по известным причинам.

Тем не менее, у страны есть потенциал, отечественными «айтишника-

ми» накоплен (хотя и не без перекосов) определённый опыт в «песочницах» Wintel и Open Source, и в коалиции с естественными партнёрами нашей страны (буде на то политическая воля прорабов «цифровой экономики») вполне возможно создание фундамента «цифровой экономики» без тех «мин и подкопов», о наличии которых свидетельствуют многочисленные международные перепалки на тему кибербезопасности. О таком возможном плодотворном сотрудничестве с заинтересованными партнёрами сочла необходимым упомянуть на BISS 2017 Наталья Касперская. Ну а более подробно о приоритетах в построении фундамента «цифровой экономики» было рассказано в докладах начальника управления информационных технологий «Сургутнефтегаза» Рината Гимранова и ИТ-директора ООО «СтройГазКонсалтинг» Гаральда Бандурина, выступившего на конференции в качестве председателя наблюдательного совета itSMF России.

В целом BISS 2017 явился комфортной площадкой для обмена экспертными мнениями по актуальным вопросам построения безопасной ИТ-инфраструктуры для бизнеса и производства. На выставке при конференции были представлены отечественные продукты для решения целого ряда частных вопросов ИБ, включая предотвращение утечки данных. И хотя функциональные возможности некоторых продуктов заставляли вспомнить самые мрачные предсказания Оруэлла, будем жить.





SKOLKOVO CYBERDAY 2017

НОВЫЕ УГРОЗЫ СУЩЕСТВУЮТ, НО ЕСТЬ ЛИ
НОВЫЕ РЕШЕНИЯ?

Анонсы сколковской конференции, посвящённой проблемам киберугроз, сулили перспективы открытия в ходе мероприятия новых решений для борьбы с растущими угрозами. Но надежды на открытие не оправдались.

В качестве новых угроз доклады представили «армии умных ботов» (именно так, умных без кавычек), «ещё не найденные уязвимости» и «искусственный интеллект». Последний, как

оказалось, мог выступать в двух ипостасях — и как новая угроза, и как система для поддержки инновационных средств киберзащиты.

Однако можно ли упомянутые выше элементы пространства киберугроз считать действительно новыми угрозами?

Ну, за исключением искусственного интеллекта, который, впрочем, пока толком никто не видел. Да, отдельные его проявления известны. В их числе посрамление шахматных гроссмей-

стеров и «гроссмейстеров» воздушных боёв. Но за триумфом этих машинных интеллектов в узких областях человеческой деятельности стоит огромный опыт в этих сферах интеллекта человеческого. Поэтому использование artificial intelligence в качестве новой возможности для противодействия киберугрозам требует предварительной детальной проработки моделей этих угроз и моделей их отражения интеллектом природным.



Что же касается армий «умных» ботов и ещё не найденных уязвимостей, то эти угрозы вряд ли можно назвать новыми. Особенно последние, упоминание о которых навеивает аллюзии на неуловимого Джо.

А появились ли новые возможности в свете этих пусть и не новых, но серьёзных угроз?

НОВЫЕ ВОЗМОЖНОСТИ ИЛИ ЗАСТАРЕЛЫЕ ПРОБЛЕМЫ?

Полагаю, что вряд ли сегодня можно говорить о новых технических возможностях для борьбы с киберугрозами для нашей страны в свете таких требований программы «цифровая экономика», как:

- ♦ использование российских технологий обеспечения целостности, конфиденциальности, аутентификации и доступности передаваемой информации и процессов ее обработки;

- ♦ преимущественное использование отечественного программного обеспечения и оборудования; ...

Ведь сегодня, как следует из материалов конференции, создатели оригинальных российских средств защиты информации, защищённых многочисленными патентами, вынуждены работать над своими продуктами:

- ♦ на зарубежном «железе», в которое интегрированы недокументированные для большинства пользо-

вателей возможности управления оборудованием;

- ♦ в условиях работы этого «железа» под управлением клонов ОС Windows, недостатки, недоработки и нестабильность которых настолько на слуху, что не нуждаются в комментариях;

- ♦ учитывая необходимость сосуществования специализированных средств защиты информации с созданными сторонними компаниями антивирусами «общего» назначения, принципы работы которых могут вступать в противоречие со специальными политиками ИБ, под которые заточены упомянутые специализированные средства защиты информации (уф, сложная фраза, но ведь и условия работы нелёгкие).

Возможность появления новых коммерческих продуктов и технологий для защиты от киберугроз обуславливается возможностью проведения значительного объёма испытаний и проверок «в поле». Зарубежные ИТ- и ИБ-компании имеют такие возможности, ибо ими контролируются существенные куски рынков, на которых используются корпоративные, банковские и промышленные киберсистемы, а многие из компаний за время своей жизни в десятки лет стали масштабными транснациональными корпорациями с многомиллиардными оборотами и практически неограниченной финансовой поддержкой.

Отечественные же специализированные ИБ-компании — это малый и средний бизнес, и они объективно не способны тягаться с зарубежными вендорами по части объёмов внедрений и финансами в условиях «свободного» рынка. Слово «свободный» взято в кавычки в связи с целым рядом обстоятельств, в числе самых свежих из которых — препоны, чинимые «Лаборатории Касперского».

В связи со сказанным отечественная реальность такова, что головным экспертом в области ИБ сегодня в нашей стране выступает фактически Сбербанк, хотя для него это далеко не профильная деятельность. Но поскольку его объёмы транзакций обязывают к особому соблюдению ИБ-гигиены, а финансовые ресурсы позволяют это делать, то положение обязывает.

НОВОЕ КАК ХОРОШО ЗАБЫТОЕ СТАРОЕ ПЛЮС ВУОД

Собственно роль и место конкретно Сбербанка в области штатных и инновационных разработок по части кибербезопасности — это лишь верхушка айсберга проблем, связанных с диспропорциями в практике отраслевого внимания к проблемам киберугроз.

В повестке дня конференции Skolkovo Cyberday 2017 была лишь небольшая секция «Реальность и практика ИБ в АСУ ТП», которая представляла ма-

лую толику проблем, связанных с киберугрозами отечественной промышленности.

И только банковская отрасль удостоилась отдельного блока условного пленарного заседания в т.н. Большом зале. Но при этом и здесь темы докладов лишь с большой натяжкой можно считать представлением новых возможностей в свете новых угроз.

«Цифровая трансформация и безопасность». Эта тема в её сущностном содержании и применительно к финансовым организациям и телекому обсуждалась ещё лет 15 назад на многочисленных «частных» конференциях компаний Sun Microsystems (чьё наследие сегодня с выгодой для себя и пользой для заказчиков использует Oracle), Intel, HP, IBM и прочих Fortune-лидеров.

«От реактивного к проактивному». Любимая тема экспертов HP в начале 2000-х применительно к «адаптивному предприятию». Вряд ли кому-то надо доказывать преимущество проактивного реагирования на любые угрозы для бизнеса, будь то угрозы конкурентоспособности бизнеса из-за детских болезней роста ИТ-инфраструктуры или киберугрозы в терминологии и понимании Skolkovo Cyberday 2017.

По-настоящему новая тема на пленарном заседании «Ключевые проблемы кибербезопасности банковской отрасли» — это мобильный банкинг и угрозы, связанные с этой услугой, являющейся одной из граней BYOD-революции. Возможности Bring Your Own Device — это сегодня один из маркетинговых локомотивов лидеров ИТ-индустрии в деле повышения своих доходов и нарастающая головная боль для служб ИБ.

В связи с этим уместно упомянуть, что в одном из малых залов на секции «Истории успеха резидентов Сколково» был представлен доклад об исследовании технологии голосовой идентификации в качестве одного из средств обеспечения безопасного дистанционного обслуживания клиентов банка. И участие Сбербанка в этом пилотном проекте оказалось вполне ожидаемым. При этом доложенная биометрическая технология ещё далека от коммерциализации, т.к. требует и дальнейшей ве-



рификации, и поддержки со стороны законодателей.

Резюмируя личные впечатления от содержательной части докладов на конференции Skolkovo Cyberday 2017, не могу вспомнить представления на ней чего-то действительно прорывного, достигшего очевидного коммерческого успеха и признания. На пленарных заседаниях речь шла скорее об уже известных или предполагаемых проблемах, и мероприятие в этой части носило просветительский характер.

В перспективе полезно расширение секционного раздела конференции в части рассмотрения большего числа отраслевых проблем и представления подходов для их решений. При этом на пользу делу пойдёт увеличение времени для обсуждения докладов, возможно за счёт более тщательного отбора самих докладов.

ВМЕСТО ЭПИЛОГА

Лицо конференции определяется авторитетом конкретных организаторов, уровнем докладов, местом и организацией проведения. Авторитет Сколково не требует комментариев, ряд докладчиков (личностей и компаний) на Skolkovo Cyberday 2017 широко известны на отечественном рынке ИБ и пользуются авторитетом у заказчиков.

Но вот проведение конференции, посвящённой столь сложным вопро-

сам, как новые угрозы и новые возможности в области кибербезопасности, в одном из углов огромного ангара, пусть и весьма хай-течного вида, вряд ли можно считать идеальным решением. И с точки зрения акустики, и температурного режима, и просто комфорта, особенно в части вида и содержания мест общего пользования. Последнее особенно недопустимо в связи с присутствием на конференции большого числа людей студенческого возраста, взгляды которых на то, что такое хорошо, а что такое плохо, находятся в стадии формирования.

Не способствовало полному погружению в тему и совпадение по времени ряда пленарных докладов и всех секционных выступлений.

Хорошим тоном при проведении конференции всегда являлось предоставление участникам тезисов докладов. Сегодня это сделать особенно просто по сравнению с временами исключительно бумажного документооборота. В связи с этим хотелось бы выразить надежду на предварительное знакомство с тезисами хотя бы на будущих конференциях Skolkovo Cyberday, а также на оперативное получение презентаций после проведения этих мероприятий.

КАК ПОВЫСИТЬ?

ГЛАВА 2. КАК ДЛЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ ОСВЕДОМЛЁННОСТИ ПЕРСОНАЛА ЗАРУЧИТЬСЯ ПОДДЕРЖКОЙ РУКОВОДСТВА

(Продолжение. Начало в № 3/2017)

Продолжая серию статей об опыте реализации программ повышения осведомлённости персонала в области информационной безопасности (далее часто будем говорить просто — повышение), обратимся теперь к ряду частных, но весьма важных на практике вопросов. Напомним: в наших статьях мы предполагаем, что читателя уже не надо склонять к пониманию необходимости и полезности повышения — статьи не содержат одобренных разного качества статистикой аргументов в пользу тезиса о том, что программа повышения осведомлённости является неотъемлемым компонентом системы обеспечения информационной безопасности любой современной организации. Мы надеемся, что читатели (многие из которых, вероятно, являются руководителями ИТ/ИБ-подразделений) уже решили для себя этот вопрос.

Итак, необходимость создания и реализации программы повышения осведомлённости ответственным за обеспечение информационной безопасности осознана. И почти сразу с деятельным воодушевлением и желанием немедленно начать повышать эту самую осведомлённость приходит понимание, что в одиночку ИТ/ИБ-подразделению де-

лать ничего нельзя. Или, хуже того, никто ничего сделать не даст.

В предыдущей статье мы говорили о том, что одним из наиболее важных факторов успеха любой программы повышения осведомлённости является её поддержка (а лучше — формальное санкционирование) высшим руководством организации. В большинстве случаев следствием такой поддержки является выделение необходимых программе ресурсов — финансовых, человеческих и материальных. Верно и обратное: нет поддержки высшего руководства — нет и денег на реализацию программы, а вы завалены другой работой так, что про повышение осведомлённости некогда даже вспомнить!

Давайте рассмотрим, как наименее болезненно и наиболее эффективно можно решать жизненно важный для самой идеи повышения осведомлённости персонала вопрос: как заручиться поддержкой руководства?

Задача эта, по нашему опыту, для многих ИТ/ИБ-руководителей является нетривиальной, поскольку обычно условия таковы:

♦ ранее в организации сколько-нибудь значимая работа по повышению осведомлённости персонала не велась (а значит, нет ни опыта обоснования затрат, ни опыта отбора и привлечения квалифицированных ресурсов);

♦ руководство не является осведомлённым в отношении современного состояния информационной безопасности, киберугроз и их последствий, зато хорошо считает деньги (что, без сомнения, есть часть его работы), а потому ко всем новым причинам роста затрат априори относится как к чему-то с недоказанной (и трудно доказуемой) целесообразностью.

ОБЩИЙ ПОДХОД: ДУМАЙТЕ КАК МАРКЕТОЛОГ

Необходимо «продать» повышение осведомлённости руководству, поэтому придётся какое-то время побыть маркетологом, обычная работа которого заключается в привлечении внимания потенциальных покупателей к товару и склонения оных к покупке. Мы умышленно не говорим здесь «действовать как маркетолог», потому что как раз действовать лучше в рамках существующих корпоративных правил.

Из необходимости думать как думают маркетологи следует, что:

1. Необходимо хорошо знать «товар» — вы сами должны понимать, знать и полностью отдавать себе отчёт в том, что, сколько и, главное, почему (зачем) вам нужно от руководства для программы повышения осведомлённости;

2. «Продавать» следует не саму программу повышения, а целевой образ (состояние) организации после того, как программа будет реализована — и вы и руководство должны хорошо представлять, какими должны быть результаты реализации программы;

3. Вероятность «покупки» существенно возрастёт, если вы будете использовать «язык», понятный «покупателю». Если представление программы будет изобиловать ИТ/ИБ-спецтерминами и излишне мелкими деталями, не уделяя внимания интегральному эффек-

**РУКОВОДСТВО НЕ ЯВЛЯЕТСЯ
ОСВЕДОМЛЁННЫМ В ОТНОШЕНИИ
СОВРЕМЕННОГО СОСТОЯНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ,
КИБЕРУГРОЗ И ИХ ПОСЛЕДСТВИЙ,
ЗАТО ХОРОШО СЧИТАЕТ ДЕНЬГИ**

ту воздействия на организацию (снижение рисков несоответствия требованиям, сокращение прямого и косвенного ущерба и т.п.) и ключевые показатели её деятельности (деньги, время, лояльность клиентов и т.п.), желаемой цели достигнуть будет весьма трудно.

ЗНАЙТЕ «ГОЛОВНЫЕ БОЛИ» СВОЕГО РУКОВОДСТВА

Давно известный, но часто забываемый и требующий определённой сноровки метод — встать на сторону оппонента и посмотреть на ситуацию его глазами. Это всегда полезно. Кроме того, у вашего руководства может быть своё руководство — попытайтесь понять, что оно требует от вашего руководства, какие цели ставит. Это поможет определить, о чём у вашего руководства «болит голова» и даст возможность лучше адаптировать к текущей ситуации идею инициации программы повышения осведомлённости.

ПОКАЖИТЕ РУКОВОДСТВУ ЕГО ЛИЧНУЮ ВЫГОДУ

Руководство — тоже люди. Поэтому оно непременно должно увидеть собственный интерес и выгоду от реализации программы повышения осведомлённости персонала. Данный совет, конечно, сильно коррелирует с предыдущим. Однако, не забывайте и про личные (т.е. не рабочие) интересы и выгоды руководства: обычно это люди среднего или старшего возраста, часто совершающие поездки, имеющие взрослых детей и, как правило, использующие современные модели сразу нескольких устройств. Показать руководству на его личном примере, что даст каждому сотруднику организации программа повышения — весьма неплохой аргумент. Однако, опять же, здесь важно не только что вы расскажете руководителю, но и как вы это будете рассказывать: ваш рассказ должен быть кратким, по сути и фокусироваться на наиболее острых проблемах.

НАЧИНАЙТЕ ЗАРАНЕЕ, ПРОДОЛЖАЙТЕ ПЕРИОДИЧЕСКИ

Всё новое часто воспринимается негативно — такова особенность человеческой психики. Поэтому если вы уже

ФАКТИЧЕСКИ ВАМ ПРИДЁТСЯ ЗАНИМАТЬСЯ ПОВЫШЕНИЕМ ОСВЕДОМЛЁННОСТИ РУКОВОДСТВА О ПОВЫШЕНИИ ОСВЕДОМЛЁННОСТИ С ПОЛНОЦЕННЫМ ПРИМЕНЕНИЕМ УПОМЯНУТЫХ В ПРЕДЫДУЩЕЙ СТАТЬЕ ПРАКТИК

приняли идею повышения, а ваше руководство всё ещё понятия не имеет ни об эволюции вашего мировоззрения, ни даже о том, что такое повышение осведомлённости и зачем оно нужно, то необходимо учитывать инерцию мышления руководства и его занятость (здесь под занятостью мы понимаем обычный режим работы руководителей — быстрое переключение с вопроса на вопрос при малом удельном времени рассмотрения каждого из них). Первое упоминание о повышении и связанных с ним нуждах в разговоре с руководством должно иметь место задолго (в некоторых сложных случаях — за год и больше) до желаемого действия с его стороны. Например, принципиального одобрения начала реализации и выделения необходимых ресурсов. Затем периодически напоминайте об идее, постепенно детализируя её контуры и наполнение. Фактически вам придётся заниматься повышением осведомлённости руководства о повышении осведомлённости с полноценным применением упомянутых в предыдущей статье практик (должное документационное обеспечение, правильные материалы для правильной аудитории, периодичность).

ИСПОЛЬЗУЙТЕ РЕЛЕВАНТНЫЕ АРГУМЕНТЫ

Часто используемый метод обоснования — «подкладывание» статистики в пользу обосновываемого тезиса — употребим и в нашем случае. Применять его, однако, необходимо со вниманием:

♦ *Источник статистических данных не должен быть ангажирован.* Применительно к повышению это условие соблюсти достаточно трудно, поскольку

большинство замеров и опросов проводится именно компаниями, оказывающими услуги в области повышения осведомлённости.

♦ *Статистика должна отражать отраслевую специфику организации.* Программы повышения осведомлённости не инвариантны по отношению к отрасли и должны отражать отраслевую специфику организации. А значит, оперировать статистикой по металлургической отрасли в банке следует с должной осмотрительностью.

♦ *Постарайтесь продемонстрировать количественные данные, характеризующие эффективность программ повышения осведомлённости.* При том, что объективных таких данных крайне мало. Это связано и со сложностью проведения подобных замеров, и с ещё пущей сложностью выбора подходящей методики анализа их результатов, и с «чувствительностью» темы. В то же время демонстрация реальных кейсов с известным эффектом реализации программы повышения осведомлённости может быть сильным аргументом в диалоге с руководством.

* * *

Упомянутые в нашей статье рекомендации достаточно высокоуровневые, однако, более подробные советы возможны лишь при изучении особенностей конкретной ситуации. Между тем высказанные рекомендации основаны на опыте компании UBS выполнения проектов по повышению осведомлённости и действительно помогут вам сократить путь до создания и реализации эффективной программы повышения осведомлённости персонала.

ПУТЕВКА В ЖИЗНЬ

О СРЕДНЕМ ПРОФЕССИОНАЛЬНОМ
ОБРАЗОВАНИИ В СФЕРЕ ИБ



Марина БРОДСКАЯ
обозреватель BIS Journal

Во времена позднего СССР школьников, чье поведение и успехи в учебе отрицательно сказывались на показателях учебного заведения, запугивали отчислением в профессионально-технические училища. Профессии токаря, слесаря, повара или парикмахера были не в чести у учителей средней школы. Со временем ПТУ превратились в колледжи, принципиально обновился список профессий, и теперь в заведениях среднего специального образования готовят, в том числе, и специалистов по информационной безопасности. Но знают об этом далеко не все работодатели.

ОБРАЗОВАТЕЛЬНЫЕ СТАНДАРТЫ

Летом 2010 г. Министерство образования и науки РФ утвердило приказ

№ 708 «Об утверждении и введении в действие государственного образовательного стандарта среднего профессионального образования по специальности 090305 «Информационная безопасность автоматизированных систем». Аналогичные стандарты среднего профессионального образования (СПО) были приняты по специальностям «Информационная безопасность» (090100) и «Информационная безопасность телекоммуникационных систем» (090303).

В 2014 г. был принят федеральный государственный образовательный стандарт (ФГОС) по специальностям направления ИБ и 090305 был заменен на 10.02.03 «Информационная безопасность автоматизированных систем». Также были приняты новые ФГОС по другим направлениям ИБ: 10.02.01

«Организация и технология защиты информации»; 10.02.02 «Информационная безопасность телекоммуникационных систем»; 10.02.04 «Обеспечение информационной безопасности»; 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Так или иначе, обучение по направлению ИБ началось в колледжах и техникумах России с 1 сентября 2010 г.

СКОЛЬКО УЧАТ

Стать техником по защите информации можно, проучившись 3 г. 10 мес. при поступлении в колледж на дневное очное отделение после 9 класса или 2 г. 10 мес. на базе 11 классов. В образовательную программу включено освоение дополнительной профессиональной программы «Оператор ЭВМ».

МНЕНИЕ ИБ-СООБЩЕСТВА

Готовя этот обзор, мы попросили коллег ответить на несколько вопросов:

1. Знаете ли вы, что современные колледжи готовят специалистов в области ИБ, которые получают квалификацию «техник по защите информации»?
2. Примете на работу такого специалиста?
3. Работают ли у вас специалисты со средним специальным образованием?
4. Считаете ли вы, что для работы на ответственной должности в департаменте по защите информации вашей организации требуются специалисты только с высшим образованием?

Мнения коллег разделились.

Михаил Одувалов, эксперт BIS Journal:

- 1 Нет.
- 2 Нет.
- 3 Нет.
- 4 Да.

Лев Шумский, начальник Управления контроля информационных рисков ДОР (АО) Связной Логистика:

1. Нет.
2. В дежурную смену оператором центра мониторинга ИБ.
3. С неоконченным высшим (студенты) профильным образованием (МИФИ, МГТУ им. Баумана).
4. Зависит от уровня должности и зоны ответственности. Для начальных должностей от уровня «специалист» с узким кругом задач вполне допустимо.

Дмитрий Левиев, председатель Совета НП «Партнерство специалистов по информационной безопасности»:

1. Да, знаю, сам участвовал в ГЭК.
2. Готов на уровень оператора УЦ или аналогичную должность.
3. В настоящий момент нет, но есть положительный опыт.
4. Не понятен вопрос, высшее образование к должности никак не относится, кроме как к требованиям по лицензии.

Для получения квалификации «Старший техник по защите информации» придется учиться на год больше. Преимущество при поступлении в колледж на бюджетные места отдается выпускникам 9 класса. Зачисление на бюджетные места на базе 11 классов возможно только в случае наличия вакантных мест после зачисления на базе основного общего образования. Но можно учиться на коммерческой основе.

Для тех, кто готов совмещать работу с учебой, многие колледжи предлагают очно-заочную и заочную формы обучения. Об этом ниже.

ЧЕМУ УЧАТ

Программа обучения по специальностям ИБ во многом схожа с программой подготовки инженерных кадров в вузах. Студенты, как гласит реклама на сайтах колледжей, «осваивают следующие виды деятельности: эксплуатацию подсистем безопасности автоматизированных систем, применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах, применение инженерно-технических средств обеспечения информационной безопасности».

Помимо базовых предметов школьной программы (для тех, кто после 9 класса) студенты изучают следующие дисциплины:

- ◆ Основы информационной безопасности;
- ◆ Основы управленческой деятельности;
- ◆ Правовое обеспечение информационной безопасности;
- ◆ Электротехника;
- ◆ Электрорадиоизмерения;
- ◆ Технические средства информатизации;
- ◆ Основы алгоритмизации и программирования;
- ◆ Метрология, стандартизация и сертификация;
- ◆ Инженерная графика;
- ◆ Организационное обеспечение информационной безопасности;
- ◆ Технические методы и средства защиты информации;
- ◆ Программно-аппаратные средства защиты информации;
- ◆ Криптографические методы защиты информации;
- ◆ Экономика отрасли.

В числе предметов и дисциплин, на усмотрение колледжа, могут быть также:

- ◆ обеспечение организации системы безопасности предприятия;
- ◆ правовая защита информации, ведение конфиденциального делопроизводства, организация и сопровождение электронного документооборота, технические методы и технологии инфор-

мации, программно-аппаратные средства информации;

◆ компьютерные сети и системы телекоммуникации с применением учебно-методических материалов и оборудования компании Cisco;

◆ технологии разработки ПО, БД, языки программирования, в т.ч. C/C++, C#, Java, Assembler, Pascal и пр.

СКОЛЬКО СТОИТ

Для выпускников 9–11 классов обучение оплачивается в основном за счет бюджета, число бюджетных мест ограничено 25, редко где набирают две группы одного возраста. Проходной балл для девятиклассников — выше 4,1. Число поданных заявлений зависит от колледжа, в популярных у школьников учебных заведениях конкурс составляет 2–3 человека на место.

Стоимость обучения по программам СПО по направлениям ИБ на коммерческой основе в ряде колледжей ненамного отличается от стоимости образования в ведущих вузах. Так, учеба в столичном Колледже современных технологий им. М. Ф. Панова обойдется от 90 тыс. руб. в год (на дневном отделении с элементами заочного образования) до 120 тыс. руб. в год (по направлению «ИБ телекоммуникационных систем»).

В те же 120 тыс. руб. обойдется год обучения в Колледже автоматизации

Сергей Вихорев, директор по информационной безопасности Филиала «ПЕТЕРС–СЕРВИС Спецтехнологии»:

1. Да, знаю. Один такой колледж есть в Москве, на Шереметьевской улице.
2. На должность стажера.
3. Нет, должностей в ИБ не так уж и много, владельцы бизнеса экономят, поэтому, как правило, выбираем универсала по принципу «И швец, и жнец, и на дуде игрец».
4. На ответственных должностях должны работать только люди с высшим образованием и опытом. Но есть и технические должности... Последнее время много просматриваю вакансий на hh.ru. Что-то техников от ИБ не наблюдаю...

Сергей Кривошеин, технический директор Angara Professional Assistance:

1. Да.
2. Да.
3. Как раз оформляем на работу такого специалиста со средним специальным образованием. Специальность «Ин-

формационная безопасность автоматизированных систем» (Проф. стандарт 10.02.03), квалификация «Техник по защите информации».

4. Нет.

Комментарий: Наш опыт работы со специалистами, имеющими различное образование, показывает, что в современных условиях нет явной зависимости между фактом наличия диплома вуза, специализацией и компетенциями кандидатов. Отсутствие высшего образования не является блокирующим фактором при поиске кандидатов в Angara Professional Assistance.

Думается, эти ответы являются своеобразным комментарием к нашему обзору. Тема среднего профессионального образования не простая, весьма противоречивая, но, безусловно, она становится все более актуальной в контексте перспективного роста отрасли ИБ. Многих сторон этой темы мы даже не затронули. Надеемся сделать это в последующих номерах журнала.

и информационных технологий № 20, а Колледж информатики и программирования Финансового университета при Правительстве РФ научит ИБ за 90 тыс. руб. в год. Чуть дешевле обучение в Московском приборостроительном техникуме РЭУ им. Плеханова (74,6 тыс. руб./год). Московский государственный колледж электромеханики и информационных технологий берет 120 тыс. руб. в год за дневное очное образование и 60 тыс. руб. в год — за заочное. Университетский колледж информационных технологий МГУТУ им. К.Г. Разумовского (Первый казачий университет) предлагает коммерческое обучение за сумму от 100 тыс. руб. в год.

Полностью заочное или очное с элементами заочного образования обойдется дешевле — от 34 тыс. руб. в год, но и срок обучения при этом увеличивается: для выпускников 9 классов он составит 5 лет и 10 мес. вместо 3 лет и 10 мес., для 11-классников — 3 года 10 мес.

Если вырваться за пределы столицы, то стоимость обучения снижается как минимум в два раза, правда, одновременно уменьшается и число колледжей, ведущих подготовку техников ИБ, и число мест — в 25 заявленных, как правило, входят 15 бюджетных и 10 платных.

В Санкт-Петербурге в рамках среднего профессионального образования подготовку специалистов по ИБ ведут три колледжа. Стоимость обучения в Петербургском Колледже строительной индустрии и городского хозяйства — 52 тыс. руб. в год. Более чем в два раза весной 2017 г. была снижена стоимость обучения на освоение образовательных программ СПО — до 50 тыс. руб. в год — в Технологическом институте Северо-Восточного федерального университета им. М.К. Амосова, что в Якутске. Учеба в Аэрокосмическом колледже Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева в Красноярске, по сравнению с запросами московских колледжей, просто «бесплатная» — всего 37360 руб. в год (9 тыс. руб. на заочном отделении на базе 11 классов).

Стоит отметить, что во многих колледжах, которые ведут подготовку

специалистов по направлениям ИБ, набор на 2017/2018 учебный год по этим специальностям открыт не был.

ПРОХОДНОЙ БАЛЛ 2017

Сколько баллов надо набрать на бюджетные места? Как правило, показатели не сильно разнятся. Так, для поступления в Колледж современных технологий им. М.Ф. Панова на специальность «ИБ АС» на базе 11 классов надо набрать 3,53 балла. В Колледже автоматизации и информационных технологий № 20 на специальности «Организация и технология защиты информации» и «ИБ АС» (на базе 9 классов) было подано 102 и 134 заявления соответственно, проходной балл составил 3,93 и 3,96. Желающих после 11 класса было намного меньше (42 и 66), проходной балл — 3,8 и 3,86.

Проходной балл на специальность «ИБ АС» (на базе 9 классов) в Московском приборостроительном техникуме РЭУ им. Г.В. Плеханова на бюджетной основе составил 4,21 (3,28 платное обучение), на базе 11 классов — 3,13 (платное обучение).

По данным сайта Московского колледжа электромеханики и информационных технологий, желающих учиться по специальности «ИБ АС» на базе 9 классов на платной основе не нашлось.

Колледж информационных технологий МГУТУ им. К.Г. Разумовского принял в 5 раз больше заявлений от желающих учиться по направлению «ИБ АС» на бюджетной основе (25 мест), а на 30 платных мест претендовали всего 14 абитуриентов.

В Петербургском Колледже строительной индустрии и городского хозяйства на «ИБ телекоммуникационных систем» после 9 класса прошли абитуриенты с минимальным баллом 3,89 (бюджет), на платной основе (72,4 тыс. руб., 25 мест) согласились учиться единицы. Зато в Технологическом институте Северо-Восточного федерального университета им. М.К. Амосова на специальность «ИБ АС» нашлось намного больше желающих (25), чем было заложено в планах (16), абитуриентов и их родителей не отпугнула плата за очное обучение в размере 114 тыс. руб./год (или 50 тыс. руб. для лиц, имеющих льготы — данные сайта учебного заведения).

В Аэрокосмический колледж Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева на специальности, связанные с ИБ, поступили абитуриенты, набравшие от 4,6 балла (бюджет) или от 3,5 (платная основа).

КЕМ РАБОТАТЬ

По окончании обучения выпускники колледжей, получившие квалификацию СПО «техник по защите информации» или «старший техник по защите информации», могут работать по различным направлениям ИТ: производство и поставка средств вычислительной техники; системная интеграция; обеспечение защиты информации; создание комплексных систем безопасности.

Цитируя госстандарты, многие колледжи красочно описывают работу техников по защите информации. «Техник по защите информации — специалист, занимающийся проверкой технического состояния, установкой, наладкой и регулировкой аппаратуры и приборов телекоммуникационных систем, их профилактическим осмотром и текущим ремонтом». Техники также «принимают участие в работе по обеспечению ИБ исследований и разработок, соблюдению гостайны, осуществляют проверку технического состояния, установку, наладку и регулировку аппаратуры и приборов, их текущий ремонт, выполняют работы по эксплуатации средств защиты и контроля информации, следят за работой аппаратуры и другого оборудования»...

Другие учебные заведения полагают, что техник может:

- ♦ Обеспечивать процесс защиты информации с использованием необходимых видов, методов, средств и технологий защиты;
- ♦ Осуществлять учет, обработку, хранение, передачу, организацию использования различных носителей конфиденциальной информации;
- ♦ Выявлять и блокировать каналы и методы несанкционированного доступа к информации, источники и способы дестабилизирующего воздействия на информацию;
- ♦ Устанавливать и адаптировать системы и средства обеспечения защиты информации;

А КАК У НИХ?

Согласно академическим критериям программы двухлетней подготовки технических кадров в сфере ИБ, разработанной АНБ США (NSA's Academic Criteria), специалист, аналог нашего техника, получает знания по предметам и направлениям:

- ◆ базовый анализ данных;
- ◆ введение в основы программирования;
- ◆ киберзащита;
- ◆ киберугрозы;
- ◆ фундаментальные принципы проектирования безопасности;
- ◆ основы информационного обеспечения;

- ◆ введение в криптографию;
- ◆ компоненты IT систем;
- ◆ основы построения сетей;
- ◆ основы политики, права, этики и соответствия;
- ◆ системное администрирование.

В четырехлетнюю базовую программу по информационной безопасности, которая соответствует программе подготовки бакалавров в области кибербезопасности, помимо указанных выше предметов, входят:

- ◆ базы данных;
- ◆ сетевая защита;
- ◆ сетевые технологии и протоколы;
- ◆ концепции операционных систем;

- ◆ вероятность и статистика;
- ◆ программирование.

В расширенных курсах есть также облачная безопасность, цифровая криминалистика, безопасность цепочки поставщиков и пр.

Зарплата специалистов в области ИБ, прошедших базовую подготовку по стандартам АНБ США, не сравнима с доходами техника по защите информации.

Для сравнения, средняя зарплата токаря в Москве составляет 41,5 тыс. руб., а оператора ЭВМ (без опыта работы или работающего удаленно) — 16,6 тыс. руб.

- ◆ Осуществлять контроль за качеством функционирования оборудования защищенных автоматизированных и телекоммуникационных систем, осуществлять анализ качественных и количественных показателей функционирования оборудования, осуществлять диагностику и устранение отказов, наладку и ремонт оборудования;

- ◆ Участвовать в подготовке технической документации;

- ◆ Осуществлять техническую эксплуатацию на объектах профессиональной деятельности, предназначенных для сбора, обработки, хранения и передачи информации.

Многие колледжи указывают, что студенты проходят практику на предприятиях от муниципальных бюджетных учреждений до крупных IT-интеграторов, занимающихся практической и научной деятельностью в области информационной безопасности. Там же они могут в последствие и работать.

Правда, по Общероссийскому классификатору профессий рабочих, должностей служащих и тарифных разрядов ОК 016–94, техник входит в перечень как «Оператор электронно-вычислительных и вычислительных машин». Выпускник может занимать такие должности как техник по защите информации в компьютерных системах, системный администратор локальных сетей, техник-программист по защите информации в компьютерных системах.

Как показал анализ вакансий на сайтах по поиску работы, отечественные работодатели не знают о существовании такой специальности — «техник по защите информации». Большинство компаний, озабочившихся своей кибербезопасностью, ищут инженеров с высшим образованием и опытом работы по специальности от 5 лет. Разброс по зарплатам для такого специалиста — от 20 тыс. руб. и выше. А многочисленным операторам ЭВМ, зарплаты которых в бюджетных учреждениях начинаются от 10 тыс. руб., не требуются углубленные знания в области ИБ.

По-армейски четко определяет профессию только Серпуховской филиал Военной академии ракетных войск им. Петра Великого Минобороны РФ, где выпускники получают звание «прапорщик» со средней военно-специальной подготовкой по военной специальности, соответствующей специальности 10.02.03 «Информационная безопасность автоматизированных систем».

Среди вариантов продолжения образования и повышения квалификации — обучение в ВУЗе по профильной специальности. Среди вузов-партнеров многие московские колледжи указывают ФГБОУ ВО «Московский государственный университет геодезии и картографии» (МИИГАиК); ФГБОУ ВО «Московский государственный тех-

нический университет радиотехники, электроники и автоматики» (МГТУ МИРЭА), ФГБОУ ВО «Национальный исследовательский университет „МЭИ“», ФГБОУ ВО «МГУТУ им. Г.К. Разумовского (ПКУ)». Многие региональные колледжи ведут обучение по программам СПО на базе крупных местных и федеральных университетов, где есть кафедры информационной безопасности.

ПРОФСТАНДАРТЫ В ДЕЙСТВИИ

В 2014 г. на государственном уровне начали активно обсуждать не только образовательные, но и профессиональные стандарты — единые требования к квалификации, которая необходима каждому работнику для выполнения определенной ему трудовой функции (по уровню образования, стажу работы, компетенциям (знаниям и умениям)). Итоги обсуждения вошли в поправки к Трудовому кодексу, 2 мая 2015 г. президент России подписал ФЗ-122 «О внесении изменений в Трудовой Кодекс Российской Федерации» и статьи 11 и 73 ФЗ «Об образовании в Российской Федерации». Для исполнения требований этого ФЗ, 27 июня 2016 г. Правительство России приняло постановление № 584, согласно которому с 1 июля 2016 г. началось поэтапное внедрение профессиональных стандартов в го-

Рег. № ПС	Код ПС	Сфера проф. деятельности	Вид проф. деятельности	Наименование ПС	Примечание
830	12.004	Обеспечение безопасности	Разработка и эксплуатация систем обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы	Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак	Текст настоящего профессионального стандарта не подлежит обязательному официальному опубликованию как содержащий сведения, составляющие государственную тайну, или сведения конфиденциального характера.
831	12.005	Обеспечение безопасности	Противодействие иностранным техническим разведкам	Специалист по противодействию иностранным техническим разведкам	Текст настоящего профессионального стандарта не подлежит обязательному официальному опубликованию как содержащий сведения, составляющие государственную тайну, или сведения конфиденциального характера.
840	06.030	Связь, информационные и коммуникационные технологии	Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним	Специалист по защите информации в телекоммуникационных системах и сетях	
841	06.031	Связь, информационные и коммуникационные технологии	Автоматизация информационно-аналитической деятельности (АИАД) в государственных органах, обеспечивающих национальную безопасность	Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности	
842	06.032	Связь, информационные и коммуникационные технологии	Защита информации в компьютерных системах и сетях	Специалист по безопасности компьютерных систем и сетей	
843	06.033	Связь, информационные и коммуникационные технологии	Обеспечение безопасности информации в автоматизированных системах	Специалист по защите информации в автоматизированных системах	
844	06.034	Связь, информационные и коммуникационные технологии	Техническая защита информации	Специалист по технической защите информации	

Таблица 1. Профстандарты по направлениям ИБ

сударственных учреждениях и организациях. Обязательное внедрение профстандартов для госорганов и госкомпаний должно произойти до 2020 г.

В соответствии с требованиями закона в ноябре 2016 г. Приказами Минтруда были приняты и утверждены Минюстом России профстандарты, в том

числе и по интересующим нас направлениям ИБ (см. таблицу 1).

Некоторые из указанных профстандартов распространяются и на средне-технический персонал, состоящий на государственной службе. Возможно, что после окончательного внедрения профессиональных стандартов и требований к квалификации персонала,

к выпускникам колледжей будут относиться с большим почтением.

Подробнее о профстандартах и требованиях к квалификации персонала в сфере ИБ мы расскажем в ближайших номерах журнала.

KASPERSKY®



Kaspersky® DDoS Prevention

Противодействие
DDoS-атакам
для непрерывной
работы вашего бизнеса

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

kaspersky.ru/ddos-prevention

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

ARinteg®

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

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

www.ARinteg.ru



КОНКУРС РАСТЕТ

ИТОГИ ВСТУПИТЕЛЬНОЙ КАМПАНИИ 2017 ГОДА

Чем ознаменовалась вступительная кампания 2017 года? С одной стороны, выпускники и их родители жаловались на сложные задания по профильным предметам на ЕГЭ, в результате чего многие потеряли столь важные для поступления в вуз баллы. А с другой, по итогам вступительной кампании руководители многих вузов отмечают значительное повышение проходного балла и рост числа победителей олимпиад.

ОБРАЗОВАТЕЛЬНЫЕ СТАНДАРТЫ

Что нового может быть в подведении итогов вступительной кампании? Казалось бы, их можно свести в таблицу с указанием вуза, специальности, конкурса на место и проходного балла. Можно отследить изменение стоимости обучения и количества бюджетных и платных мест. Однако учебный 2017/2018 год имеет свою особенность. Он ознаменовался введением единого подхода к учебным программам высшего образования.

В декабре-январе 2017 г. Минобрнауки РФ приняло Федеральные государственные образовательные стандарты высшего образования (ФГОС ВО). В том числе по направлениям бакалавриата (10.03.01. Информационная безопасность), специалитета (10.05.01. Компьютерная безопасность; 10.05.02. Информационная безопасность телекоммуникационных систем; 10.05.03. Информационная безопасность автоматизированных систем; 10.05.04. Информационно-аналитические системы безопасности; 10.05.05. Безопасность информационных технологий в правоохранительной сфере) и магистратуры (10.04.01. Информационная безопасность). Также можно стать кандидатом технических наук по специальности ИБ, окончив аспирантуру и защитив диссертацию по направлению 10.06.01. Информационная безопасность.

Поскольку в российских университетах чаще всего представлены программы специалитета, рассмотрим подробнее эти требования ФГОС ВО.

Профессиональная деятельность выпускников, освоивших программу специалитета по ИБ, включает: области науки, техники и технологии, охватывающие совокупность проблем, связанных с разработкой и эксплуатацией средств и систем защиты информации компьютерных систем, доказательным анализом и обеспечением защищенности компьютерных систем от вредоносных программно-технических и информационных воздействий в условиях существования угроз в информационной сфере.

Выпускники, получившие знания в области ИБ, смогут работать с защищаемыми компьютерными системами и входящими в них средствами обработки, хранения и передачи информации; системами управления информационной безопасностью компьютерных систем; методами и реализующими их средствами защиты информации (СЗИ) в компьютерных системах; математическими моделями процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; методы и реализующими их системами и средствами контроля эффективности защиты информации в компьютерных системах; процессами (технологиями) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах.

Выпускники, освоившие программу по направлению «10.05.01. Компьютерная безопасность», могут специализироваться по следующим направлениям:

- ◆ Анализ безопасности компьютерных систем;
- ◆ Математические методы защиты информации;
- ◆ Безопасность распределенных компьютерных систем;
- ◆ Разработка защищенного программного обеспечения;

◆ Безопасность высокопроизводительных вычислительных систем;

◆ Безопасность программного обеспечения мобильных систем;

◆ Информационно-аналитическая и техническая экспертиза компьютерных систем;

◆ Информационная безопасность объектов информатизации на базе компьютерных систем;

◆ Специальные технологии противодействия компьютерным атакам.

Для специальности «ИБ телекоммуникационных систем» ряд специализаций определяется квалификационными требованиями к профессиональной подготовке выпускников с учетом потребностей государственных организаций. По этому направлению также можно получить знания в области ИБ космических телекоммуникационных систем (ТКС); научиться разрабатывать защищенные ТКС, изучать системы подвижной цифровой защищенной связи, погрузиться в защиту информации в радиосвязи и телерадиовещании или в защиту информации в системах связи и управления. Также предусмотрена специализация в области ИБ мультисервисных ТКС и систем на транспорте или ИБ ТКС информационного взаимодействия.

Выпускник, освоивший программу «Информационно-аналитические системы безопасности» (10.05.04) может применить свои знания в области автоматизации информационно-аналитической деятельности, ИБ финансовых и экономических структур или в сфере информационно-аналитического мониторинга.

По какой программе ни учился бы студент, на выходе из стен университета он должен быть готов заниматься научно-исследовательской и проектной деятельностью, уметь разрабатывать технические задания (ТЗ) на проектирование эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом

действующих нормативных и методических документов; разрабатывать проекты систем и подсистем управления ИБ объекта в соответствии с ТЗ; проектировать программные и аппаратные СЗИ в соответствии с ТЗ с использованием средств автоматизации проектирования; оценивать эффективности реализации СЗИ и действующих политик безопасности в компьютерных системах; знать методы оценки и способы поиска уязвимостей, уметь оценивать безопасность компьютерных систем при проведении контрольного анализа системы защиты; выполнять экспериментально-исследовательские работы при проведении сертификации программно-аппаратных средств защиты и анализировать результаты. А также многое другое с учетом специфики конкретного направления.

ВШЭ БЬЕТ РЕКОРДЫ

На пресс-конференции по итогам вступительной кампании проректор Высшей школы экономики В. Радаев отметил, что в ВШЭ было подано рекордное число заявлений на бюджетные места — на 20% больше, чем в предыдущие годы. Выросло и число желающих учиться на коммерческой основе. Средний балл зачисления по итогам ЕГЭ приблизился к 90, средний конкурс — 13 человек на место, на некоторые специальности — до 45 человек на место.

Направление «Информационная безопасность» на базе МИЭМ (МИЭМ НИУ ВШЭ) в этом году побilo собственные рекорды. На 30 бюджетных мест, из которых 9 были определены под целевой набор и обладателей социальных льгот, было подано 573 заявления, а еще 29 абитуриентов — победителей различных олимпиад — имели право поступления без вступительных испытаний. На 60 платных мест подали документы 269 человек. Всего же направление ИБ при подаче документов выбрали 613 абитуриентов. Проходной балл составил 293, что существенно

выше показателей 2016 г. — 281 балл. Стоимость обучения в 2017–2018 учебном году — 260 тыс. руб., что на 20 тыс. руб. больше, чем в прошлом году.

ХОЧЕШЬ ЗНАНИЙ — УЧИСЬ В СТОЛИЦЕ

Как показывают исследования, около половины поступающих в столичные вузы приехали из регионов. Например, в МФТИ поступало 43% москвичей и жителей области и около 49% жителей других регионов. Такая же пропорция сохранилась и по итогам зачисления на первый курс.

Традиционно высокие требования к поступающим в МИФИ. По направлению ИБ там было открыто 45 бюджетных и 15 коммерческих мест. Платное обучение стоит порядка 109 тыс. руб. за семестр, учеба в магистратуре обойдется в 119,7 тыс. руб., в аспирантуре — 125 тыс. руб. Однако для поступления в МИФИ мало просто заплатить. Минимальный проходной балл на платные места составил 210 на все направления.

В МГТУ им. Н.Э. Баумана в этом году набирали первокурсников на специальности «Компьютерная безопасность» (10.05.01) и «Информационная безопасность автоматизированных систем» (10.05.03). На 20 бюджетных мест по первому направлению претендовали 480 человек, на 30 бюджетных мест по второму — 360. На коммерческой основе — 10 и 30 мест соответственно (стоимость обучения — 257 572 руб./год). Проходной балл по общему конкурсу на направление 10.05.01 составил 280, на 10.05.03 — 270. По сравнению с предыдущими годами, уровень подготовки абитуриентов значительно вырос: в 2016 г. можно было поступить, набрав 269 и 268 баллов, а в 2015 г. от абитуриента требовалось всего 250 или 254 балла соответственно.

МФТИ в этом году принял всего 15 человек по направлению «Компьютерная безопасность» (10.05.01). Чтобы попасть в конкурс на 9 бюджетных мест

(205 заявлений), требовалось набрать по итогам ЕГЭ не менее 65 баллов по математике и физике и 50 баллов по русскому языку. Минимальный проходной балл составил 286. На 5 коммерческих мест (250 тыс. руб./год) были поданы 22 заявления.

МАИ готовит бакалавров по направлению «Информационная безопасность» (10.03.01) и «Информационная безопасность телекоммуникационных систем» (10.05.02). Минимальный балл по итогам первого этапа составил 251 (ИБ) и 238 (ИБ ТКС), на втором этапе 241 и 247 баллов соответственно. Для сравнения, в 2016 г. надо было набрать 242 и 214 баллов на первую специальность и 236 и 226 баллов на вторую. При зачислении на платной основе (150 230 руб./год) в МАИ в этом году принимались абитуриенты, набравшие по итогам ЕГЭ от 152 и 147 баллов соответственно.

Конкурс в РГГУ на специальность «Информационная безопасность» (10.03.01) составил 21 человек на место (в 2016 г. — 5,94 человека на место). Всего университет набирал на бюджетные места 36 человек по общему конкурсу и 4 по квоте. Конкурс на 10 платных мест составил 4,9 заявлений на место. Отметим, что год учебы в университете стоит 208 800 руб. Минимальный проходной балл первого этапа зачисления на бюджетные места составил 199, второго этапа — 201. На платной основе в университете смогли учиться обладатели 159 баллов и выше.

В Российском университете транспорта (МИИТе) число желающих получить квалификацию по специальности «Информационная безопасность объектов информатизации на базе компьютерных систем» (10.05.01.65) превысило число мест в 13,87 раза (бюджет) и в 3,47 раза (платная основа). Конкурс в бакалавриат по направлению 10.03.01 составил почти 21 человек/место. Среднестатистический показатель прошедших на 10 бюджетных мест составил 226 баллов, в бакалавриат — 224 балла. Стоимость платного обучения — 79,2 тыс. руб. за семестр.

В Московском технологическом университете (МИРЭА) представлен, наверное, самый большой выбор специальностей по направлению ИБ. Подразделение

КАК ПОКАЗЫВАЮТ ИССЛЕДОВАНИЯ, ОКОЛО ПОЛОВИНЫ ПОСТУПАЮЩИХ В СТОЛИЧНЫЕ ВУЗЫ ПРИЕХАЛИ ИЗ РЕГИОНОВ

ПЕРВЫЕ ТРИ МЕСТА СРЕДИ ВУЗОВ С САМЫМ БОЛЬШИМ НАБОРОМ НА БЮДЖЕТНЫЕ МЕСТА ЗАНЯЛИ ВШЭ, СПБГУ И МГУ ИМ. ЛОМОНОСОВА

«Институт комплексной безопасности и специального приборостроения» набирало первокурсников в бакалавриат по специальности 10.03.01 и в специалитет по направлениям 10.05.03, 10.05.04 и 10.05.05. Другое подразделение — «Институт кибернетики» — открыло специальности 10.05.01 и 10.05.02.

Минимальные проходные баллы составили:

10.05.01 — 236 (1 этап), 222 (2 этап);
10.05.02 — 235, 233;
10.03.01 — 240, 238;
10.05.03 — 227, 228;
10.05.04 — 225, 224;
10.05.05 — 232, 228.

Для обучения на коммерческой основе достаточно было просто принести аттестат, иметь положительные оценки за ЕГЭ (в списках поступивших есть абитуриенты с 112 баллами) и заплатить деньги. Обучение в специалитете — 160 тыс. руб. (130 тыс. руб. со скидкой), в бакалавриате — 142 тыс. руб. (120 тыс. руб. со скидкой) в год.

Если в прошлом году в Московском государственном лингвистическом университете на Факультет информационной безопасности был огромный конкурс (21,32 человека на одно бюджетное место, и 33,16 — на платное), то в этом году в бакалавриат по направлению 10.03.01 принимали только на коммерческой основе. На 36 мест были поданы 172 заявления, конкурс составил 4,78 человека на место. Минимальный проходной балл составил 135. Стоимость первого года обучения — 215 тыс. руб., второго и последующих — 220 тыс. руб.

Минимальный проходной балл в магистратуру по профилю «Информационная безопасность в международном сотрудничестве» (10.04.01) составил 152 балла, обучение платное, 220 тыс. руб./год.

ДАЛЬШЕ УЕДЕШЬ— БЫСТРЕЙ ПОСТУПИШЬ

По мере удаления от МКАД падают не только цены на товары повседневного спроса, но и цены на обучение, а также

и требования к абитуриентам. Хотя без исключений и тут не обходится.

Так, в Санкт-Петербургском политехническом университете Петра Великого велся набор по 4 специальностям ИБ: «Информационная безопасность» (10.03.01); «Компьютерная безопасность» (10.05.01), «Информационная безопасность автоматизированных систем» (10.05.03); «Информационно-аналитические системы безопасности» (10.05.04). Первоначальный конкурс составил 28,5 заявлений на бюджетное место. Минимальный проходной балл на бюджет составил 261, на платное обучение — 163 (плата 76,5 тыс. руб. за семестр).

Собственный рекорд побил проходной балл на специальность 10.05.01 в Санкт-Петербургском государственном электротехническом университете «ЛЭТИ» им. В.И. Ленина. Если последние три года средний проходной балл колебался вокруг 220, то минимум 2017 г. — 241 балл (1 этап) и 282 балла (2 этап). На 60 бюджетных мест было подано 400 заявлений, также были открыты 15 контрактных мест (157 тыс. руб./год).

В Институте космических и информационных технологий Сибирского Федерального университета в этом году набирали студентов на три направления ИБ: 10.03.01 (ИБ), 10.05.01 (Компьютерная безопасность) и 10.05.03 (ИБ АС). Минимальные проходные баллы на специальность 10.03.01 составили 219 (1 этап) и 173 (2 этап), на направление 10.05.01—226 и 222, на специальность «ИБ АС» — 212 и 174 соответственно. Минимум баллов для зачисления на платной основе (70 290 руб. за семестр) составил 132.

В Алтайском государственном техническом университете им. И.И. Ползунова на специальность 10.03.01 (ИБ) минимальный проходной балл первого этапа зачисления — 213, второго — 181. На коммерческие места (88,5 тыс. руб./год) — 160 баллов по ЕГЭ.

Физико-технический факультет Алтайского государственного университета набирал в этом году 35 студентов на бюджетные места также по направлению 10.03.01 (ИБ). В прошлом году конкурс на бюджет составил 8,8 человек на место, а проходной балл 184. В этом году минимальный проходной балл для первого этапа зачисления составил 186, второго — 173. Стоимость платного обучения — 92,5 тыс. руб./год.

Дальневосточный федеральный университет допускал к конкурсу тех, кто набрал совсем немного баллов по ЕГЭ: 27 по русскому языку, 36 по физике и профильной математике. В сфере ИБ были открыты специальности 10.03.01 (ИБ) и 10.05.01 (КБ). Минимальный проходной балл для ИБ составил 175 (1 этап) и 183 (2 этап), на КБ прошли набравшие 190 и 173 баллов соответственно. Платное обучение ИБ на Дальнем Востоке стоит 170 тыс. руб./год.

В Воронежском государственном техническом университете на специализацию «Безопасность распределенных компьютерных систем» на 15 бюджетных мест подали заявления 193 человека. Минимальный балл по итогам зачисления составил 211. На направление «Системы подвижной цифровой защищенной связи» на бюджетные места претендовали 110 человек, минимальный проходной балл составил 203, а на 15 мест по специальности «Обеспечение информационной безопасности распределенных информационных систем» подали заявления 118 человек. Минимальный проходной балл составил 216. Платное обучение в ВГТУ — 95,1 тыс. руб./год.

ПОДВОДЯ ИТОГИ

По данным Минобрнауки, средний балл ЕГЭ зачисленных на бюджетные места в 2017 г. увеличился относительно уровня прошлого года на 1,6 балла и составил 68,2 балла. В вузах Москвы и Санкт-Петербурга средний балл ЕГЭ зачисленных на бюджетные места составил 76,2 и 75,8 балла соответственно.

Среди вузов с приемом на бюджетные места свыше 1,5 тысяч человек самые высокие показатели также приходятся на Москву и Санкт-Петербург: средний балл по ним составляет 79,9.

ВУЗ	Специальность	Число мест (бюд./пл.)	Экзамены по ЕГЭ	Мин./ср.балл на конкурс	Конкурс чел/ место (бюд./пл.)	Проходной балл бюд./пл.	Мин. балл 2016 г.	Стоимость 1-го уч. года (тыс.руб)
ВШЭ	10.05.01	30/65	МРИ/ИКТ	58,3/ 96,7	27,3/4,14	293 из 310/нд	281 из 310	260
НИЯУ МИФИ	10.03.01	45/15	МФР	63,3/нд	нд	нд/218	260	109
	10.05.04			60/нд			280	108,7
	10.05.05			58,3/нд			275	108,7
МФТИ	10.05.01	10/5	МФР	60/нд	41,2/4,4	286/272	274,4	250
МВТУ	10.05.01	20/10	ФМР	40/96,4	24/нд	284/188	269	257,572
	10.05.03	30/30		40/90	12/нд	270/150	268	
МАИ	10.03.01	20/30	МРИ/ИКТ	45,67/нд	нд	241/152	214	150,23
	10.05.02	14/22		45,67/нд		238/147	226	
РГГУ	10.03.01	36/10	МРИ/ИКТ	40/нд	21/4,9	199/159	208	208,8
МИИТ	10.05.01.65	15/15	МФР	33/нд	13,87/3,47	226/149	223/152	158,4
	10.03.01	15/15			20,9/4,7	224/150	205/152	
МИРЭА	10.03.01	36/70	МРИ	34,3/нд	нд	238/нд	239,5/	142
	10.05.03	56/40	МФР	33/нд		227/нд	232,3	160
	10.05.04	30/20	МРИ	34,3/нд		224/нд	250,7	142
	10.05.05	30/25		228/нд		235,7		
	10.05.01	56/60		222/нд		242,8		
	10.05.02	66/60		233/нд		238,8		
МГЛУ	10.03.01	нд/36	МРИ	нд/28,3	нд/4,78	нд/135	нд	215
СПбПУ	10.03.01	24/нд	МФР	41,7	24,4/	261/163	235/нд	153
	10.05.01	36/нд	МФР	41,7	15/	236/147	212/нд	
	10.05.03	24/нд	МРИ	45	19,7/	254/151	215/нд	
	10.05.04	36/нд	МРИ	41,7	12,1/	255/187	245/нд	
ЛЭТИ	10.05.01	60/15	МФР	46,7	6,6/нд	241/	220/	157
СПбГУТ	10.03.01	26/60	МРИ/ИКТ	38,3	8,9/1,45	238	235	146
ПГУПС	10.05.03	10/15	МФР	33	4,7/нд	215/нд	202	116,2
РГГМУ	10.05.02	нд/25	МРИ	нд	нд	нд/128	нд	115
СФУ	10.03.01	22/25	МРИ/ИТК	36,7	нд	57,67/46,33	73/39,33	140,58
	10.05.01	20/7				72,33/44	64,33/42	
	10.05.03	20/25				72,33/55,33	67,67/42	
АлтГТУ	10.03.01	30/10	МФР	40	6,1/нд	181/160	157/нд	88,5
АГУ	10.03.01	35/5	МФР	33	нд	173	184	92,5
ДВФУ	10.03.01	22/3	МФР	33	нд	175/нд	217	170
	10.05.01	35/1				173/нд	184	
ВГТУ	10.05.01	15/5	МФР	33	19,3/нд	211/нд	202	95,1
	10.05.02	15/5			11/нд	203/нд	204	
	10.05.03	15/5			11,8/нд	216/нд	217	

Таблица 1. Итоги вступительной кампании 2017 года

Федеральные университеты по этому показателю уступают ведущим столичным вузам примерно на 11,6 баллов (их средний балл 68,3). Крупнейшие вузы в регионах уступают столичным по показателям бюджетного приема в среднем на 13 баллов (их средний балл 66,9).

Первые три места среди вузов с самым большим набором на бюджетные места заняли ВШЭ, СПбГУ и МГУ им. Ломоносова.

В среднем по России конкурс на бюджетные места составил 8,2 заявлений на место. Среди технических направлений самые высокие баллы — на направления, связанные с информатикой и вычислительной техникой и безопасностью информации — 69,9 балла.

В вузы поступили все победители и призеры Всероссийской олимпиа-

ды школьников, чемпионы и призеры Олимпийских и Паралимпийских игр, которые изъявили желание поступить в высшие учебные заведения. На бюджетные места поступили 6202 победителя и призера олимпиад, что выше уровня прошлого года (5950 человек). Доля зачисленных победителей и призеров олимпиад от общего количества зачисленных составила 2,2% в целом (2% в 2016 г.).

РЕЛИКВИЯ РУССКОГО ФЛОТА

«ВЫ БЫЛИ НАШИМ МАЯКОМ, ПО ВАМ
МЫ ОПРЕДЕЛЯЛИСЬ»

Среди событий, ярко связанных с криптографической деятельностью во время Первой мировой войны, особое место принадлежит морской обороне Рижского залива в августе 1915 года. Именно тогда дешифровальщики Радиостанции особого назначения (РОН), недавно созданного разведывательного

центра Балтийского флота, успешно
выдержали свой главный экзамен.

ГИБЕЛЬ НЕМИНУЕМА

Как известно, к концу первого года войны сложилась тяжёлая обстановка для русских войск. Всего за три месяца были оставлены Польша, Литва и часть Белоруссии, фронт приближал-



Иллюстрация 1. Место разыгравшихся событий



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

ся к Риге. И вот, из добытой морской радиоразведкой информации, стало известно о подготовке прорыва немецкого флота в Рижский залив с целью огневой поддержки сухопутного наступления на Ригу. Направив часть своих морских сил из Северного моря, немцы сосредоточили у Ирбенского пролива — входа в Рижский залив крупное соединение (более пятидесяти!) боевых кораблей. Оно превосходило по огневой мощи весь русский Балтийский флот в 2,5 раза.

А в Рижском заливе тогда находилась небольшая группировка русских кораблей с единственным мощным бойцом — броненосцем «Слава». Казалось бы, их гибель неминуема.

НЕОЖИДАННЫЙ ПОВОРОТ СОБЫТИЙ

Но события стали разворачиваться неожиданным для немцев образом. Действуя весьма грамотно, они, тем не менее, долго не могли обезопасить проход в залив, теряя корабли на минах и от залпов русских кораблей. Они подвергались торпедным атакам с кораблей и подводных лодок, бомбардировке с самолётов «Илья Муромец». Тайное, как им казалось, ночное проникновение в Рижский залив двух германских эсминцев сразу же было обнаружено: их обстрелял дозор русских кораблей. При выходе этих эсминцев из залива после неудачного рейда произошёл их бой с русским эсминцем «Новик». Это известное морское сражение закончилось победой моряков



Иллюстрация 2. Флотский подарок А.И. Непенину



Иллюстрация 3. Поднос, подаренный А.И. Непенину

«Новика», один из вражеских эсминцев погиб, а другой был сильно повреждён. Даже немецкая броненосная эскадра прикрытия, не участвовавшая в боях, постоянно ожидала торпедные атаки.

И 19 августа её дерзко атаковала британская подводная лодка Е 1. Командир Е 1 Н. Лоуренс, искусно преодолев боевое охранение вражеской эскадры, торпедировал броненосный крейсер «Молотке» с расстояния всего 200 метров, за что был удостоен ордена св. Георгия 4-й степени. Из-за угрозы новых потерь немцы отменили свои планы. 21 августа, спустя две недели после начала операции, германский флот ушёл от Рижского залива на свои базы. Это привело затем и к срыву наступления немецких войск на Ригу, так как оно не было поддержано с моря.

КТО СПАСИТЕЛЬ?

Теперь-то мы знаем причину поразительной осведомлённости русских моряков о замыслах и действиях противника в августовские дни и ночи 1915 года. По мнению военных специалистов, «использование командованием БФ данных радиоразведки при срыве прорыва германского флота в Рижский залив считается одним из наиболее впечатляющих результатов разведывательного обеспечения военных действий на море в Первой мировой войне» [1]. Более того, излишние потери «заставили германское командование отказаться от активных действий крупными силами флота на Балтике. До конца кампании 1915 г. немецкий флот в Балтийском море предпринимал лишь оборонительные и демонстративные действия».

За таким успехом стояли достижения радиоразведчиков и дешифровальщиков РОН, а также слаженная работа всех звеньев механизма эффективного использования разведанных сведений. О преодоленных командованием БФ сложностях можно судить по тому факту, что британскому флоту не удалось эффективно использовать информацию, предоставленную радиоразведчиками «Комнаты 40», в Ютландском бою 31 мая 1916 года. Это сражение британского и германского флотов считается крупнейшим морским сражением в истории. Годы спустя, английский адмирал Дж. Харпер писал: «почти точными были сведения, сообщённые Адмиралтейством, но из них только одно было получено в срок и могло быть использовано. Но в то время большим доверием пользовались, естественно, те сведения, которые получались от кораблей, фактически имевших контакт с противником, а не от береговых радиопеленгаторных станций, тогда ещё только развивавшихся» [2].

На БФ было иное отношение к данным радиоразведки и к самим радиоразведчикам. Плоды их самоотверженных усилий, скрытых от посторонних взоров, высоко ценились на флоте. Радиоразведку и её достижения для моряков-балтийцев олицетворял контр-адмирал Адриан

Иванович Непенин, начальник Службы связи БФ. Он пользовался неизменным уважением и авторитетом во флотской среде. У нас есть возможность увидеть материальное подтверждение сказанных слов, а именно, подарок флотских командиров, преподнесённый А.И. Непенину 15 марта 1916 года.

ПОДАРОК

Сам подарок представляет собой поднос и набор для глинтвейна, популярного среди офицеров-балтийцев в начале XX столетия: кувшин, черпак, бокалы (Илл. 2). Кувшин изготовлен в виде маяка с чертами конкретного маяка из Цереля, а на поднос нанесён фрагмент карты Рижского залива (Илл. 3). Подарок, разумеется, со смыслом. Замысел дарителей раскрыт в сопроводительном письме, оглашённом контр-адмиралом П.Л. Трухачёвым при вручении подарка А.И. Непенину.

ДОРОЖЕ НАГРАДЫ

Познакомимся с содержанием письма. «Ваше Превосходительство Дорогой Адриан Иванович.

Прошлым летом 915 года в Рижском заливе произошли некоторые действия части Балтийского флота, которые были признаны Высшим Командо-

**РАДИОРАЗВЕДКУ И ЕЁ ДОСТИЖЕНИЯ
ДЛЯ МОРЯКОВ-БАЛТИЙЦЕВ
ОЛИЦЕТВОРЯЛ КОНТР-АДМИРАЛ
АДРИАН ИВАНОВИЧ НЕПЕНИН,
НАЧАЛЬНИК СЛУЖБЫ СВЯЗИ БФ**

ванием действиями, заслуживающими быть отмеченными как серьёзные по своему значению.

Мы, здесь присутствующие, представляем собой эту часть Балтийского флота. Многие из нас отличены более или менее высокими наградами за это время. Многие, например, я, очень высокими. Не смея утверждать, что наша работа соответствовала наградам, мы тем не менее думаем, что эти награды являются отметками в летописи событий. Отметками, по которым будущий Историк будет в этих событиях разбираться. Но, думается нам, Адриан Иванович, что ошибётся этот историк, если он будет в событиях этих разбираться, не связывая их с работой Службы Связи, или вернее не исходя из неё, т.е. от Вас, так как кто же не знает, что до Вас её не было. Работа историка трудна и кропотлива. Разбираясь в материалах, самые большие историки впадали в ошибки. Исторические документы затериваются, бумажки тлеют, единичные свидетельства опровергаются, историки запутываются, и истинные виновники больших событий бывают не отмеченными.

Мы, от лица всех бывших у Ирбена и видевших лицом к лицу Германский флот, позволяем себе свидетельствовать об том участии, которое Вы принимали в этих событиях. Слово «участие» мало для характеристики Вашей работы, даже «помощь» мало, я скорее назвал бы это одухотворением работы. И эту духовную Вашу помощь, которую мы глубоко ценим, мы пришли засвидетельствовать. Свидетельство это мы записали на нетлеющем серебре и на этом подносе поставили немого посредника между Вами и нами, немого, но так много нам сказавшего в те дни.

Ваше Превосходительство, у Цереля произошли главные события. Церель нас связывал летом 1915 года — да свяжет он нас и впредь, как эмблема, и да послужит он Вам доказательством того, что мы, жившие Вами в самые трудные моменты, не забывали, что Вы были нашим маяком, по Вам мы определялись и благодаря Вам погибли не наши корабли, а вражеские. Дай Вам Бог здоровья, Адриан Иванович. Дай Бог Вам ещё долго светить родному флоту

во славу России. 15 марта 1916 года». Далее 17 подписей: контр-адмирал, капитаны 1-го и 2-го ранга.

ИСТОРИЧЕСКОЕ СВИДЕТЕЛЬСТВО

Перед нами поразительное свидетельство, не оставляющее никаких сомнений в ведущей роли А. И. Непенина и его детища — Службы связи в одержанной победе. Это и признание факта, что, спустя год после начала войны, Служба связи со всеми её разнообразными новыми подразделениями, включая дешифровальные, достигла состояния возможности эффективной работы в реальном времени. Эффективность деятельности Службы связи подтверждают и объективные показатели: к концу 1915 года потери немецкого флота по боевым кораблям превосходили аналогичные русские потери в 3,4 раза.

Обратим внимание на удачное сравнение Службы связи с маяком. Действительно, как маяк во тьме высвечивает кораблям безопасный путь и ориентирует их, так и разведанные о неприятеле сведения разрушают мрак неизвестности, устраняют излишние опасения, вселяют уверенность и позволяют командирам наметить путь к успеху.

Дорого стоят слова флотских командиров: «благодаря Вам погибли не наши корабли, а вражеские». Чтобы убедиться в их справедливости, достаточно упомянуть печальную участь канонерской лодки «Сивуч». Её командира не успели предупредить о приближении немецких кораблей к Рижскому заливу. Встретив крейсера противника, лодка приняла бой, была немедленно расстреляна и героически погибла.

Обратим внимание и на дату поднесения подарка: 15 марта 1916 года. Совпало ли так, или время выбрано со смыслом, но ровно год прошёл с момента создания РОН — главного разведывательного центра Службы связи БФ. И ведь именно РОН сыграла ключевую роль в достижении победы над врагом у входа в Рижский залив.

КОНТР-АДМИРАЛ ПЕТР ТРУХАЧЕВ

Вероятно, автором текста является контр-адмирал Пётр Львович Трухачёв.

Его подпись стоит первой. Вот краткие факты его биографии.

Петр Львович Трухачев. (11.1867–11.1916). Вице-адмирал с 31.10.1916. Во время русско-японской войны, командуя миноносцем «Бесстрашный», участвовал в обороне Порт-Артура. В годы Первой мировой войны командовал крейсером «Олег», затем Минной дивизией и 1-й Бригадой крейсеров Балтийского флота. Умер на службе. Награжден Георгиевским оружием (03.1915), орденом св. Георгия 4-й степени (8.09.1915): «за то, что он, командуя вверенной ему дивизией в Рижском заливе, при наступлении неприятельских миноносцев... с целью форсировать Ирбенский пролив, имея в своем распоряжении силы значительно слабейшие, чем у германцев — искусным маневрированием, артиллерийским огнем и бдительной охраной нашего минного заграждения вынудил превосходные силы неприятеля отступить с потерей не менее двух неприятельских судов, при этом ... находясь под сильнейшим огнем, ... обеспечил наш успех, не понеся сам никаких потерь».

КАПИТАН 1-ГО РАНГА АЛЕКСАНДР РАЗВОЗОВ

Присутствовал при вручении подарка и подписал письмо капитан 1-го ранга Развозов Александр Владимирович (07.1879–06.1920). Именно он стал последним командующим БФ дооктябрьского периода. Участвовал в обороне Порт-Артура. После падения этой крепости отказался дать японцам подписку о дальнейшем неучастии в войне и наряду с матросами был помещён в лагерь военнопленных. В феврале 1906 года прибыл в Россию с последним эшелоном пленных. В 1913–1916 годах: командир эсминца «Уссуриец»; начальник 5-го, затем 9-го дивизиона эсминцев. 30 декабря 1915 года награжден Георгиевским оружием. С 6 марта 1917 — начальник Минной дивизии, с 7 июля по декабрь 1917 — командующий Балтийским флотом. С 18 июля 1917 — контр-адмирал. Руководил действиями флота во время Моонзундского сражения в октябре 1917 года.

20 ноября 1917 года А. В. Развозов изъявил готовность подчиняться правительству большевиков и был представлен к производству в вице-адмира-

лы. Уже 5 декабря он уволен в отставку в связи с введением коллегиального управления флотом. 12 марта 1918 года назначен на вновь введенную должность начальника морских сил Балтийского моря. 20 марта 1918 года снят со своего поста и арестован, но вскоре освобожден. Работал в Военно-морской исторической комиссии над описанием действий флота в Первой мировой войне. В сентябре 1919 года арестован ВЧК по обвинению в участии в военном заговоре, умер в больнице петроградской тюрьмы «Кресты».

ЛЕЙТЕНАНТ ДМИТРИЙ ФЕДОТОВ

Среди подписей старших офицеров в конце дарственного письма привлекает внимание подпись «лейтенант Федотов», причём не последняя в списке, старшинство по званию явно было не соблюдено. Несомненно, право на подпись получено заслуженно и она была весьма уместна.

Лейтенант Дмитрий Иванович Федотов служил на эсминце «Новик» и, так же, как его командир капитан 2-го ранга Михаил Андреевич Беренс, был награждён орденом св. Георгия 4-й степени за бой в Ирбенском проливе: «за то, что он, управляя огнём артиллерии миноносца «Новик» в Ирбенском проливе в бою с превосходящими силами неприятеля, с третьего залпа накрыл неприятельский головной миноносец и, перейдя на беглый огонь, продолжал его поражение. ... После чего неприятель обратился в бегство, а огонь был перенесен на второй миноносец. Первый миноносец, вследствие полученных повреждений, затонул у Михайловского маяка» (Иллюстрация 4).

Д. И. Федотов в 1910 году окончил Морской кадетский корпус, с 1913 — артиллерийский офицер эсминца «Новик», с апреля 1917 состоял в распоряжении

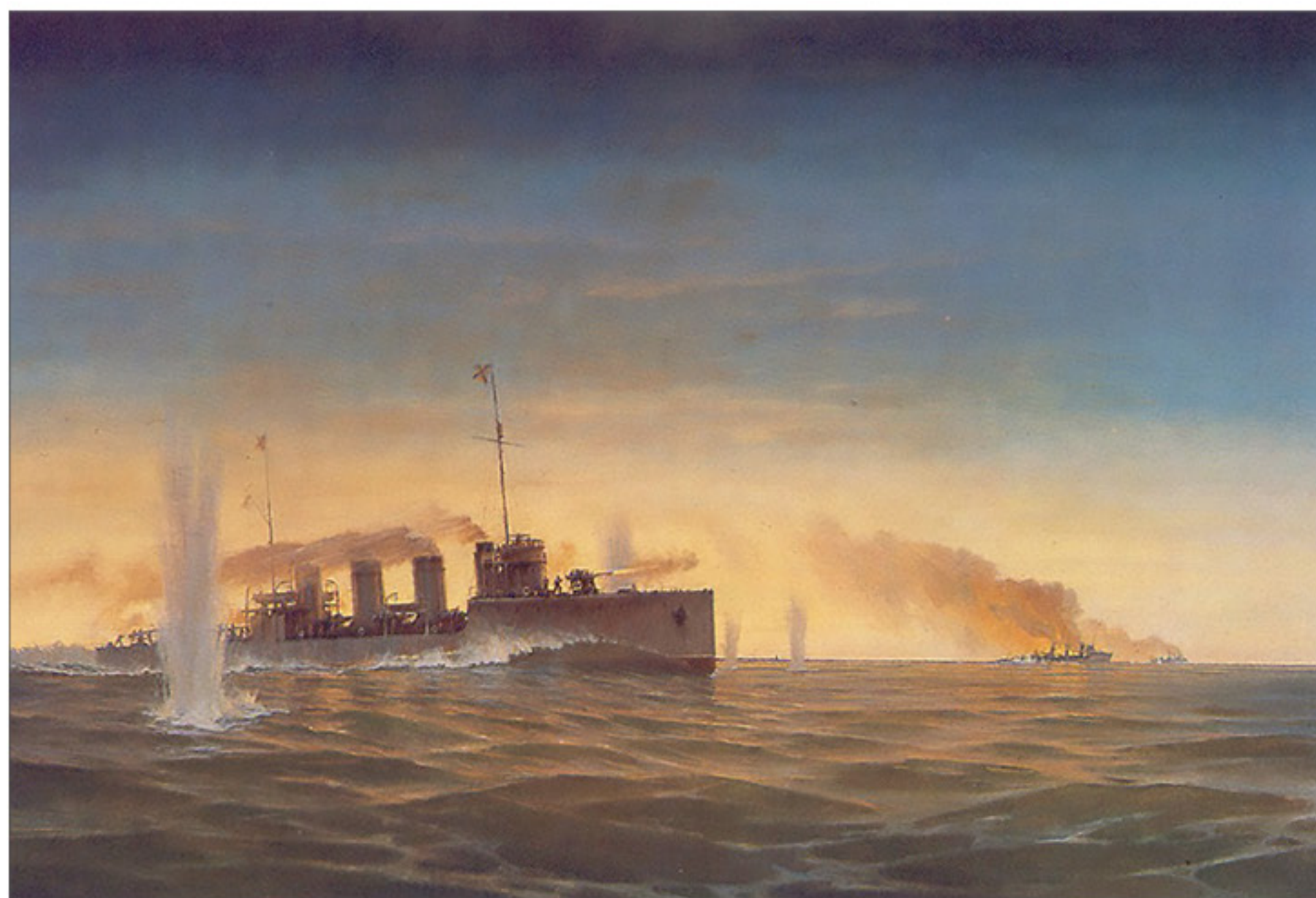


Иллюстрация 4. Бой эсминца «Новик» с германскими эсминцами. Худ. Г. В. Горшков

Главного морского штаба. В 1918 году перешёл в Красный флот, служил начальником Онежской озёрно-речной флотилии. В 1921 уволен в запас: не прошёл фильтрационную комиссию. Работал в Морской исторической комиссии. В начале 1923 года арестован, но в мае освобождён, с июня преподавал в Морской академии. В мае 1925 опять арестован как «участник монархической организации в 1919 году» и заключён в Бутырскую тюрьму в Москве. В начале декабря 1925 Д. И. Федотов был освобождён из тюрьмы, его дальнейший жизненный путь неизвестен.

СУДЬБА РЕЛИКВИИ

Пора прояснить историю попадания памятного подарка моряков в поле зрения нашего времени. Об этой реликвии и её пути к известности впервые поведал рижский писатель Юрий Мелконов [3]. На его сайте автор настоящего очерка обнаружил и представленные здесь фотографии.

Вероятно, памятный подарок после гибели А. И. Непенина хранился в его семье, выехавшей в эмиграцию в годы лихолетья. Моряки не оставляли вниманием семью своего товарища и командира, а потому реликвия не могла покинуть флотскую среду. В 30-е годы прошлого столетия памятный подарок оказался в США, где в ту пору собралось много бывших морских офицеров. Реликвия до 90-х годов не покидала одной из семейных коллекций в Лос-Анджелесе, но в 1997 году уже готовилась быть выставленной на аукционе Сотбис.

* * *

Именно тогда памятный подарок вместе с письмом непосредственно у владельцев приобрёл коллекционер Владимир Анатольевич Островский. Теперь его семья сохраняет реликвию русского флота и даёт возможность узнать о ней всем, кому дорога память о защитниках нашего Отечества.

ЛИТЕРАТУРА

1. 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.
2. Харпер Дж. Правда о Ютландском бое. // В книге Шеер Р. Германский флот в мировую войну. М., 2002.
3. <http://www.melkon.lv>

**Геннадий ЕМЕЛЬЯНОВ**член-корреспондент
Академии криптографии РФ**Дмитрий ЛАРИН**кандидат технических
наук

КРИПТОГРАФЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ

В предыдущих номерах мы рассказали о криптографах С. С. Толстом и Б. А. Аронском. Эта статья посвящена людям, также работавшим в нашей криптографической службе во время Великой Отечественной войны и после ее окончания.

В 1941 году в состав дешифровальной службы (ДРС РУ ГШ) была зачислена большая группа молодых ученых с основательной математической и технической подготовкой — выпускников ведущих вузов, призванных в армию (В. Х. Бадалян, Ф. А. Бахшиян, И. В. Матвеев, Г. С. Погосов, В. С. Полин, Г. И. Пондопуло, М. И. Соколов, Г. И. Чуриков и др.). В ноябре 1941 года для укомплектования пятых (дешифровальных) отделений разведотделов штабов фронтов туда направили всех выпускников спецотделения разведывательных (дешифровальных) курсов усовершенствования Высшей школы Генштаба.

К сожалению, авторам не удалось найти сведения о всех этих людях. При-

ведем краткие биографии В. С. Полина, Г. И. Пондопуло, М. И. Соколова, М. С. Одноробова, а также И. Я. Верченко.

ВЛАДИМИР ПОЛИН

Полин Владимир Степанович (1907–1975). Кандидат технических наук полковник В. С. Полин родился 19 июля 1907 года в Туле в семье потомственного оружейника. Перед Великой Отечественной войной успел защитить кандидатскую диссертацию в Московском педагогическом институте им. Карла Либкнехта. Пришел в криптографическую службу после всеобщей мобилизации в июне 1941 года и вскоре стал конструктором и организатором применения вспомогательной техники криптоанализа. Его труд во время войны отмечен несколькими орденами и медалями. Позднее, во время гонений на кибернетику как «буржуазную лженауку», Полин собирал коллектив единомышленников для создания ЭВМ общего и специального применения. В заслугу этому коллективу можно по-

ставить разработку целого ряда компьютеров. В частности, одна из последних в Союзе ламповых машин «Иней» и одна из первых в стране ЭВМ 2-го поколения полупроводниковая «Весна» превосходили по ряду параметров широко известные отечественные М-20 и БЭСМ-6 и долго работали во многих отраслях науки и промышленности. За эти работы В. С. Полин, его соратникам и ученикам — в том числе и воспитанникам Школы криптографов — впервые в истории ГУСС была присуждена Ленинская премия.

В. С. Полин преподавал в Высшей школе криптографов дисциплину о вспомогательной технике криптоанализа. Эта техника в то время представляла собой отдельные релейные или многоламповые устройства, облегчавшие криптографу трудоёмкие процессы статистического анализа шифрперехвата, однако было ясно, что вскоре ей предстоит занять в криптоанализе более важное место. Умер Владимир Степанович 20 августа 1975 года [Кузьмин, 1998–2, с. 94].

ГЕОРГИЙ ПОНДОПУЛО

Пондопуло Георгий Иванович (1910–1994) родился на юге России в семье фельдшера и учительницы. В 1928 году окончил Краснодарский педагогический техникум и три года работал учителем в станице Смоленской. Там же был избран секретарем комсомольской ячейки. В 1932 году поступил на механико-математический факультет МГУ им. Ломоносова и в 1937 г. окончил его с отличием. Во время учебы в аспирантуре был избран секретарем комитета комсомола МГУ. К маю 1941 г. он полностью подготовил к защите диссертацию, посвященную обтеканию решетки газом при больших скоростях.

К этому времени он был призван в Спецслужбу Красной Армии. Однако в связи с тем, что все отзывы на его диссертацию уже были получены, а день защиты в Совете МГУ назначен, 26 июня командование в порядке исключения предоставило Георгию Ивановичу отпуск на полдня. Диплом кандидата наук он получил уже по окончании войны. В 1941–42 гг. Г. И. Пондопуло работал в Специальной службе Генерального штаба РККА. Приход в Службу Георгия Ивановича и других специалистов с основательной математической и технической подготовкой явился важным фактором активизации деятельности Службы, расширения фронта её работ, вне-



Владимир Полин



Георгий Пондопуло

дрения в её работу математических методов.

Ещё в апреле-мае 1941 года в отечественную криптографическую службу были направлены несколько десятков молодых математиков и физиков из МГУ и Военной академии связи. Они привнесли в криптографическую работу новые идеи. Вот что пишет о вкладе этих специалистов Л. А. Кузьмин: «Если «старики» умели кропотливо, шаг за шагом накапливать сведения о ключе шифра противника, то математики, анализируя логику построения лишь частично известного ключа, находили алгоритмы его существенного пополнения. Инженеры и физики начали создавать и внедрять в анализ шифров вспомогательную технику. Эти два фактора способствовали совершению качественного скачка в раскрытии часто

изменяющихся ключей вермахта. Уже к началу Курской битвы такие методы стали приносить Ставке ценнейший материал о перегруппировках сил противника и его планах» [Кузьмин, 1998–2, с. 91]. Немалый вклад в становление этих методов внес Г. И. Пондопуло. Вообще следует отметить, что в ходе войны он занимался исследованием наиболее сложных шифрсистем противника [Кузьмин, 1998–2], [Кузьмин, 1999].

С 1942 по 1946 год Г. И. Пондопуло проходил службу в НКВД (НКГБ) на различных должностях от старшего оперуполномоченного до заместителя начальника отдела. В 1946–50 гг. он работал в МГБ СССР в должности заместителя начальника отдела. Георгий Иванович обладал высоким авторитетом среди советских математиков и механиков. Вполне закономерно, что, когда в 1949 году для подготовки специалистов по криптографии было организовано закрытое отделение мехмата МГУ, его возглавил именно Г. И. Пондопуло. Он также являлся заместителем декана мехмата МГУ, при этом педагогической деятельностью Георгий Иванович занимался по совместительству без отрыва от основной службы. Обладая хорошей математической и криптографической подготовкой, Г. И. Пондопуло многое сделал для организации, становления и развития закрытого отделения, в частности он преподавал новые математические методы анализа современных шифров. Выпускники отделения имели глубокие математические знания и в значительной степени способствовали повышению научного уровня работы ГУСС (в 1949 году было создано Главное Управление Специальной Службы — основная криптографи-



Строительство главного здания МГУ, 1951 г.

ческая организация страны) и успешно-му решению стоящих перед ним задач. В 1950–53 гг. Г.И. Пондопуло был начальником лаборатории в НИИ-1 ГУСС при ЦК ВКП (б). Пребывая на этих должностях, он продолжал научную работу по исследованию глубоких свойств современных шифров [Кузьмин, 1998–2], [Кузьмин, 1999], [Энциклопедия, 2004].

Совместно с И. Я. Верченко и Е. Ф. Баженовым Георгий Иванович принимал участие в становлении технического факультета Высшей школы КГБ. Заслуга в создании внутри чекистского вуза особой, неповторимой научной атмосферы, сочетавшей в себе высокую воинскую требовательность и дисциплину с глубоким уважением слушателей к своим педагогам, безусловно принадлежит профессорам И. Я. Верченко и Г. И. Пондопуло. С мая 1953 по 1976 год Георгий Иванович возглавлял кафедру криптографии на техническом факультете. Он внёс значительный вклад в подготовку специалистов для практических подразделений и уделял большое внимание подготовке научных кадров. Научные интересы Г.И. Пондопуло были связаны с изучением свойств дисковых шифраторов. Эти проблемы были весьма актуальны, ими занимались многие специалисты-криптографы (М. И. Соколов, Г. В. Чуриков, А. А. Блинов, В. И. Бобылев и многие др.).

Г.И. Пондопуло поддерживал тесный контакт с широким кругом представителей математической общественности СССР. Благодаря этому у слушателей и аспирантов имелась возможность посещать семинары крупных математиков: члена-корреспондента АН СССР Андрея Андреевича Маркова, академика (позже Героя Социалистического труда) Константина Константиновича Марджанишвили и др. Осуществлялось тесное взаимодействие с представите-

лями практических подразделений. Тесное творческое общение с прекрасными специалистами и уже накопленный опыт позволили преподавателям и сотрудникам приступить к работе над учебными пособиями на новом уровне [Кузьмин, 1999].

В 1965 году ВАК СССР утвердила Г. И. Пондопуло в звании профессора по кафедре прикладной математики, а Президиум Верховного Совета РСФСР 5 февраля 1975 года присудил почётное звание Заслуженного деятеля науки и техники (возможно, это единственный случай в Спецслужбе того времени). За свои заслуги перед страной Георгий Иванович награжден орденом «Знак Почета» и многими медалями, а также знаком «Почетный сотрудник госбезопасности». В отставку полковник Пондопуло вышел в 1976 году, после чего длительное время преподавал в Московском институте электронного машиностроения. Умер он 15 сентября 1994 года и похоронен на Хованском кладбище [Кузьмин, 1998–2], [Кузьмин, 1999], [Энциклопедия, 2004, с. 672–673].

МИХАИЛ СОКОЛОВ

Соколов Михаил Иванович (1914–1998) родился в Москве, детдомовец. В 1938 году с отличием окончил механико-математический факультет МГУ. Затем успешно окончил аспирантуру при НИИ Механики МГУ. В 1941 году М. И. Соколову была присвоена ученая степень кандидата физико-математических наук. С 1941 года работал в Специальной службе Генерального штаба Красной Армии, а затем в Специальной службе органов госбезопасности. Внес большой вклад в дешифрование шифр-переписки Германии и её союзников во время Великой Отечественной войны, а также подготовку молодых специалистов. После войны М. И. Соколов рабо-



Михаил Соколов

тал в криптографических подразделениях и продолжал преподавательскую деятельность.

М. И. Соколов был первым начальником кафедры криптографии в Высшей школе криптографов ГУСС. Он является автором многочисленных научных и учебно-методических работ. Также М. И. Соколов работал ученым секретарём в НИИ-1 ГУСС, был редактором ряда научно-технических сборников. Был научным руководителем шести аспирантов, которые успешно защитили диссертации. Доцент, старший научный сотрудник, полковник. Награжден двумя орденами и 20 медалями [Кузьмин, 1998–2], [Кузьмин, 1999], [Энциклопедия, 2004, с. 718].

МИХАИЛ ОДНОРОБОВ

Одноробов Михаил Спиридонович (1910–1997) окончил МГУ им. Ломоносова. В специальной службе с 1941 года по 1973 год. За 32 года своей работы внес заметный вклад в совершенствование советской криптографической службы и подготовку кадров для неё. М. С. Одноробов был криптографом военной мобилизации. Он внес немалый вклад в становление математических методов криптоанализа.

М. С. Одноробов был участником Великой Отечественной войны, в 1943–44 гг. был заместителем начальника

**ЗАСЛУГА В СОЗДАНИИ ВНУТРИ
ЧЕКИСТСКОГО ВУЗА ОСОБОЙ,
НЕПОВТОРИМОЙ НАУЧНОЙ
АТМОСФЕРЫ БЕЗУСЛОВНО
ПРИНАДЛЕЖИТ ПРОФЕССОРАМ
И. Я. ВЕРЧЕНКО И Г. И. ПОНДОПУЛО**



Михаил Одноробов

7-го Полевого отдела (1-й Белорусский фронт). После войны неоднократно выполнял поручения Правительства по оказанию помощи дружественным странам в организации шифрованной связи. С 1951 по 1965 годы был начальником отдела 8 Главного управления КГБ СССР. С 1965 по 1973 годы был начальником Службы 8 Главного управления.

М. С. Одноробов принимал активное участие в подготовке инженеров и специалистов для советской криптографической службы. В Высшей школе криптографов ГУСС Одноробов преподавал ряд дисциплин, в том числе «Основы криптографии». Вот что вспоминал Л. А. Кузьмин: «Лекции Михаила Спиридоновича состояли из двух частей. Первая содержала систематизированное описание классических шифров с анализом их слабостей и подходов к их взлому, вторая же знакомила с только что опубликованной в западной печати математической теори-



Связисты 1-го Белорусского фронта, 1944 г.

ей стойкости секретных систем Клода Шеннона. Практические занятия по курсу состояли, как и следовало ожидать, в дешифровании всё более сложных шифров. Это было столь увлекательно, что добрая половина группы «заболела» страстью раскрытия шифр-переписки, несмотря на заветы матерей, считавших, что «читать чужие письма — грешно!». Однако успехи советских криптографов времен войны заставляли забыть материнский наказ, находились и слова классиков марксизма (особенно Энгельса), подтверждавшие необходимость такой работы. И хотя не все однокурсники в дальнейшем посвятили свою жизнь

криптографии, думаю, что большинство «отступников» покинули её не из-за твёрдости своих моральных устоев, а испугавшись тягот каждодневного напряженного умственного труда, не отпускавшего мозг полностью даже во сне» [Кузьмин, 1998–2, с. 91].

Почетный сотрудник госбезопасности, полковник М. С. Одноробов был награжден орденами Красного Знамени, Отечественной войны и Красной Звезды (дважды), а также 25 медалями [Кузьмин, 1998–1], [Кузьмин, 1998–2], [Кузьмин, 1999], [Серов, 1994], [Энциклопедия, 2004, с.650].

(Окончание в следующем номере)

ЛИТЕРАТУРА

1. [Бутырский, 2012] Бутырский Л. С., Ларин Д. А., Шанкин Г. П. Криптографический фронт Великой Отечественной. Монография. М.: Гелиос АРВ, 2012. 2 изд. исправл. и дополн. М. 2013.
2. Голованов П. Н., Ларин Д. А. К 100-летию Г. И. Пондуполо. // Защита информации. INSIDE, Спб. 2010. № 3, с. 79.
3. [Калачев, 2000] Калачев Константин. В круге третьем. Воспоминания и размышления о работе Марфинской лаборатории в 1948–1951 годах. М.: Элиас рекордз, 2000.
4. [Код 2007] Код Верченко. Документальный фильм. Производство ЗАО «Видео-пресс», 2007.
5. [Кузьмин, 1998–1] Кузьмин Л. А. Не забывать своих героев // Защита информации. Конфидент № 1, 1998, с. 83–85.
6. [Кузьмин, 1998–2] Кузьмин Л. А. ГУСС — этап в развитии советской криптографии // Защита информации. Конфидент. № 4, 1998, с. 89–94.
7. [Кузьмин, 1999] Кузьмин Л. А. Становление кафедры криптографии // Защита информации. Конфидент. № 1–2, 1999, с. 85–90.
8. [Энциклопедия, 2004] Энциклопедия секретных служб России. М.: Астрель, 2004.



Валерий КУЛИКОВ
эксперт BIS Journal,
доктор технических
наук

КАК В МЕДИЦИНЕ...

ПРИНЦИПЫ БОРЬБЫ С ИММУНОДЕФИЦИТОМ ИБ В ИТ-ИНФРАСТРУКТУРЕ

Так уж случилось, что наиболее узнаваемые метафоры и аналогии в ИБ связаны с биологией и медициной. Началось всё с вирусов, червей и коней, сегодня же актуальна тематика профилактики, здорового образа жизни и ИБ-иммунитета ИТ.

«Иммунитет» ИТ-системы к рискам информационной безопасности бази-

руется на отказоустойчивости вычислительной платформы и сетевой инфраструктуры, а также на программном обеспечении, защищённом от «дурака», от умных хакеров (будь они хоть в джинсах, хоть в погонах), и от конфликтов внутри себя. Эти краеугольные камни иммунитета ИТ должны быть подкреплены надёжным хранением и резервным копированием данных.

Рынок в избытке предлагает вычислительные платформы, оборудование и технологии для создания сетей, программные приложения, системы и технологии хранения и резервного копирования данных. Но почему эти штуки, собранные в единую ИТ-систему, зачастую оказываются беззащитны перед непрошенными вторжениями или отказывают в доступе добросовестным пользователям?



В МИРЕ БИЗНЕСА, В ТОМ ЧИСЛЕ И СВЯЗАННОГО С ИТ, БАЛОМ ПРАВЯТ СЕГОДНЯ БУХГАЛТЕРА И ЮРИСТЫ, ОТЯГОЩЁННЫЕ, КАК ПРАВИЛО, ДИПЛОМАМИ MBA, А НЕ СТЕПЕНЬЮ PhD. ДЛЯ ТЕХНИКИ БУХГАЛТЕРСКИЙ ДИКТАТ ОКАЗЫВАЕТСЯ ГУБИТЕЛЕН

тив может исходить как от вендоров с интеграторами, так и от заказчиков.

Развитие компьютерных технологий в части оборудования приводит к тому, что всё большие функциональные возможности «упаковываются» во всё меньшие габариты. При этом самим разработчикам до конца не понятно, как работают транзисторы с характерными размерами конструктивных элементов размерами в несколько атомных слоёв, как обрабатываются пакеты данных на частотах в сотни мегагерц и вплоть до гигагерц. А это не способствует надёжности работы, а, стало быть, целостности данных и доступности систем.

Отдельного упоминания стоит качество программного кода. Тут вспоминается «забавный» эпизод: при перелёте несколько американских F-22 с Гавайских островов на базу ВВС Кадена на Окинаве в первые годы эксплуатации этих машин, после пересечения международной линии перемены дат истребителям пришлось вернуться на Гавайи, т.к. бортовые компьютеры автоматически интерпретировали ситуацию как слишком долгое пребывание в воздухе и предпосылку к исчерпанию запасов топлива. Достоверных официальных результатов расследования инцидента найти не удалось, но вполне вероятно, что корень зла кроется в принципах agile и латентном аутсорсинге.

В мире бизнеса, в том числе и связанного с ИТ, балом правят сегодня бухгалтера и юристы, отягощённые, как правило, дипломами MBA, а не степенью PhD. Для техники бухгалтерский диктат оказывается губителен. Постановка во главу угла т.н. эффективности в однобоком понимании её смысла в снижении собственных финансовых издержек вкупе со стремлением к быстрому выходу на рынок

с новым товаром приводит к тому, что падает не только надёжность предлагаемых ИТ-продуктов при эксплуатации, но зачастую и сами эти продукты представляют собой бета-версии, предлагаемые фактически для тестирования заказчиком. Для примера можно вспомнить эпопею с серверами на базе Itanium. Благо, что этот, похоже, завершившийся, эксперимент был инициирован компаниями, неплохо упакованными финансово и оказавшимися способными сохранять относительно хорошую мину при плохой (так уж случилось, и это не вина, а беда) игре.

Не играет на руку ИБ и скудость технической документации всё более сложной продукции, что делает потребителя полностью зависимым от службы поддержки компании-производителя. А в техподдержке в силу всё того же бухгалтерского понимания «эффективности» прямая связь между заказчиками и собственно инженерами вендора разорвана слоем «технических представителей», компетенции которых хватает зачастую лишь на трансляцию вопросов заказчиков на следующий уровень технической поддержки. Это может растянуть процесс консультации до неприемлемых времён.

Для нашей страны все описанные предпосылки к «иммунодефициту» ИБ в развернутых ИТ-системах во много крат острее из-за отсутствия собственной индустрии ИТ и краха системы технического регулирования использования оборудования для ответственных применений.

При наличии же двух только что упомянутых факторов — отрасли и системы технического регулирования — вполне возможно появление ИТ-оборудования со встроенными при рождении компонентами для под-

«ДИРЕКТОР, ЛЫСЫЙ ЧЁРТ, ПОЩЁЛКАЛ СЧЁТАМИ, БУРКНУЛ: «КРИЗИС», И ВЫВЕСИЛ СЛОВО «РАСЧЁТ»

Есть как объективные, так и субъективные причины, которые в ряде случаев дают негативный синергетический эффект с точки зрения влияния на ИБ. Речь идёт об объективном усложнении техники и субъективных представлениях бизнеса о том, «что такое хорошо и что такое плохо» при создании ИТ-оборудования и эксплуатации ИТ-систем. Причём говоря о бизнесе, нега-

держки информационной безопасности, включая гарантии высокой доступности, минимизацию возможностей для отказа в обслуживании.

«А ЕСЛИ В ПАРТИЮ СГРУДИЛИСЬ МАЛЫЕ — СДАЙСЯ, ВРАГ, ЗАМРИ И ЛЯГ...»

Примером осознанного внутриотраслевого технического регулирования могут служить процессы в телекоммуникационной индустрии. В начале 2000-х годов усилиями лидеров отрасли был сформирован базисный набор стандартов, соответствующих специфическим требованиям телекоммуникационной индустрии и определяющих «лицо» платформы:

◆ Семейство спецификаций PICMG Advanced Telecom Computing Architecture (AdvancedTCA) объединило на-

бор рекомендаций по созданию аппаратной платформы.

◆ В качестве решения для массового применения утвердилась ОС Carrier Grade Linux (см. врезку), операционная система консорциума OSDL (Open Source Development Labs, некоммерческий консорциум десятков компаний по развитию Linux).

◆ На основе спецификаций организации Service Availability Forum (SA Forum) были сформированы принципы управления вычислительной телекоммуникационной платформой как системой (platform management) и принципы поддержки технологии высокой готовности (high availability).

В 2006 году в отрасли были созданы две новые организации, работа которых должна была окончательно подготовить почву для «запуска» про-

изводства конкурирующего коммуникационного оборудования на базе стандартной платформы:

◆ Оформился альянс SCOPE Alliance для помощи рынку в создании и продвижении платформ операторского класса на основе «строительных блоков», созданных на базе концепций использования продуктов класса Commercial Off The Shelf (COTS) и Free Open Source Software (FOSS). Альянс SCOPE не «генерировал» стандарты, но вырабатывал рекомендации, которые делали бы возможным использование COTS- и Open Source-продуктов, созданных на базе спецификаций других промышленных объединений, работающих в сфере стандартизации, включая деятельность по пропаганде мероприятий для поддержки совместимости оборудования.

CARRIER GRADE LINUX

Разработка для телекоммуникационного оборудования открытой операционной системы семейства Linux была инициирована Лабораторией по разработке программных продуктов на базе принципов Open Source (Open Source Development Laboratory, OSDL). Проект CGL объединил специалистов компаний, представляющих разные элементы телекоммуникационной экосистемы: операторы связи, производители сетевого оборудования (network equipment providers, NEPs), производители телекоммуникационного оборудования (telecom equipment manufactures, TEMs), независимые производители программного обеспечения (independent software vendors, ISVs), дистрибутеры Linux.

Штабом проекта стала рабочая группа CGL Working Group (OSDL Carrier Grade Linux Working Group). Ею были выработаны рекомендации по дополнению базовой операционной системы Linux компонентами, обеспечивающими соответствие уровню операторского класса реализацию таких характеристик, как масштабируемость и информационная безопасность, включая высокую готовность и отказоустойчивость. CGL Working Group занялась также изучением ре-

зультатов проектов в области развития компонентов важнейших клонов Linux для использования лучшего опыта этих проектов, инициации проектов на базе принципов Open Source для создания необходимых компонентов и интерфейсов.

Регистрация дистрибутива Carrier Grade Linux означает, что его вендор полностью раскрыл способы, с помощью которых были выполнены приоритетные требования стандарта (priority 1 requirements from the CGL Requirements Definition). Разработаны документированные указания по поводу того, какие данные следует представить для подтверждения соответствия. Подтверждающая регистрацию информация публикуется на сайте производителя дистрибутива и на сайте OSDL. Если производитель дистрибутива не проводит проверку реализации каких-либо приоритетных требований стандарта CGL, он может привести обоснование для этого. Зарегистрированным дистрибутивам Carrier Grade Linux присваивается классификация «OSDL CGL Registered».

Carrier Grade Linux позволяет управлять системной архитектурой в ИТ, управлять восстановлением узлов сети

и других ресурсов после возможных сбоев.

Использование Carrier Grade Linux уместно в центрах обработки данных (ЦОД), где работает множество приложений, связанных с обработкой больших объемов данных и множество систем, для которых необходимо обеспечение высокой доступности на уровне 5 или 6 девяток.

В корпоративных ИТ место Carrier Grade Linux прежде всего в системах, работоспособность которых наиболее критична для бизнеса. Операционные системы класса CGL могут применяться и в центре, и на периферии корпоративной ИТ-инфраструктуры, где используются кластеризованные системы, поддерживающие резервирование. В этих применениях дополнительные возможности Linux операторского класса в части системного мониторинга и сокращения времени восстановления после сбоев, которыми не обладают «классические» дистрибутивы Linux корпоративного уровня, являются конкурентными преимуществами.

Интерес к Carrier Grade Linux проявляют аэрокосмическая и оборонная промышленность, ИТ-технологии в медицине и приборостроение.

♦ Сформирована Ассоциация производителей коммуникационных платформ (Communications Platforms Trade Association / CP-TA), занявшаяся развитием практики применения сертификационных процедур для подтверждения совместимости работы оборудования от разных поставщиков.

На сегодняшний день существует несколько дистрибутивов, отвечающих требованиям спецификации Carrier Grade Linux, на рынке работает десятки поставщиков телекоммуникационного и сетевого оборудования, предлагающих платформы, поддерживающие и поддерживаемые ОС класса Carrier Grade Linux.

«ВРЕМЯ ПОТОМУ, ЧТО РЕЗКАЯ ТОСКА СТАЛА ЯСНОЙ ОСОЗНАННОЙ БОЛЬЮ...»

Приведённый пример создания рамок основ для производства продуктов и управления качеством телекоммуникационного оборудования со встроенным ИБ-иммунитетом является примером т.н. «открытой» стандартизации. Её рабочие процессы направлены на поддержание долгосрочного диалога сторон на основе открытых встреч, достижения консенсуса на каждом этапе согласований и постоянного улучшения стандарта.

«Открытый» стандарт не служит односторонним выгодам какого-то участника рынка, доступен для участников процесса, служит развитию рынка и не препятствует «проприетарным» инновациям отдельных компаний (для этого неизменными сохраняются стандартизованные интерфейсы для сопряжения с внешним окружением).

Положительный опыт технического регулирования был и в нашей стране. В связи с этим предлагаем читателям возможность поиска плодотворных аналогий обеспечения ИБ-иммунитета ИТ с системой обеспечения единства и точности измерений, успешно разработанной, документированной и поддерживаемой в своё время Госстандартом СССР.

При этом в связи с возможными возражениями по части жёсткости былой отечественной системы стандартизации напомним, что в нашей стране стандарты подразделялись на



ряд категорий: государственные стандарты (ГОСТы), утверждаемые Госстандартом СССР (за исключением стандартов, утверждаемых Советом Министров СССР, Госстроем СССР и министерством здравоохранения СССР) и действующие на всей территории СССР; отраслевые стандарты (ОСТы), утверждаемые министерством и обязательные для всех предприятий отрасли; республиканские стандарты союзных республик (РСТ), утверждаемые Советом Министров республики и обязательные для всех предприятий, расположенных на её территории, независимо от ведомственного подчинения; стандарты предприятий и объединений (СТП), обязательные только для предприятия, утвердившего данные стандарты.

Уместность воспоминаний о государственных инициативах в сфере стандартизации, которые также могут происходить на основе принципов «открытой» стандартизации связана с тем, что имеется не только былой отечественный опыт, но и достаточно недавний пример из практики ЕС, а именно проект INTERESTED (INTERoperable Embedded Systems Tool chain for Enhanced rapid Design, prototyping and code generation, набор совместимых инструментальных средств для быстрой

качественной разработки, прототипирования и генерации кода [для приложений для встроенных систем]).

Его инициация была обусловлена бухгалтерскими аспектами (снижение издержек компаний на производство программных приложений), необходимостью повышения качества программного кода, что очевидно важно для обеспечения ИБ, а также (sic!) и необходимостью:

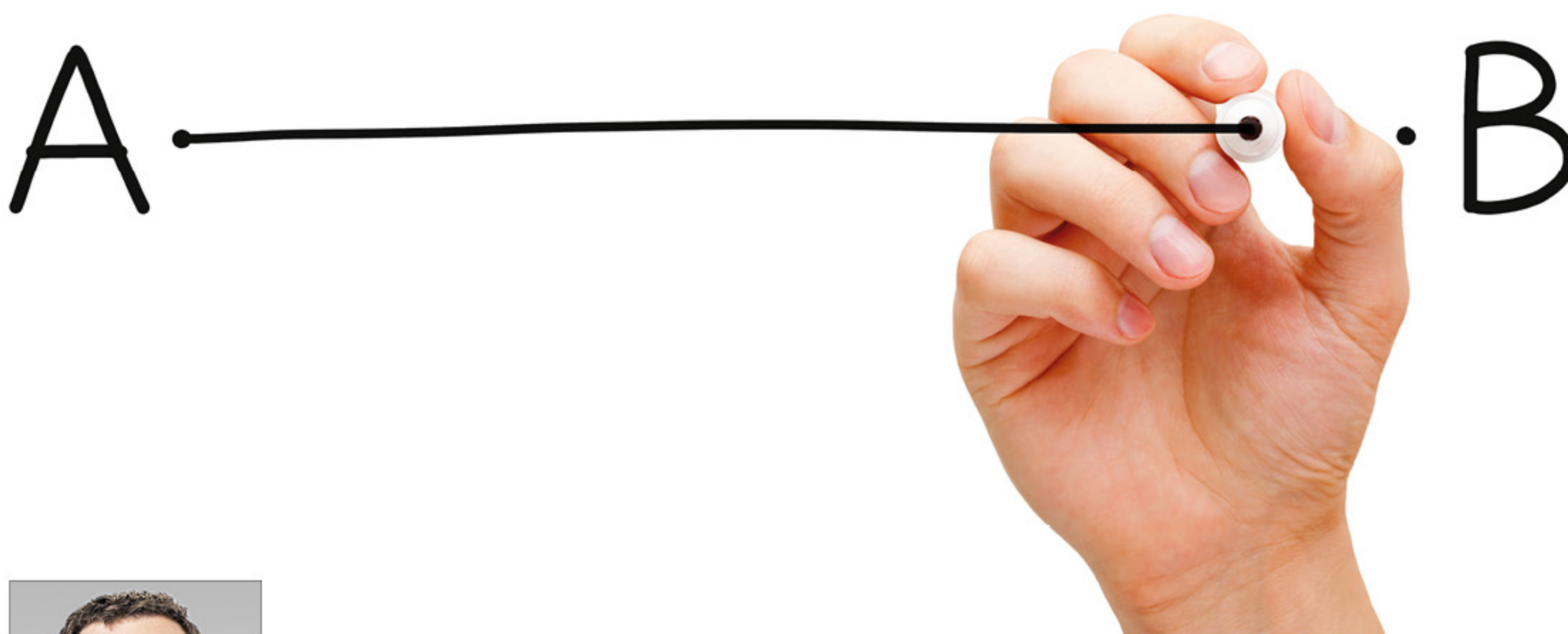
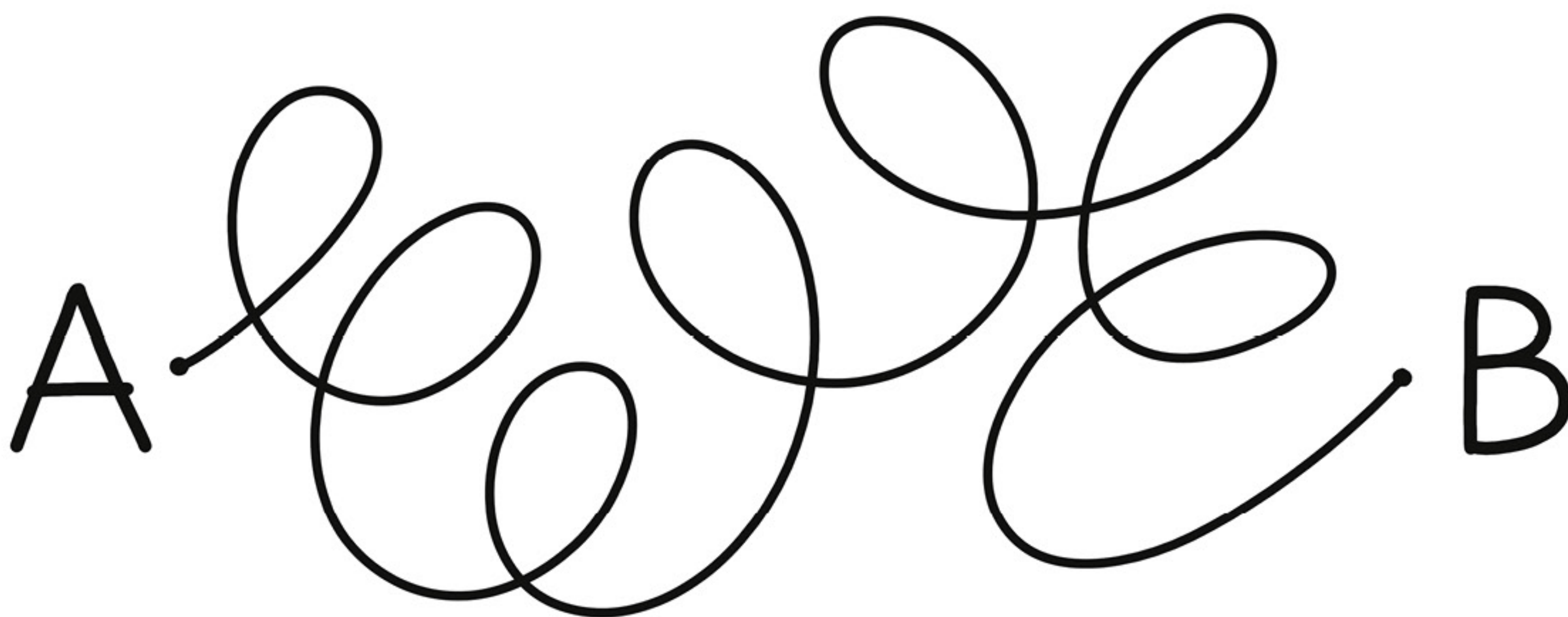
- ♦ укрепления лидерства европейской науки и инженерии;
- ♦ создания специализированного научного направления в Европе;
- ♦ содействия возникновению и росту высокотехнологичных европейских компаний.

* * *

То есть госпроекты в области ИТ (подобные INTERESTED) вполне могут иметь отраслеобразующее и отраслеконсолидирующее значение, что актуально для отечественных ИТ в целом и их ИБ-иммунитета в частности. А консолидация отрасли ИТ под знамёнами ИБ с помощью механизмов технического регулирования является безусловно необходимым условием для перехода к «цифровой экономике».

СИЛА ПРОСТОТЫ

ЗАМЕТКИ БЕЗОПАСНИКА



Александр БОДРИК
заместитель генерального
директора ANGARA
Professional Assistance,
CISA, ITIL Expert

УРОКИ КИБЕРРАЗВЕДКИ

Семь лет назад я работал аналитиком подразделения Global Research одной из крупнейших на тот момент киберразведывательных компаний. В сферу интересов компании входило все, что касалось киберпреступлений, отмыва денежных средств, «мягкого» мошенничества («партнерки», спам и т.п.).

Клиентами компании были крупнейшие мировые корпорации в сферах фи-

нансов и ИТ, и они регулярно покупали продукты компании — информационные отчеты. Отчеты содержали описания различных типов угроз и уязвимостей, а также рекомендации — как защититься от них наиболее быстро и качественно.

Что интересно, в этих рекомендациях практически не упоминались специфические продукты безопасности. Рекомендации были намного — на-

много! — проще и банальней: поставьте обновление, посмотрите журналы событий, запустите проверку, обучите пользователей. Единственное, что их отличало, они были предельно конкретны: что именно проверить, где именно смотреть и какие именно обновления ставить.

Как показал недавний WannaCry, эти простые советы актуальны и по сей день. Но не стоит думать, что CISO их не знают.

КОРПОРАТИВНЫЕ «КАНЬОНЫ»

Информационная безопасность как вид наиболее заметна в корпорациях. Там уже есть определенная специализация, есть активы, что надо бы защитить, есть клиенты, президент, которых желательно развести в случае серьезных инцидентов... Все аспекты корпоративной жизни управляются с помощью внутренних законов и правил, управление безопасностью корпорации — не исключение.

Но регламент регламентом, а влияние в корпорациях все равно больше у бизнес-руководителей, людей, что приносят деньги, обслуживают клиентов, решают проблемы с правительством, прессой и привлечением финансирования. В такой компании CISO может (и часто так оно и есть) выглядеть «бедным родственником» — вроде отвечает за информационную безопасность, а ресурсов не дают, и, нередко случается, делают «стрелочником».

Особенно «вдохновляют» вопросы общей инфраструктуры, например, установка обновлений. С одной стороны, без установки обновлений уязвимость сети корпорации растет, с другой, эта самая установка имеет прямую цену (стоимость времени сотрудников) и непрямую — риск сбоя в работе информационных систем, многие из которых (особенно в промышленных корпорациях) построены в незапамятные времена незнамо кем и незнамо как.

Никто не может поручиться, что после установки обновлений бизнес-процесс, приносящий миллиарды долларов, не встанет, а значит, обновления откладываются минимум до следующего согласованного перерыва в обслуживании. То есть обновления производятся максимум раз в квартал. И повлиять на

этот процесс CISO крайне сложно — не он деньги зарабатывает (это функция продаж и маркетинга), не он и тратит основную их часть (это функции производства и капитальных инвестиций).

УРОКИ СОСЕДЕЙ

Кроме информационной безопасности в корпорациях существует много других служб — юристы, бухгалтера, финансисты, АХО, HR. Развиваясь более длительное, чем службы ИБ, время они нашли рецепты адекватного и эффективного влияния на бизнес и смогли выстроить устойчивые системы управления и контроля своих аспектов деятельности в корпорации. Особенно отличились здесь финансисты.

Например, они внедряют P&L ответственность. Это значит, что каждое бизнес-подразделение отвечает за свою финансовую прибыльность, получает бонусы, только если их заработает и отвечает за свою деятельность как в части доходов, так и в части затрат. В области информационной безопасности существует аналогичная мера, а именно ответственность за активы. Эта простая мера приравнивает информационные активы к финансовым и иным активам бизнес-направлений и позволяет довести простую мысль: если бизнес не озабочится своей безопасностью, то он же пострадает от убытков.

Вторая критичная практика — окупаемость инвестиций. На языке ИБ это означает, что от инвестиций в ИБ должен быть понятный эффект. А значит, постройка пирамиды Хеопса в виде SOC за миллиард рублей в течение трех лет — это много хуже, чем небольшие инвестиции в обучение команды ИБ, чтобы хотя бы начать смотреть существующие IDS уже завтра. Тем более, что если инженеры не смотрят IDS, то с чего они будут смотреть более сложные и непонятные системы класса SIEM? Они ведь на порядок сложнее IDS, требуют настройки не только самих себя, но и источников событий.

Третья практика относится к дисциплине по слияниям и поглощениям. Если кратко, растущим направлениям дают денег, бюджеты стагнирующих режут. Это приводит нас к итеративному и гибкому подходу к ИБ: сделали А — получили бизнес-эффект (быструю по-

беду или quick win), сделали Б, и так по спирали, все время развивая полученный эффект. Не развиваемся — стагнируем в глазах руководства, отстаем от коллег по корпорации.

Четвертая практика пришла из финансового анализа — анализ по накопленным инвестициям. В информационной безопасности накопить инвестиции в технологии крайне трудно, но возможно в персонале и знаниях. К сожалению, из встреченных мной служб ИБ только единицы создавали форумы и википедии по ИБ, единицы извлекали максимум полезного из накопленного человеческого капитала — перекрестное обучение, менторство, и, конечно, удержание персонала.

СИНЕРГИЯ ПРОСТЫХ ПРАКТИК

Приведенные 4 практики вместе с 4 классическими (всего 8 практик вместо десятков из стандартов) — сильные пароли, установленные обновления, отключение лишних служб и обученный персонал — дополняют и усиливают друг друга. Ответственность за информационные активы помогает бизнес-руководителям понять, что слабые пароли — это их проблема. Это их информацию сотрудники унесут конкурентам. Отсутствие установленных обновлений останавливает их бизнес-процессы после очередного WannaCry, а невнимательный персонал накликает еще не одну беду.

КОНТРОЛЬ НА ВХОДЕ

«Хорошо быть богатым и здоровым», — так, наверняка, подумали многие CISO, дочитав до этого момента. И правда, многие компании пребывают в перманентном бардаке и для них P&L ответственность — это нечто запредельное. Совет тут может быть только один: не нужно в таких компаниях работать. Профессионал всегда найдет себе место, а «мастер каратэ не пойдет в темный переулок». Со временем компании без CISO просто потеряют конкурентоспособность — информацию сольют конкурентам, вирусы приостановят процессы, а бэкапы окажутся на основном сервере (реальный кейс ТОП-5 компаний агропромышленного сектора России). В результате им придется уйти с рынка, а на их месте появятся новые, с более зрелым подходом.

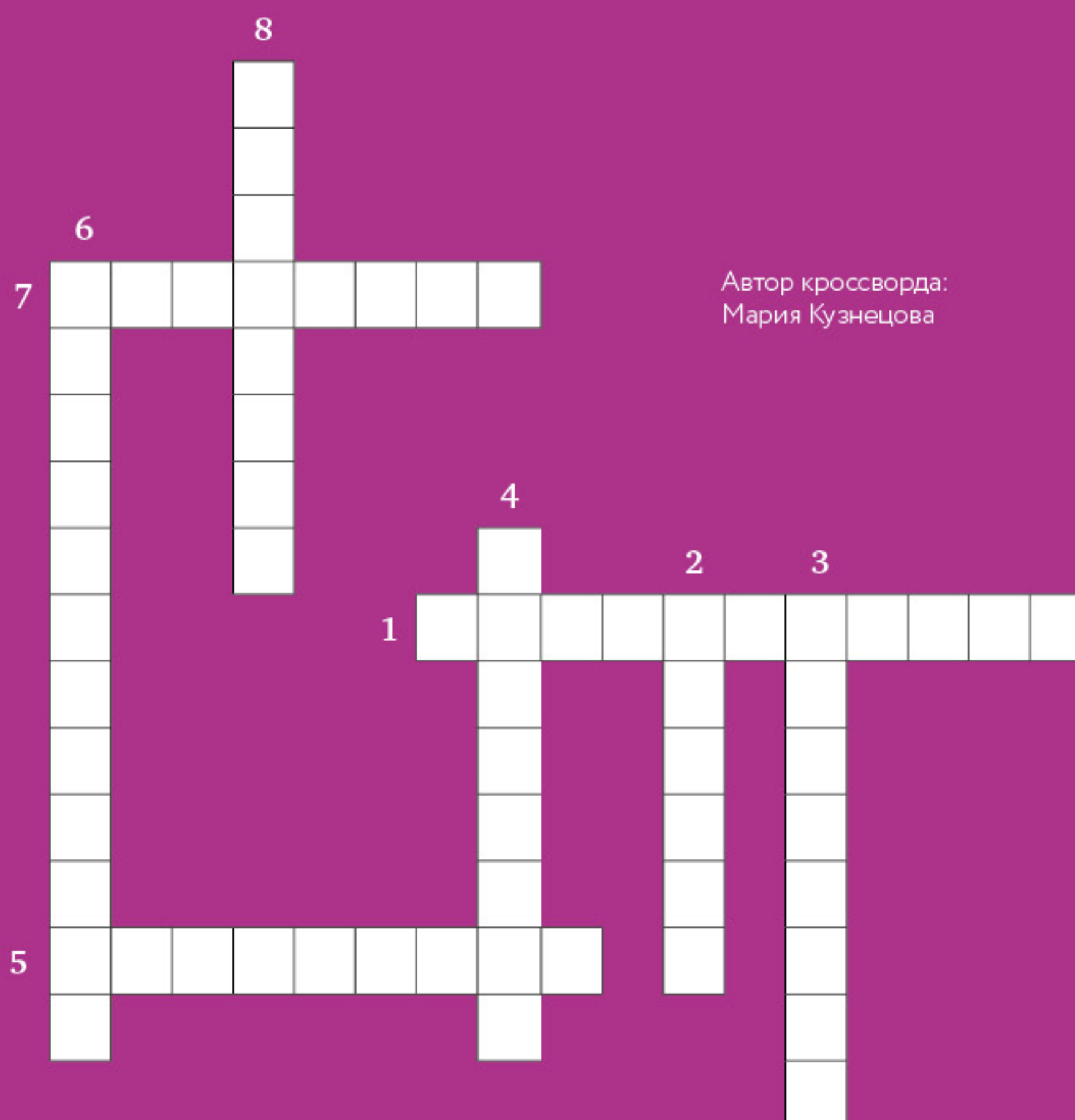
КРОССВОРД

ПО ГОРИЗОНТАЛИ

1. Регистрация данных, защищенных третьей стороной, что в дальнейшем позволяет обеспечить точность характеристик данных.
5. Программа или аппаратное устройство, предназначенные для перехвата клавиатурного ввода.
7. Более чем однократное использование компонента при различном выполнении операций.

ПО ВЕРТИКАЛИ:

2. Программа, предназначенная для сокрытия в системе определенных объектов, либо активности.
3. Одна из специализаций внутри организованных преступных группировок, занимающихся технологиями интернет-мошенничества.
4. Распространившаяся в 2008 году вредоносная программа, создающая bot-сети.
6. Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленных к зашифрованным данным.
8. Пара букв (символов), блоков текста в криптографии.



Автор кроссворда:
Мария Кузнецова

КАК ВСЕ ЗАПУЩЕНО!

Вир-р-усы!
Вир-р-усы!



БЛОГЕРЫ УСМЕХАЮТСЯ

Если вас ещё не взломали, то это не ваша заслуга.

В любом программном коде есть ошибки.

Инвестиции в безопасность — это всего лишь повышение стоимости взлома.

Для защиты от кибератак требуется не индивидуальный, а индустриальный ответ.

Использование зарубежных ИТ-технологий — гарантия незадекларированной функциональности.

Основная защитная мера от киберугроз — молитва.

Любое ТЗ постоянно меняется — зафиксировать его невозможно.

Всё, что для бизнеса возможности, для безопасности — угрозы.

Неопределенность в сфере ИБ становится доминирующей, и это точно не остаточный риск.

Разумный риск — это когда вы хотели рискнуть, но не рискнули.

Поделится Валерий Естехин
<https://estekhin.blogspot.ru>



Медиа Группа **АВАНГАРД**



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Книжное
издательство

Нам 10 лет!

12–16 ФЕВРАЛЯ 2018 ГОДА

ДЕСЯТЫЙ ЮБИЛЕЙНЫЙ УРАЛЬСКИЙ ФОРУМ

РЕГИСТРАЦИЯ ОТКРЫТА

ural.ib-bank.ru

