

- 12>** Эрнест ВАЛЕЕВ
Государственная Дума РФ
**Ответственность будет
соразмерна опасности**



- 16>** Георгий ЛУНТОВСКИЙ
Банк России
Вектор 2017 года

- 28>** Иван ЯНСОН
Сбербанк
**Новое время — новые
инструменты**

- 34>** Матвей ГЕРИНГ
SWIFT
**Повышаем самооценку
банков**



- 38>** Сергей ДЕМИДОВ
Московская биржа
**Киберустойчивость биржи
полна оттенков**

КУЛЬТУРА ИБ — ЗАЛОГ КИБЕРУСТОЙЧИВОСТИ



VI симпозиум «Современные тенденции в криптографии»

Тематика симпозиума включает, но не ограничена следующими направлениями:

- исследование криптографических алгоритмов, в том числе анализ криптографических алгоритмов, являющихся международными стандартами;
- эффективная реализация методов анализа криптографических алгоритмов;
- оценка криптографической стойкости российских криптографических алгоритмов;
- эффективная реализация российских криптографических алгоритмов;
- перспективные направления в криптографии.

ОРГАНИЗАТОРЫ



ГЕНЕРАЛЬНЫЙ ПАРТНЕР



ОРГАНИЗАЦИОННАЯ ПОДДЕРЖКА



В рамках Симпозиума пройдёт обсуждение специальных тем в формате дискуссий:

1) Блокчейн: ожидания рынка и мнения экспертов

- опыт внедрения решений на основе технологии блокчейн: плюсы и минусы;
- безопасность решений на основе технологии блокчейн с позиции современных подходов к защите информации;
- пользовательские сценарии.

2) Квантовая криптография: от теории к практике

- использование квантовых криптографических систем в контексте существующей методологии создания СКЗИ (Методических рекомендаций ТК 26 «Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации»);
- необходимость и возможность нормативного регулирования разработки и применения квантовых криптографических систем;
- востребованность квантовых криптографических систем: технико-экономическая обоснованность против безопасности.



Артем ЗУБКОВ
генеральный директор
Медиа Группы
«Авангард»



Павел БЫЛЕВСКИЙ
шеф-редактор
BIS Journal

Наступило время маленьких торжеств. Вышел в свет 25-й — вполне юбилейный — номер журнала. Который, и это главное, предвещает 10-летие в мае своего издателя — Медиа Группы «Авангард».

Конечно, «25 номеров» и «10 лет» звучит не столь фундаментально, как век, полвека или даже четверть века, но и на дворе, извините, не XIX или XX век. Жизнь ускорилась до предела, темпы развития информационных технологий — словно только что разжали пружину, а в нашей отрасли — банковской и финансовых рынков — еще стремительней.

Совсем недавно, несколько лет назад хакеры мнили всесильными, электронные финансовые сервисы были всего лишь модным «довеском» к наличным деньгам и бумажным платёжкам, а информационная безопасность играла роль Золушки при дворе общей безопасности. Именно в те былинные времена на собственный страх и риск — издателя в первую очередь — выходит первый номер BIS Journal. Редколлегия формируется из подлинных профессионалов, в то же время — энтузиастов, верящих в новое начинание. Инициатива поддерживается отраслевыми регуляторами, тепло принимается читательской аудиторией, сразу проявляют интерес рекламодатели.

Сегодня отрасль, по нашим оценкам, завершила этап становления. Информационная безопасность правит бал, киберзащита становится задачей государственного уровня и масштаба, развивается целый свод федеральных законов, ведомственных нормативных актов.

Банк России регулирует информационную безопасность финансового рынка в целом, не только кредитных, но и других финансовых организаций — платёжных систем, страховых, инвестиционных, брокерских компаний... Вчерашние энтузиасты сейчас — зрелые маститые специалисты на ответственных постах. Ведётся сквозная профильная подготовка специалистов — школа, вуз, повышение квалификации. На повестке дня — ликбез для всех граждан в отношении правил информационной безопасности.

Рука об руку с развитием отрасли развивается и наш журнал. В онлайн-режиме выходит интернет-версия, ежеквартально — печатный «глянец». В полную мощь функционируют интернет-телевидение BIS TV и издательство специализированной литературы. На низком старте — проект кадрово-образовательного портала BIS JOB. Значительно расширились авторский коллектив и читательская аудитория, появились надежные друзья и партнеры.

Таким образом, бросив короткий взгляд на пройденный путь, видим: времени прошло мало, а сделано много. Но до ближайшего — большого — юбилея предстоит сделать многократно больше. И, главное, быстрее.

Еще быстрее!

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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

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

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

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Былевский П.Г. — шеф-редактор, кандидат философских наук
Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков,

руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук

Виноградов А.Ю. — начальник управления информационной безопасности АО КБ «Златкомбанк»

Вихорев С.В. — директор по информационной безопасности Филиала «ПЕТЕР-СЕРВИС Спецтехнологии»

Дзержинский Ф.Я. — главный эксперт — координатор системной экспертизы блока «информационные технологии» департамента информационных технологий ОАО «Промсвязьбанк», CSDP

Зубков А.Н. — генеральный директор

ООО «Медиа Группа „Авангард“»

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 «Национальная система платёжных карт», кандидат технических наук

Пазизин 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

Филипчук А.А. — вице-президент АБ «ГПБ-ипотека» (группа «Газпромбанк»)

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**

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, 37.611150

Тел./факс: +7 499 271-70-85

Интернет-версия: journalib-bank.ru

E-mail: bis@ib-bank.ru

Отдел рекламы: reklama@ib-bank.ru

Отдел распространения: tirazh@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство ПИ № ФС77-55062 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 03.04.2017. Тираж 7000 экз.

Заказ № 675/V87. Цена договорная.

Отпечатан в «Типографии на Угрешской»

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

Тел. +7 495 720-62-28

© BIS Journal, 2017

НОВОСТИ

5 В России, в мире, криминал, угрозы

РЕГУЛЯТОРЫ

- 12** **Законодательство /**
Эрнест ВАЛЕЕВ (Государственная Дума)
Надёжный фундамент
- 16** **Стратегия /**
Георгий ЛУНТОВСКИЙ (Банк России)
Вектор 2017 года
- 21** **Стратегия /**
Владимир ЧИСТЮХИН (Банк России)
Бумажный век уходит в прошлое
- 25** **Киберустойчивость /**
Артем СЫЧЕВ (Банк России)
Киберустойчивость финансовой сферы:
что это такое?



БАНКИ

- 28** **Управление /**
Иван ЯНСОН (Сбербанк)
Партнерство с бизнесом и Agile
- 34** **SWIFT /**
Матвей ГЕРИНГ (SWIFT)
SWIFT повысит самооценку банков
- 38** **Биржи /**
Сергей ДЕМИДОВ (Московская биржа)
Разнообразие оттенков киберустойчивости
- 40** **Поисковые системы /**
Кирилл ЕРМАКОВ (QIWI)
Мировые тренды ИБ на службе финтеха
- 42** **ДБО /**
Анатолий МОРОЗОВ,
Александр БОНДАРЕНКО (Сбербанк)
Ключ для ДБО





УГРОЗЫ И РЕШЕНИЯ

- 46** **Идентификация /**
Алексей САБАНОВ («Аладдин Р.Д.»)
Такая разная...
- 48** **Инструментарий /**
Сергей ВАХОНИН («Смарт Лайн Инк»)
Банк России поднимает требования по борьбе с утечками информации на уровень отраслевого стандарта
- 50** **SIEM /**
Андрей БИРЮКОВ (АМТ-ГРУП)
SIEM в финансовой сфере
- 52** **VPN-продукты /**
Александр ВЕСЕЛОВ (С-Терра СиЭсПи)
Старая сказка на новый лад



ИНФРАСТРУКТУРА

- 54** **Деловые мероприятия /**
Компас для безопасника.
Дневник IX Уральского форума
- 62** **Олимпиады /**
Герои научных горизонтов



ОБРАЗОВАНИЕ И КАРЬЕРА

- 64** **Стандарты /**
Андрей ВЫБОРНОВ (Банк России)
Кадры по новым стандартам
- 67** **Корпоративная культура /**
Александр ГОЛУБЕВ (Вымпелком)
Осведомленный сотрудник —
защищенная компания
- 69** **Корпоративная культура /**
Алексей ГОРЕЛКИН («Лаборатория Касперского»)
Игра в безопасность
- 72** **Обзор /**
Марина БРОДСКАЯ (BIS Journal)
Сам себе учитель
- 75** **Обзор /**
Марина БРОДСКАЯ (BIS Journal)
Кибербезопасность в школах: у нас и у них



СУБЪЕКТЫ

- 78** **Корифеи /**
Геннадий ЕМЕЛЬЯНОВ (Академия криптографии РФ),
Дмитрий ЛАРИН (кандидат технических наук)
Шифры трех войн. О мастере взлома кодов
Б.А.Аронском
- 84** **История /**
Борис СТОЛПАКОВ (историк криптографии)
Сто лет назад. Триумф и трагедия радиоразведки
Балтийского флота
- 88** **Мысли вслух /**
Александр БОДРИК (ГК Иридис)
Заметки безопасника
- 90** **Мысли вслух /**
Павел РОГОВ (читатель BIS Journal)
Россия — Великобритания: люди и банки

ОФФТОПИК

- 92** **Блогеры улыбаются**
Кроссворд, юмор

НАТАЛЬЯ КАСПЕРСКАЯ СТАЛА «ЖЕНЩИНОЙ ГОДА-2016»

Президент ГК InfoWatch Наталья Касперская награждена премией Евразийского женского форума «Общественное признание: Женщина года-2016» в номинации «Высокие технологии и информационная безопасность». Церемония награждения прошла в Совете Федерации накануне Международного женского дня.

Председатель верхней палаты парламента РФ Валентина Матвиенко вручила премиальные сертификаты и ценные подарки отличившимся в различных номинациях руководителям крупнейших российских учреждений, институтов и компаний. «Сегодня мы чествуем женщин, внесших особый вклад в социально-экономическое развитие России. Их должны знать, на их примерах должна расти молодежь», — подчеркнула В.И. Матвиенко, отметив, что потенциал женщин огромен в продвижении позитивного образа России за рубежом.



«Я признательна Валентине Ивановне и всем участникам форума за высокую оценку моего труда. Группа компаний InfoWatch объединяет производителей решений по защите предприятий от внутренних и внешних угроз ИБ. Появление номинации «Высокие технологии и информационная безопасность» свидетельствует о понимании обществом важности защиты информации и о признании нашей работы», — прокомментировала Наталья Касперская.

К САЙТАМ-НАРУШИТЕЛЯМ ЗАКОНА «ЗАМЕДЛЯТ» ДОСТУП

Весной этого года правительство планирует внести в законодательство поправки, которые позволят «замедлять» доступ к сайтам компаний, нарушившим российские законы.

Многие иностранные интернет-компании не стали выполнять решения российских судов и госорганов, аргументируя это тем, что они подчиняются законам стран, в которых зарегистрированы. При этом, в случае принятия поправок, норма будет распространяться и на российские компании.



Отметим, что идея ввести новые поправки появилась в ходе обсуждений дела ФАС против американской корпорации Google. По словам специалистов, некоторые иностранные интернет-компании, работающие также и на территории России, не выполняют законы РФ. Так, Facebook и Twitter отказывались удалять противоправный контент по решениям судов, Роскомнадзор добился вечной блокировки в России социальной сети LinkedIn из-за нарушения закона о персональных данных.

В разработке законопроекта участвуют Федеральная антимонопольная служба (ФАС), Роскомнадзор и другие ведомства. В настоящий момент инициатива находится «на финальной стадии согласования» и проходит проверку в администрации президента.

РУССКИЕ СМАРТФОНЫ ХОРОШО ЗАЩИЩЕНЫ

Благодаря госзаказу на рынке РФ досрочно начались продажи российских смартфонов марки INOI с первой отечественной операционной системой, разработанной с ориентацией на повышенную информационную безопасность.

Для начала официальных продаж выпустили около 500 гаджетов. Есть основания полагать, что использование российской Sailfish Mobile OS Rus будет серьезным конкурентным преимуществом на рынке, особенно среди покупателей, которых беспокоит вопрос сохранности персональных данных.

Поводом для реализации отечественного проекта послужило то, что из 75 млн смартфонов около 94% работают на основе далеко небезопасных американских платформ Google и Apple.

В РОСГВАРДИИ ПОЯВИЛАСЬ КИБЕРРАЗВЕДКА

В Росгвардии создано подразделение киберразведки. В его обязанности в первую очередь входит мониторинг соцсетей для выявления случаев экстремизма.

Подразделению поставлены задачи по выявлению актуальных угроз и подготовке к отражению атак. Упор сделан на выявление экстремизма, однако функции киберразведчиков могут значительно расшириться. В частности, рассматривается вопрос о создании комплексной системы мониторинга Интернета. Возглавила подразделение Лариса Горячко, ранее работавшая в системе МВД РФ.

Напомним, что в декабре 2016 года первый замглавкома Росгвардии Сергей Меликов заявил, что одной из задач новой силовой структуры станет выявление угроз для Госстроя России.

САМАЯ БОЛЬШАЯ УТЕЧКА ДАННЫХ В 2017 ГОДУ

Обнаружен незащищенный общедоступный репозиторий резервных копий файлов, принадлежащих легальной маркетинговой компании RCM, ежедневно рассылающей порядка 1 млрд рекламных электронных писем.

Обнаруженная БД содержит электронные адреса, полные имена, IP-адреса и даже реальные адреса порядка 1,4 млрд человек. В базе также хранятся конфиденциальные сведения об операциях компании. Например, RCM за один день разослала спам-письма на 18 млн адресов Gmail, заработав \$36 тыс. Для пополнения базы спамеры используют незаконные техники. В том числе атаку Slowloris, заставляющую атакуемый сервер обслуживать множество открытых соединений путем непрерывной отправки незавершенных HTTP-запросов.

В США СУДЯТ «РУССКОГО ХАКЕРА»

Министерство юстиции США обвиняет «русского хакера» Марка Вартамяна в разработке и распространении в сети вируса «Цитадель». Ущерб, нанесенный вирусом, атаковавшим 11 млн компьютерных устройств, оценивают в сумму \$500 млн.

В ведомственном докладе США Вартамяна признали профессионалом мирового уровня и полагают, что его арест и изоляция ослабят киберпреступность в мире. Вартамян, известный в сетях как Kolymro, был арестован в Норвегии в 2015 году, а в прошлом году экстрадирован в США.

Российские эксперты сомневаются в методике определения ущерба. Они отмечают, что показатель 11 млн компьютеров не является существенным в международном масштабе, и потому не может стать основанием для приговора длительного срока наказания.

РЫНОК УСЛУГ ПО ИССЛЕДОВАНИЮ КИБЕРУГРОЗ ВЫРОС НА 23,1 %

Объем рынка услуг по исследованию киберугроз в 2016 году составил \$14,17 млн, что на 23,1% больше по сравнению с показателем 2015 года. Такие данные приводит компания IDC в обзоре Russia Threat Intelligence Security Services 2016 Market Analysis and 2017–2021 Forecast, посвященном ситуации на российском рынке услуг безопасности.

Ведущее положение на рынке, судя по обзору, занимает компания Group-IB. На втором и третьем местах в списке основных поставщиков находятся компании Positive Technologies и «Лаборатория Касперского». Вместе тройка лидеров генерирует более 70% от общего объема рынка.

В ходе исследования компания IDC рассмотрела факторы, стимулирующие и сдерживающие развитие рынка, а также составила прогнозы развития



рынка по его сегментам и отраслям экономики до 2021 года.

Как отметил старший аналитик IDC Россия и СНГ Денис Масленников, услуги по исследованию киберугроз являются одним из наиболее сложных сегментов всего рынка информационной безопасности. По его словам, растущее число киберугроз обусловит крайнюю востребованность услуг подобного рода. В этой связи российский рынок услуг по исследованию киберугроз в течение ближайших пяти лет будет стабильно расти, прогнозирует аналитик.

WIKILEAKS ПУБЛИКУЕТ СЕКРЕТЫ ЦРУ

Сайт WikiLeaks опубликовал первую порцию утечек из центра киберразведки ЦРУ США. Обнародованные документы рассказывают о глобальной программе для взлома устройств и тайной «хакерской» базе ЦРУ в Германии.

Первая порция публикаций получила название Year Zero. Она включает в себя свыше 8,7 тыс. документов и файлов, полученных из центра

киберразведки ЦРУ в Лэнгли, штат Виргиния. Данная серия публикаций, в частности, демонстрирует существование глобальной программы для взлома различных устройств и систем американского и европейского производств, таких как смартфоны iPhone от Apple, операционные системы Android от Google и Windows от Microsoft и даже телевизоры Samsung, которые способны были превращаться в записывающие устройства.

В пресс-релизе WikiLeaks также отмечается, что консульство США во Франкфурте-на-Майне в Германии является тайной «хакерской» базой ЦРУ для организации кибератак на Европу, Ближний Восток и Африку. Кроме того, утверждается в пресс-релизе WikiLeaks, ЦРУ крадет чужие компьютерные вирусы и может с их помощью устраивать кибератаки «под ложным флагом».





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.

СТИРАЛ СВЕДЕНИЯ О ШТРАФАХ

В Улан-Баторе арестовали 25-летнего хакера, обвиняемого в неоднократном взломе сервера центра управления дорожным движением Улан-Батора с целью уничтожения информации о штрафах за нарушение правил дорожного движения.

Хакер договаривался с нарушителями и за вознаграждение удалял с сервера сведения об их электронных штрафах. В настоящее время дело рассматривается в отделе Уголовной полиции по борьбе с интернет-преступностью. Также, немногим ранее, хакеры вывели из строя систему камер фото- и видеофиксации правонарушений в Подмоскowie. Причиной поломки камер стало вредоносное ПО, внедренное злоумышленниками в ходе кибератаки. В общей сложности в результате инцидента вышло из строя 120 из 144 камер.

ИЗ БЛАГОРОДНЫХ РАЗБОЙНИКОВ В ГНУСНЫЕ ВЫМОГАТЕЛИ

Компьютерные взломщики повсеместно начали разменивать свой талант на банальное вымогательство. К такому мнению пришли аналитики, отслеживающие деятельность, как хакерских групп, так и одиночек.

Амбиции хакеров первого и второго поколений остались в прошлом. «Робин Гуды» компьютерных сетей, для которых сам процесс взлома «жирной» банковской ячейки был сродни искусству, отошли в прошлое. Теперь жулики, называющие себя хакерами, занялись вымогательством денег не у политиков или банкиров, но у простых пользователей.

Технология кибер-вымогательства проста. Компьютерные вирусы могут блокировать ваши ПК, гаджеты, устройства в любое время. После чего вы получите уведомление о сделке, при согласии на которую у вас «все за-



работает». Сумма выкупа естественно меньше, чем та, которую придется выложить за покупку нового компьютера, планшета или смартфона. Кстати, эксперты предупреждают, что объектами шантажа могут стать и «умные» телевизоры, холодильники, игрушки, которые довольно просто дистанционно вывести из строя.



Ассоциация
Российских
Банков



VII Международная конференция
МОБИЛЬНЫЕ ФИНАНСЫ 2017
MobiFinance-2017 www.mobifinance.ru

18 апреля 2017 г. Москва

18 апреля 2017 года в Москве в Event-холле «Инфо-Пространство» пройдет VII Международная конференция **«МОБИЛЬНЫЕ ФИНАНСЫ 2017»**.

Организаторы: Ассоциация российских банков, «АйФин Медиа». Спонсор — BSS. Партнеры: БИФИТ, ГК «Центр Финансовых Технологий».

В Конференции примут участие представители Центрального банка РФ, Государственной Думы РФ, Министерства финансов РФ, Министерства связи и массовых коммуникаций РФ, банков, операторов сотовой связи, электронных платежных систем, систем мобильных платежей, разработчиков оборудования и программного обеспечения, контент- и сервис-провайдеров.



Тематика конференции:

- Мобильные финансовые услуги в России – состояние и перспективы развития. Основные тенденции и тренды 2017 года.
- Анализ развития различных сегментов рынка: мобильный банкинг, мобильная коммерция, мобильные платежи и переводы, бесконтактные мобильные платежи, мобильные информационные финансовые сервисы и т. д.
- Современные технологии, оборудование и сервисы, необходимые для создания и предоставления мобильных финансовых услуг.
- Вопросы правового регулирования рынка мобильных финансовых услуг.

ПОСЛЕДНЯЯ МОДЕЛЬ СКИММЕРА ПРОДАЕТСЯ В ИНТЕРНЕТ-МАГАЗИНЕ

Хакерская группировка The CC Buddies начала продажу устройства для бесконтактного считывания и клонирования кредитных карт, оснащенных RFID-чипами. Новое устройство способно считывать 21 карту в секунду.

Ранее The CC Buddies выпустили похожий скиммер Contactless Infusion X5, который был способен считывать информацию со скоростью 15 карт в секунду. Теперь хакеры представили новую версию — Contactless Infusion X6. Что интересно, злоумышленники больше не скрываются в даркнете, а продают аппарат на обычном общедоступном сайте.

Согласно сопроводительной информации, Infusion X6 может считывать банковские карты с расстояния 8 см (предыдущая версия «захватывала»

карты на расстоянии 15 см). Кроме того, устройство стало более компактным, незаметным. Скиммер также оснащен системой блокировки, позволяющей заблокировать устройство и зашифровать данные в случае столкновения с полицией.

Как и предыдущая модель, Infusion X6 собирает информацию о номере карт, дате окончания срока ее действия и т.д. Стоимость устройства составляет 1,5 биткойна (примерно \$ 1700). В комплект входит док-станция, браслет, с помощью которого скиммер крепится на руку, и другие аксессуары.



ЛИТВА — США. \$100 МЛН — 20 ЛЕТ

В Литве задержан Элдас Римасаускас, которому предъявлены обвинения в кибермошенничестве и незаконном получении \$ 100 млн.

Римасаускас взломал электронную почту двух американских компаний и параллельно зарегистрировал в Литве фирму с названием, похожим на название известной азиатской компании. Вышеупомянутые американские организации задолжали последней деньги, и литовец этим воспользовался. Под видом азиатской компании он отправил жертвам электронные письма с требованием вернуть долг, и деньги были перечислены.

Согласно обвинению, кибермошенник также занимался подделыванием писем, инвойсов и контрактов. В случае экстрадиции в США ему грозит наказание в виде лишения свободы на срок до 20 лет.

IT & SECURITY FORUM 2017

ОДИННАДЦАТАЯ
ВСЕРОССИЙСКАЯ
КОНФЕРЕНЦИЯ

24–26 мая

Казань, отель «Корстон»



IT & SECURITY FORUM* – всероссийская конференция, посвященная вопросам информационных технологий и информационной безопасности.

Представители регуляторов, ведущие мировые и отечественные ИТ-бренды, крупнейшие предприятия ключевых отраслей российской экономики, независимые эксперты соберутся на одной площадке, чтобы обсудить актуальные проблемы ИТ-индустрии, познакомиться с технологическими новинками, поделиться опытом решения практических задач.

* Форум АИТи
и безопасность

Заявки на участие принимаются на сайте форума: <http://itsecurityforum.ru>

16+

НЕ ИМЕЕТ ОБЛИК ФАЙЛА

В России появился вирус, который даёт возможность хакеру получить наличные из банкомата в обход всех датчиков.

Описание угрозы Банк России разослал всем учреждениям, которым выдал лицензию. По словам представителей ЦБ, вирус находится во временной памяти банкомата и не имеет облика файла, чтобы его нельзя было обнаружить. Антивирусные программы не могут с ним справиться. При введении кода банкомат начинает выдавать деньги самыми крупными купюрами, до срока штук за раз.

Такие программы сейчас широко распространены за рубежом, но малоизвестны в России. Центральный банк заблаговременно перестраховался и сообщил характеристики вредоносного ПО и как оно работает, чтобы финансовые учреждения смогли подготовиться к будущим атакам.



ВЫМОГАТЕЛИ ОБЛЮБОВАЛИ RDP

Протокол удалённого рабочего стола (RDP) становится все более популярным вектором для распространения вымогателей. Статистика Webroot показывает, что в этом он даже обошел электронную почту — 66 % против 33 %.

В прошлом году были зарегистрированы атаки, распространяющие следующие вредоносы: Busbi, Apocalypse, Shade. В феврале этого года Trend Micro показала, что вымогатель Crysis распространялся также с помощью RDP-атак. По сравнению с предыдущими месяцами, в январе количество таких атак выросло в два раза.

РОСТ СПАМА: ОТ ВОЛНЫ К ЦУНАМИ?

Спам-кампании вновь становятся одним из основных инструментов хищения данных, применяемых злоумышленниками. На протяжении 2016 года эксперты подразделения IBM X-Force Threat Intelligence наблюдали заметный рост «мусорной» корреспонденции с вложениями, содержащими банковские троюны и вымогательское ПО.

По словам эксперта Ральфа Ифферта, более 35 % спам-сообщений имели URL-адреса на общих доменах верхнего уровня .com и .info, свыше 20 % сайтов-распространителей спама использовали национальный домен.ru. Также злоумышленники используют менее известные домены верхнего уровня, такие как .click, .top, .xyz, .link, .club, .space и .site.

Новые домены верхнего уровня позволяют спамерам использовать различные web-адреса и тем самым

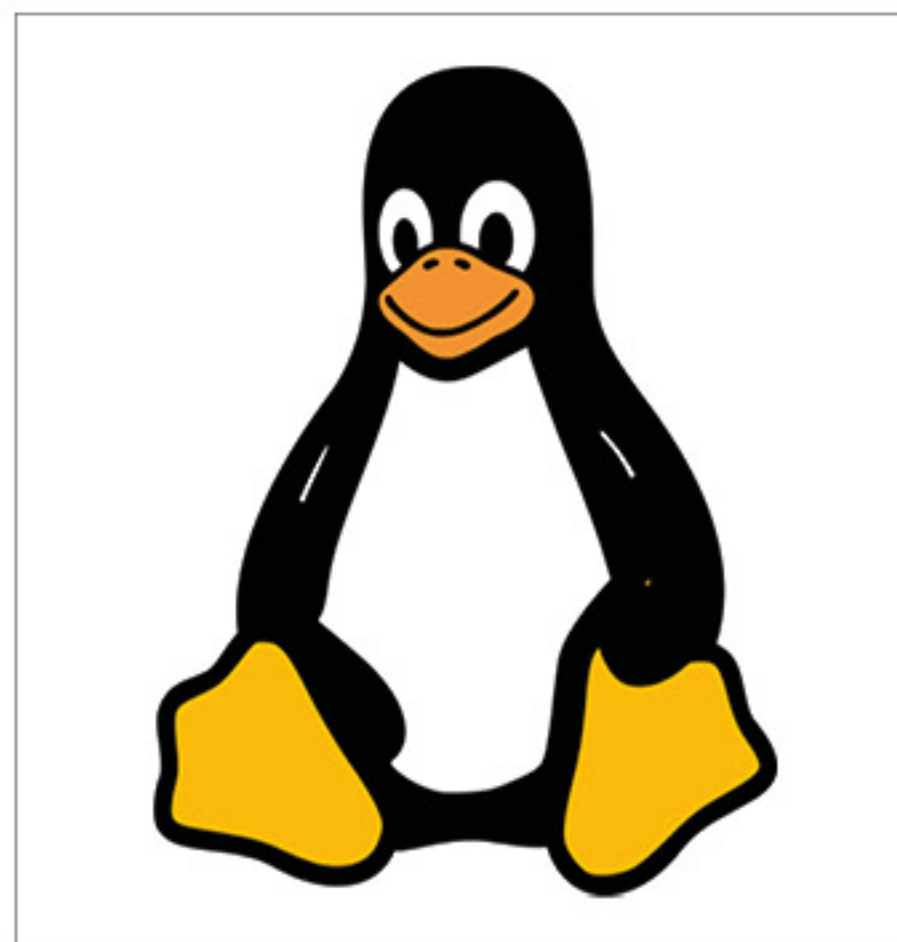


обходить спам-фильтры. Стоимость регистрации такого домена составляет всего \$1, что позволяет регистрировать сотни доменов в день.

По прогнозам тенденция будет усиливаться. Преступники продолжают использовать для рассылки спама web-адреса в зоне .xyz. В этой зоне уже зарегистрировано более 6 млн доменов и почти половина из них предоставляет только WhoIs-информацию о лице, зарегистрировавшем домен, что является индикатором его сомнительности.

УЯЗВИМОСТИ В ЯДРЕ LINUX — 7 ЛЕТ

Эксперт компании Positive Technologies Александр Попов выявил уязвимость в ядре Linux, которая позволяет локальному пользователю повысить привилегии в атакуемой системе или вызвать сбой в ее работе. Данная проблема актуальна для большинства популярных дистрибутивов Linux, в том числе RHEL 6/7, Fedora, SUSE, Debian и Ubuntu.



Исследователь выявил ошибку типа «состояние гонки» (race condition) в драйвере n_hdlc, приводящую к двойному освобождению памяти ядра, что может быть использовано для повышения привилегий в операционной системе. Уязвимость оценена в 7.8 баллов по шкале CVSS v3, что соответствует высокому уровню опасности.

Обнаруженная ошибка существует в ядре с 22 июня 2009 года и была выявлена с помощью тестирования системных вызовов Linux фаззером syzkaller. 28 февраля 2017 года исследователь сообщил об уязвимости на kernel.org, приложил прототип эксплойта и патч, который ее устраняет. 7 марта состоялось публичное разглашение информации о CVE-2017-2636, после чего были выпущены обновления безопасности. Защититься также можно с помощью специальных правил блокировки загрузки модулей ядра.

Я уверен.

Решения С-Терра надежно защищают
сеть моего банка.



Преимущества сетевой защиты С-Терра:

- Защита всех участков сети: от банкомата до ЦОД
- Использование мировых стандартов IKE/IPsec
- Соответствие ГОСТ и СТО БР ИББС
- Сертификация ФСБ России и ФСТЭК России
- Отсутствие зависимости от поставщика оборудования
- Защита подключения к СМЭВ
- Высокая экономическая эффективность продуктов
- Качественная, оперативная служба техподдержки



НАДЁЖНЫЙ ФУНДАМЕНТ

В ФЕДЕРАЛЬНОМ ЗАКОНОДАТЕЛЬСТВЕ
СОЗДАЁТСЯ ОРГАНИЗАЦИОННО-
ПРАВОВАЯ ОСНОВА ДЛЯ
ОБЕСПЕЧЕНИЯ БЕЗОПАС-
НОСТИ КРИТИЧЕСКОЙ
ИНФОРМАЦИОННОЙ
ИНФРАСТРУКТУРЫ



Эрнест ВАЛЕЕВ
Депутат Государственной
Думы РФ, Первый
заместитель председателя
комитета Госдумы
РФ по безопасности
и противодействию
коррупции

27 января 2017 года пакет из трёх законопроектов о безопасности критической информационной инфраструктуры был принят Государственной Думой РФ в первом чтении. Основной законопроект — о безопасности критической информационной инфраструктуры. Ещё два посвящены внесению соответствующих изменений в ряд законодательных актов Российской Федерации, в Уголовный и Уголовно-процессуальный кодексы РФ. Пакет законопроектов был внесён Правительством России 16 декабря 2016 года и рассмотрен Государственной Думой РФ в кратчайшие сроки.

НОВЫЕ УГРОЗЫ НАШЕЙ БЕЗОПАСНОСТИ

Предварительно внесённые Правительством России законопроекты были проработаны и поддержаны профильными комитетами Государственной Думы РФ:

- ♦ по информационной политике, информационным технологиям и связи;
- ♦ по безопасности и противодействию коррупции;
- ♦ по государственному строительству и законодательству;
- ♦ по экономической политике, промышленности, инновационному развитию и предпринимательству.

После этого пакет законопроектов об обеспечении безопасности критической информационной инфраструктуры был вынесен на рассмотрение пленарного заседания.

Проблема защиты информации, информационных ресурсов имеет богатую историю. 21 июля 1993 года был принят закон РФ № 5485-1 «О государственной тайне», в который потом вносились изменения. Одним из первых федеральных законов в этой сфере, принятых после вступления в силу ныне действующей Конституции России 1993 года, был Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Затем был принят ФЗ-152 от 27 июля 2006 года «О персональных данных» и ряд других отраслевых федеральных законов.

Почему в настоящее время возникла необходимость принятия федерального закона об обеспечении безопасности критической информационной инфраструктуры в России? В последние годы информационные технологии начали массово применяться практически во всех сферах жизни и масштабно расширились на трансграничное пространство. Если в 2011 году было выявлено 4,5 млн компьютерных атак на объекты критической информационной инфраструктуры, то в прошлом, 2016 году их количество возросло до 70 млн. Поэтому проблема защиты информации вышла на качественно новый уровень.

За последние годы ущерб от вредоносных программ, исходя из различных методик оценки ущерба, составлял от \$300 млрд до \$1 трлн, то есть от 0,4% до 1,4% общемирового ежегодного ВВП — валового внутреннего продукта. Эти показатели имеют тенденцию к неуклонному росту. Информационные технологии используются и для достижения недружественных нашей стране геополитических целей, и террористами, и прочим криминалитетом.

Компьютерные атаки могут повлечь за собой нарушение важнейших технологических процессов, включая те, что обеспечивают государственную деятельность. Компьютерные атаки могут полностью парализовать критическую информационную инфраструктуру государства, спровоцировать политическую, социальную, финансовую и экологическую катастрофу. Примерами последствий таких воздействий могут послужить остановка центрифуг иранской атомной станции с помощью компьютерного вируса StuxNet в сентябре 2010 года, а также и паралич работы нескольких крупных финансовых учреждений Южной Кореи в марте 2013 года.

Стабильность социально-экономического развития и безопасность нашей страны находятся в прямой зависимости от надежности и безопасности функционирования информационно-телекоммуникационных сетей и информационных систем. Работа по обеспечению безопасности критически важной инфраструктуры велась и раньше. Обеспечение их безопасности регламентируется и другими законами: их физическая защита, в случаях чрезвычайных ситуаций, военных, вооружённых и террористических нападений... Велась работа и по обеспечению информационной безопасности критической информационной инфраструктуры Российской Федерации.

Ярким примером является создание в 2013–2016 годах Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГОССОПКА). Создание этой системы ранее регламентировалось подзаконными актами — Указами Президента России, Постановлениями Правительства РФ и ведомственными нормативными документами, включая Приказы ФСБ России.

СИСТЕМАТИЗИРУЮЩИЙ ЗАКОНОПРОЕКТ

Однако эффективное правовое регулирование в данной сфере было затруднено из-за отсутствия системообразующих законодательных актов, устанавливающих порядок отношений в сфере обеспечения безопасности критической информационной инфраструктуры в Российской Федерации. Пришла пора обосновать, с учётом зарубежной практики и отечественного опыта, безопасность критической информационной инфраструктуры в России на уровне федерального законодательства.

Пакет законопроектов о безопасности критической информационной инфраструктуры Российской Федерации формирует полноценную правовую основу для развития и функционирования Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак.

**ЗА ПОСЛЕДНИЕ ГОДЫ УЩЕРБ
ОТ ВРЕДНОСНЫХ ПРОГРАММ,
ИСХОДЯ ИЗ РАЗЛИЧНЫХ МЕТОДИК
ОЦЕНКИ УЩЕРБА, СОСТАВЛЯЛ
ОТ \$300 МЛРД ДО \$1 ТРЛН**

Определено, что относится к критической информационной инфраструктуре: информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами в 13 сферах. К ним относятся государственное управление, энергетика, транспорт, связь, кредитно-финансовая сфера, здравоохранение и ряд отраслей промышленности. А именно: оборонная, топливная, атомная, ракетно-космическая, горнодобывающая, металлургическая и химическая.

Устанавливаются основные принципы обеспечения безопасности критической информационной инфраструктуры. Чётко регламентируются полномочия различных органов государственной власти, в том числе различных ведомств и других субъектов отрасли, включая операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

Выстроен порядок их взаимодействия для защиты информационных сетей от компьютерных атак. Вводятся категорирование объектов критической информационной инфраструктуры, порядок их классификации, различия степени защищённости. Оценку степени защищённости смогут проводить организации, аккредитованные уполномоченными государственными органами

Принятие основного федерального закона — «О безопасности критической информационной инфраструктуры Российской Федерации» требует внесения изменений в ряд действующих законодательных актов. Прежде всего, в Закон РФ № 5485-1 «О государственной тайне» — об отнесении ресурсов обеспечения защиты критической информационной инфраструктуры к категории государственной тайны. В Федеральный закон от 07 июля 2003 года № 126-ФЗ «О связи» — об обязанности операторов телекоммуникаций выполнять требования к технологической оснащённости и обеспечивать сохранность технических средств, задействованных в защите объектов критической информационной инфраструктуры.

Кроме того, вносится норма о защите прав юридических лиц и индивидуальных предпринимателей при проведении профильных контрольно-надзорных мероприятий. Что обусловлено тем, что в основном законопроекте подробно прописаны меры государственного контроля: основания и процедуры проведения проверок, действия по их результатам. Эти правоотношения в отрасли будут регулироваться не Федеральным законом от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», а законом о безопасности критической информационной инфраструктуры.

КОМПЛЕКС ПРИНИМАЕМЫХ ЗАКОНОПРОЕКТОВ ВНОСИТ ИЗМЕНЕНИЯ И В УГОЛОВНЫЙ КОДЕКС РФ

ОТВЕТСТВЕННОСТЬ СОРАЗМЕРНА ОПАСНОСТИ

Комплекс принимаемых законопроектов вносит изменения и в Уголовный кодекс РФ. В действующем законодательстве была установлена ответственность за три состава преступлений в сфере компьютерной информации: статьями 272, 273 и 274. Это, во-первых, неправомерный доступ к компьютерной информации, повлекший её изменение, уничтожение или блокирование; во-вторых, производство и распространение вредоносного программного обеспечения; и, в-третьих, нарушение правил эксплуатации компьютеров и компьютерных сетей.

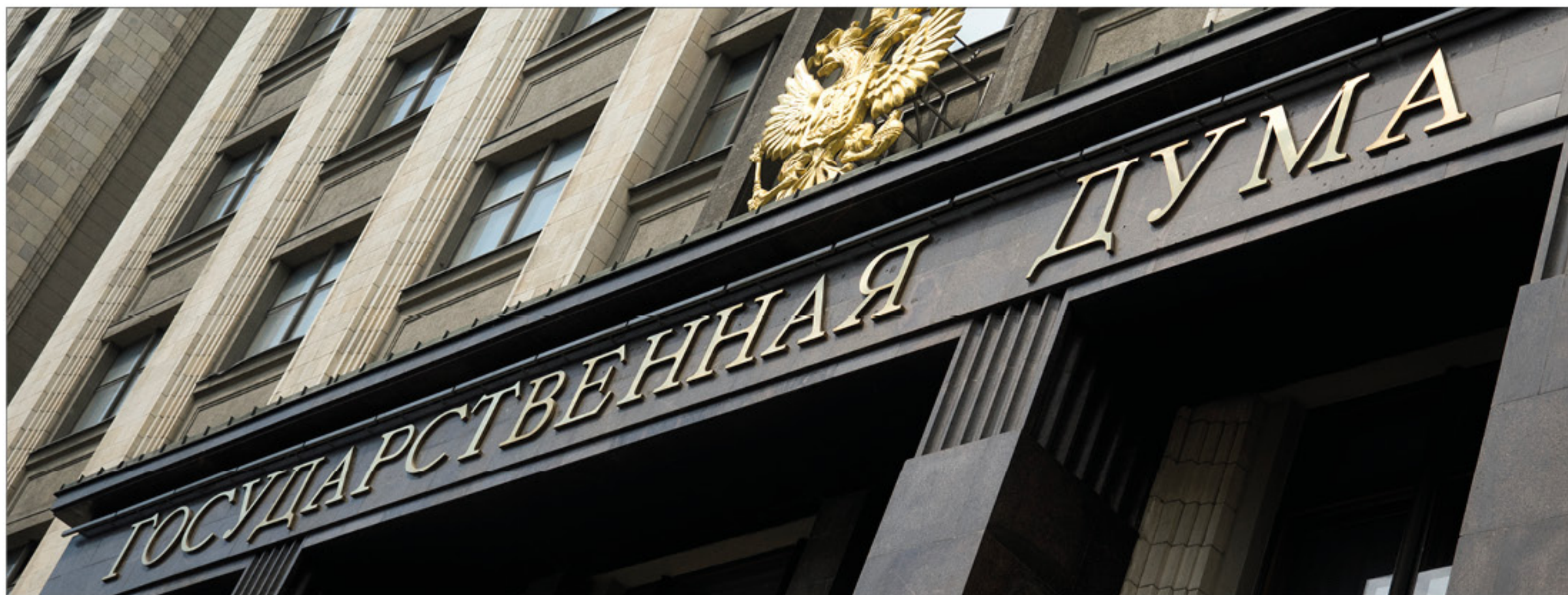
К этим статьям будет добавлена новая, 274–1, конкретизация компьютерных преступлений применительно к объектам критической информационной инфраструктуры, с повышенной ответственностью. Предлагается выделить составы посягательств на критическую информационную инфраструктуру Российской Федерации в отдельную статью Уголовного кодекса — «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Ответственность предусматривается:

- ♦ за создание, распространение компьютерных программ, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру России;
- ♦ за неправомерный доступ к охраняемой законом компьютерной информации в критической информационной инфраструктуре;
- ♦ за нарушение правил эксплуатации в ней средств хранения, обработки или передачи охраняемой компьютерной информации.

Учитывая высокую общественную опасность таких деяний, санкции за них будут предусматривать, с учётом различных квалифицирующих признаков, наказания в виде штрафа, принудительных работ, лишения свободы на срок до 10 лет, с лишением права занимать определённые должности или заниматься определённой деятельностью. Кроме того, прописываются возможности использования Кодекса административных правонарушений РФ, в котором есть 33 состава проступков в компьютерной сфере. Также применение гражданской ответственности при нанесении ущерба компьютерными атаками.

Общественное обсуждение этих вопросов проводилось на самых разнообразных площадках, в частности, на Национальном форуме информационной безопасности «Инфофорум — 2017», проходившем 2–3 февраля 2017 года. Вопросы защиты объектов критической информационной инфраструктуры в финансовой сфере рассматривались на IX Уральском форуме «Информационная безопасность финансовой сферы», проведённого 13–17 февраля этого года. Разработчиками законопроекта учтены более 300 замечаний, поступивших от представителей более 60 регионов страны.

Можно достаточно уверенно прогнозировать социальные, экономические, экологические, политические — внешние и внутренние, а также иные негативные последствия, которые могут наступить в результате атак на те или иные объекты критической информационной инфраструктуры. Исходя



из такого прогнозирования, на основе принятого пакета законопроектов Правительство России своими нормативными документами может определять требования по обеспечению её безопасности к каждой из сфер, отраслей.

Элементы критической информационной инфраструктуры включаются в государственный реестр значимых объектов, им на основании определённых критериев может присваиваться одна из трёх категорий значимости — высокая, средняя или низкая. Присвоенным категориям должна соответствовать степень защищённости, которую должны обеспечивать собственники, владельцы, управляющие этими объектами. Что такое системы безопасности объектов критической информационной инфраструктуры, какими они должны быть, — в законопроекте прописано подробно.

ФАКТОР МЕЖДУНАРОДНОЙ ОБСТАНОВКИ

Что касается технического обеспечения, то, по оценкам экспертов, наша страна способна самостоятельно обеспечить выполнение принимаемых законопроектов, и аппаратное, и программное. Дело в том, чтобы этими техническими средствами оснастить все требующие защиты объекты критической информационной инфраструктуры. Согласно финансово-экономическому обоснованию, сопровождающему законопроект, дополнительных финансовых затрат из государственного бюджета, федерального и региональных, его реализация не требует. Потому что создание ГОССОПКА было начато четыре года назад.

Сейчас ГОССОПКА работает как централизованная территориально распределённая система, полноценно обеспечивает защиту объектов критической информационной инфраструктуры. Принимаемый законопроект просто развивает регламентацию её работы, переносит её с подзаконных нормативных актов на новый правовой уровень — федерального законодательства.

Затраты на организационно-техническое обеспечение реализации законопроекта и их источники уже были определены ранее. Как из государственного бюджета, так и негосударственных собственников объектов критической информационной инфраструктуры. Обеспечение безопасности,

конечно, требует затрат, но такие расходы необходимы. Существенного их возрастания в связи с принятием законопроектов, о которых идёт речь, ожидать не приходится.

Разработчики законопроектов учитывали зарубежный опыт и практику противодействия информационным атакам на объекты критической инфраструктуры. Были учтены все международные обязательства Российской Федерации в этой области. Подытожен опыт правового регулирования безопасности критической информационной инфраструктуры стран с развитой информационной инфраструктурой, таких как Германия, США, Великобритания, Япония и Южная Корея.

Даже то, что в последнее время в некоторых странах чаще стали использоваться политические спекуляции вокруг компьютерных атак, не препятствует международному взаимодействию для противодействия киберпреступности. В ряде сфер, взять хотя бы атомную промышленность, компьютерные атаки могут нанести огромный международный ущерб. Поэтому выполняются, на паритетных началах, существующие договорные отношения о привлечении к уголовной ответственности тех виновных в компьютерных преступлениях, кто находится за рубежом.

Следует отметить, что компьютерные атаки иностранных государственных структур, совершаемые, например, в разведывательных целях, не подпадают под российское уголовное законодательство, которое распространяется на физические, а не на юридические лица. Проблемы со странами, избличёнными в подобных действиях, должны решаться политическими способами.

* * *

Принятие пакета законопроектов создаст организационно-правовую основу для эффективной работы системы безопасности критической информационной инфраструктуры Российской Федерации. В первую очередь — для предупреждения компьютерных инцидентов, а также для существенного снижения общественно-политических, финансовых и иных негативных последствий компьютерных атак.



Георгий
ЛУНТОВСКИЙ
первый заместитель
Председателя
Банка России

НАПРАВЛЕНИЯ РАБОТЫ
БАНКА РОССИИ ПО
СНИЖЕНИЮ РИСКОВ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
В КРЕДИТНО-
ФИНАНСОВОЙ СФЕРЕ

ВЕКТОР 2017 ГОДА



Основными целями Банка России при реализации мероприятий по противодействию информационным угрозам в организациях кредитно-финансовой сферы является минимизация рисков нарушений финансовой стабильности этих организаций в результате компьютерных атак на их информационные ресурсы. Собственно, речь идет о поддержании таким образом финансовой стабильности государства и страны в целом.

В прошлом году мы постоянно наблюдали попытки атак. Тем не менее, прогноз на декабрь об агрессивных массированных нападениях с целью дискредитации нашей кредитно-финансовой сферы не оправдался. Все атаки были успешно отражены. Но в целом проблема остаётся. Прежде всего — проблема несанкционированных финансовых транзакций, наносящих прямой ущерб клиентам и контрагентам организаций кредитно-финансовой сферы.

Обеспечение доверия клиентов и контрагентов организаций кредитно-финансовой сферы с помощью электронных технологий и сервисов. По данным, полученным из форм обязательной отчётности об инцидентах информационной безопасности, официально предоставляемых кредитными организациями в Банк России, и данным, полученным в рамках информационного обмена, организованного ФинЦЕРТ, объём несанкционированных операций со счетами юридических лиц по итогам 2016 года составил 1,9 млрд рублей. Для сравнения, в 2015 году аналогичный показатель составил 3,8 млрд рублей.

Объём несанкционированных операций с использованием платёжных карт за 2016 год составил порядка 1,08 млрд рублей. В 2015 году — порядка 1,15 млрд рублей. При этом в 2016 году Банк России выявил 9 покушений на хищение денежных средств с корреспондентских счетов кредитных



организаций, открытых в платёжной системе Банка России, на сумму порядка 2,18 млрд рублей. Из них на сумму порядка 1,5 млрд рублей наступила окончательность перевода денежных средств. То есть эти деньги были похищены.

С учётом оценочной информации об объёме несанкционированных переводов денежных средств, осуществляемых в национальной платёжной системе России с использованием платёжных карт, эмитированных на территории Российской Федерации, удельный вес несанкционированных переводов денежных средств составляет 0,002 %. Это данные за прошлый год. В условиях общего роста платежей, совершаемых в безналичной форме, Банк России ставит цель удерживать этот показатель на уровне, не превышающем 0,005 %. Для международных платёжных систем эта цифра несколько выше — 0,009 %, что даёт нам хорошую возможность удерживать данный показатель на приемлемом уровне.

В составе ключевых направлений работы по противодействию информационным угрозам в кредитно-финансовой сфере Банк России реализовывает следующие направления:

- ♦ Проработка совместно с ФСТЭК России, ФСБ России вопроса о законодательном закреплении полномочий Банка России по нормативному регулированию и контролю всех вопросов, связанных с обеспечением информационной безопасности в организациях кредитно-финансовой сферы. В том числе вопросов защиты информации, отнесённой к категории банковской тайны, а также вопросов возврата денежных средств, переведённых без согласия клиента. Разработан законопроект, посвященный основам деятельности по реализации противодействия хищениям денежных средств системой антифрод и созданию ФинЦЕРТа на базе Банка России. В настоящее время законопроект находится на рассмотрении в Государственной Думе Российской Федерации.

- ♦ Обеспечение разработки национальных стандартов, регулирующих технические вопросы обеспечения информационной безопасности. В частности, разработан проект национального стандарта «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер защиты информации». Проект стандарта рассмотрен и в целом одобрен на заседании подкомитета № 1 и размещён на сайте Росстандарта для публичного обсуждения, сбора замечаний и предложений. Ввод этого стандарта в действие пла-

нируется в III–IV квартале 2017 года. Предполагается, что он будет использоваться как основной документ, регламентирующий технические вопросы защиты информации в организациях кредитно-финансовой сферы. Обязательность применения стандарта планируется обеспечить путём установления на него нормативных ссылок в нормативных актах Банка России, регулирующих действия разных категорий организаций кредитно-финансовой сферы.

♦ Пересмотр технологических требований, связанных с осуществлением переводов денежных средств, внедрение безопасных технологий, в том числе для участников платёжной системы Банка России. В настоящее время проводятся мероприятия по переносу подписи распоряжений о переводах денежных средств из АРМ КБР в автоматизированные банковские системы кредитных организаций. Завершение данной работы планируется в 2018 году.

♦ Дополнительно в 2017 году Банком России планируется внесение изменений в 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». Теперь в нём будут предусмотрены и меры по применению средств, обеспечивающих распределение контуров подготовки и подтверждения поручений на переводы денежных средств. В том числе при использовании системы дистанционного банковского обслуживания. Указанные меры по разделению контуров подготовки и подтверждению платёжных поручений позволят наряду с обязанностью кредитных организаций по выпуску платёжных карт, оснащённых только микропроцессорами, обеспечить эффективность противодействия несанкционированным переводам денежных средств с применением платёжных карт и систем дистанционного банковского обслуживания.

♦ Пересмотр технологий контроля за соблюдением участниками платёжной системы Банка России требований к обеспечению информационной безопасности. Банком России разработано и введено в действие положение Банка России от 24 августа 2016 года №552-П «О требованиях к защите информации в платёжной системе Банка России», в соответствии с которым всем участникам платёжной системы вменяется в обязанность информирование Банка России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации, в том числе

ПО ДАННЫМ ФИНЦЕРТ

На IX Уральском форуме заместитель начальника ГУБиЗи Банка России Артем Сычев и начальник отдела ФинЦЕРТ Артем Сударенко представили официальный документ «Обзор несанкционированных переводов денежных средств за 2016 год». Для ФинЦЕРТ это подтверждение очень достойного итога первого года работы. Публикуем наиболее интересную, на наш взгляд, главу обзора.

СВЕДЕНИЯ О НЕСАНКЦИОНИРОВАННЫХ ОПЕРАЦИЯХ СО СЧЕТОВ ЮРИДИЧЕСКИХ ЛИЦ

Динамика количества и объема несанкционированных операций со счетов юридических лиц

Под несанкционированными операциями со счетов юридических лиц в контексте настоящего обзора понимаются события, связанные с покушением на хищение денежных средств со счета юридического лица с использованием систем ДБО.

В 2016 году в Банк России была представлена информация о 717 несанкцио-

нированных операциях со счетов юридических лиц на общую сумму 1,89 млрд рублей.

Из них на долю остановленных операций приходится не менее половины от общего объема денежных средств. К остановленным операциям относятся операции, перевод денежных средств по которым не достиг окончательности, либо окончательность перевода денежных средств наступила, но денежные средства заблокированы на счете получателя в соответствии с законодательством Российской Федерации до полу-

чения обоснования перевода денежных средств.

На графике представлены значения общего объема несанкционированных операций, при этом в процентном соотношении отражены доли неостановленных операций. Высокий процент остановленных операций свидетельствует об эффективности работы систем выявления и противодействия несанкционированным операциям (систем класса антифрод), а также о высоком уровне межбанковского взаимодействия.



и о несанкционированных переводах денежных средств, не позднее трёх часов после выявления инцидента.

♦ Разработка и ввод в действие стандарта, устанавливающего правила выявления и расследования инцидентов информационной безопасности, связанных с функционированием автоматизированных банковских систем и приложений, применяемых национальной платёжной системой. С 1 января 2017 года введен в действие стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств». Банк России разработал этот стандарт совместно с правоохранительными органами для формализации подготовки данных об инцидентах при взаимодействии с правоохранительными органами в рамках расследования киберпреступлений.

Основные направления деятельности Банка России по противодействию правонарушениям в кредитно-финансовой сфере в 2017 году:

♦ Будет продолжена разработка и ввод в действие национальных стандартов, регулирующих технические вопро-

сы обеспечения информационной безопасности в организациях кредитно-финансовой сферы. Для этого в 2017 году будет разработан проект национального стандарта «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия информационной безопасности финансовой организации требованиям ГОСТ Р». Ввод в действие — I–II кварталы 2018 года.

♦ Реализация совместно с ФСБ России и ФСТЭК России системы независимого подтверждения соответствия обеспечения информационной безопасности кредитно-финансовых организаций требованиям национальных стандартов, что должно, по мнению Банка России, повысить качество надзорных мероприятий по контролю технических аспектов обеспечения информационной безопасности.

♦ Разработка и ввод нормативных актов Банка России, предусматривающих совершенствование требований к управлению операционными рисками, в том числе требований к политике кредитных организаций в сфере информационных технологий, включая информационную инфраструктуру, безопасность и целостность системы платежей и расчётов.

Распределение несанкционированных операций со счетов юридических лиц в разрезе объема каждой несанкционированной операции в отдельности

Объемы операций со счетов юридических лиц значительно превышают аналогичные значения для операций с использованием платежных карт как по абсолютным показателям, так и в рамках отдельных операций. Если для осуществления несанкционированной операции с использованием платежной карты злоумышленники вынуждены учитывать максимальные размеры суммы операции (лимиты на операции со счета, установленные банком или клиентом), то при проведении подобной операции со счетов юридических лиц злоумышленники для успешного ее осуществления в лучшем случае вынуждены имитировать модель операций юридического лица, а в худшем — ограничены только количеством денежных средств на банковском счете юридического лица. Таким образом, для несанкционированных операций со счетов юридических лиц формирует-

ся особенность в виде больших сумм каждой несанкционированной операции в отдельности. Основное количество несанкционированных операций приходится на сегмент от 10 тыс. руб. до 10 млн руб. и достигает пика в сегменте от 100 тыс. руб. до 1 млн рублей. Подобное распределение указывает на то, что интерес злоумышленников сфокусирован на юридических лицах, имеющих на своих банковских счетах суммы, объемом не превышающие нескольких миллионов рублей, и не имеющих возможности на должном уровне выполнять мероприятия по защите информации при использовании дистанционных платежных сервисов.

Распределение по причинам совершения несанкционированных операций

Данные, предоставленные отчитывающимися операторами в рамках формы отчетности 0403203, свидетельствуют о том, что причинами осуществления несанкционированных операций со счетов юридических лиц, среди прочего, являются нарушение порядка ис-

пользования ЭСП и использование ЭСП без согласия клиента. С учетом того, что юридические лица в основном осуществляют операции через системы ДБО со стационарных компьютеров, наиболее вероятной причиной совершения несанкционированных операций является воздействие вредоносного кода.

Распределение по обращениям в правоохранительные органы

В случае несанкционированных операций со счетов юридических лиц операторы по переводу денежных средств и операторы услуг платежной инфраструктуры обладают большим объемом данных о факте обращения в правоохранительные органы, чем в случае подобных операций с использованием платежных карт. Только в 42 % случаев операторы по переводу денежных средств и операторы услуг платежной инфраструктуры не обладают соответствующей информацией. Приведенные данные свидетельствуют о различиях в порядке разбора отчитывающимися операторами конфликтных ситуаций

♦ Установление подходов Банка России к оценке уровня операционного риска и дополнительных требований к капиталу на покрытие уровня операционного риска, принятого кредитными организациями.

♦ Создание правовых и организационных условий по внедрению в кредитно-финансовой сфере руководства по киберустойчивости для инфраструктур финансового рынка, которые дополняют международный стандарт Комитета по платежам и рыночным инфраструктурам. Формулирование принципов для инфраструктур финансового рынка.

♦ Оптимизация и повышение достоверности отчетности, которая предоставляет сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств. Цель данной работы — исключение из отчетности вопросов технической реализации инцидентов защиты информации и сбор информации о технических способах реализации инцидентов защиты информации по каналам взаимодействия, организованным ФинЦЕРТ. Установление в новой форме отчетности только экономических показателей. Повышение достоверности предоставляемой отчетности, в том числе путём анализа изменений по счетам бухгалтерского учёта.

♦ Разработка совместно с ФСТЭК России типовой программы дополнительного профессионального образования для специалистов по информационной безопасности организаций кредитно-финансовой сферы продолжительностью более 500 учебных часов. В настоящее время высшие учебные заведения не готовят специалистов по данному направлению, а проводят обучение в рамках повышения квалификации объёмом не более 72 учебных часов, что в современных условиях явно недостаточно. Разработка такой типовой программы обучения позволит обеспечить возможность организации вузами системной работы по подготов-

ВСЕ ПРЕДСТАВЛЕННЫЕ НАПРАВЛЕНИЯ ПРЕДЛАГАЮТСЯ К ШИРОКОМУ ОБСУЖДЕНИЮ ПРОФЕССИОНАЛЬНОЙ ОБЩЕСТВЕННОСТЬЮ

ке специалистов в области информационной безопасности в организациях кредитно-финансовой сферы.

♦ Отдельное внимание Банк России будет уделять созданию условий по применению организациями финансово-кредитной сферы стандартов Банка России по вопросам информационной безопасности. По оценкам регулятора комплекс отраслевых документов имеет высокий уровень зрелости. Он покрывает основные и наиболее актуальные направления обеспечения информационной безопасности. Вместе с тем степень и глубина применения отраслевых стандартов организациями кредитно-финансовой сферы невелики. Для организации указанной работы планируется создание координационного совета с участием заинтересованных организаций кредитно-финансовой сферы, разработчиков банковских систем и средств защиты информации.

* * *

Все представленные направления предлагаются к широкому обсуждению профессиональной общественностью. Всестороннее детальное обсуждение будет традиционно способствовать определению оптимальных решений, которые в перспективе позволят преодолеть негативные явления, вызванные деятельностью киберпреступников.

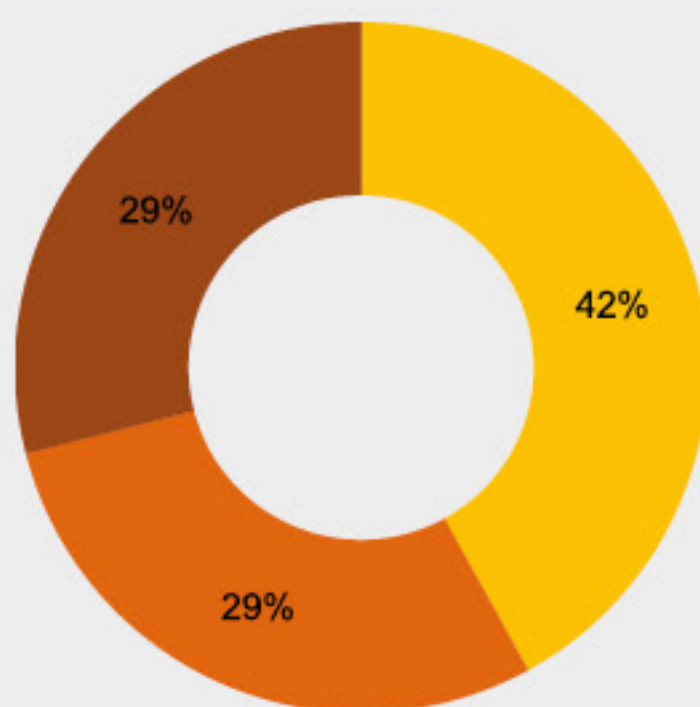
в случаях несанкционированных операций со счетов юридических лиц и аналогичных операций с использованием платежных карт. Причиной подобных различий может быть разница в величине убытка, который понесет оператор по переводу денежных средств или оператор услуг платежной инфраструктуры: средний объем несанкционированной операции с использованием платежной карты находится в пределах 3,7 тыс. руб., в то время как средний объем несанкционированной операции со счета юридического лица — в пределах 2,76 млн руб. (различия более чем в 700 раз).

Вместе с тем нельзя не учитывать различия в количестве несанкциониро-

ванных операций с использованием платежных карт и несанкционированных операций со счетов юридических лиц (больше чем в 400 раз). Подобный порядок не позволяет отчитывающимся операторам проводить детальный

разбор каждой в отдельности несанкционированной операции с использованием платежной карты.

В полном объеме материалы обзора — на www.cbr.ru



- сведения о направлении информации в правоохранительные органы отсутствуют
- сведения были направлены в правоохранительные органы
- сведения не направлялись в правоохранительные органы

БУМАЖНЫЙ ВЕК УХОДИТ В ПРОШЛОЕ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ НЕОБХОДИМО ДЛЯ
УСПЕШНОЙ РЕАЛИЗАЦИИ СТРАТЕГИИ
РАЗВИТИЯ ФИНАНСОВОГО РЫНКА



**Владимир
ЧИСТЮХИН**
заместитель
Председателя
Банка России

Значение информационных технологий растёт по всем направлениям государственного регулирования, контроля и надзора на финансовом рынке: в его развитии, расширении доступности сервисов, в отношении профессиональных участников и в защите прав потребителей. Всё больший удельный вес занимает электронный документооборот, а бумажный сокращается.

Однако вместе с этим растут и киберугрозы. Растущая зависимость от технологий, а также увеличивающийся масштаб их применения в различных секторах экономики означают потенциальное увеличение киберрисков в ближайшем будущем. Поэтому возрастает значение управления такими рисками, выстраивания соответствующих систем.

СТРАТЕГИЮ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬЮ

В наши дни киберпреступность «обходится» глобальной экономике в \$ 445 млрд ежегодно (*The Center for Strategic and International Studies and McAfee*). Риски масштабных кибератак названы наиболее значимыми рисками для ведения бизнеса в 18 странах с ведущими экономиками, включая G7 (*The World Economic Forum's 2016 Global Risk Report*). Порядка \$ 294 млрд ВВП крупнейших городов мира подвержены масштабным кибератакам (*Lloyd's City Risk Index*).

Для реализации упомянутых функций Банка России в сфере развития финансового рынка была принята стратегия — документ под названием «Основные направления развития финансового рынка на период 2016–2018 годов». В нём указаны десять основных направлений работы, и практически в каждом всё больше применяются информационные технологии, которым сопутствуют киберриски. Перечисленные направления могут развиваться только на базе учёта подобных рисков и их минимизации. В полной мере это относится и к отдельным инновационным финансовым продуктам.

Принципиально важно заниматься киберрисками на всех уровнях инфраструктуры финансового рынка — как банков, так и некредитных финансовых организаций, включая организаторов электронных торгов, бирж, депозитариев, которые работают с огромными базами критических данных.

Эти участники рынка, в частности, биржи, в свою очередь прилагают значительные усилия для управления операционными киберрисками.

Местами выстроенные ими системы обеспечения информационной безопасности не хуже, чем у крупных банков, а по ряду показателей и лучше. Потому что эта работа курируется на уровнях правления, совета директоров, в неё вкладываются солидные средства. Что значит идти в ногу со временем, соответствовать современным требованиям к развитию информационных технологий.

ЭЛЕКТРОННОЕ ОСАГО: УДОБСТВА БЕЗ ИЗДЕРЖЕК

Управление киберрисками важно как для организаций — участников рынка, так и для отдельных инновационных финансовых продуктов. Так, среди электронных средств платежа, электронных технологий в практике продаж и предоставлении финансовых продуктов и услуг присутствует **электронный полис ОСАГО**. С 1 января 2017 года такой полис стал обязательным для страховых компаний, работающих на рынке ОСАГО, они обязаны любому потребителю его предоставлять.

Возможности электронного полиса ОСАГО позволяют профессиональным участникам финансового рынка не тратить на содержание офисов и армии страховых агентов: такие услуги можно предоставлять через интернет. Но вместе с тем возникают серьёзные проблемы, связанные с возможными мошенничествами. Появились поддельные сайты страховых компаний, где продавались фальшивые электронные полисы ОСАГО. Злоумышленники даже сделали клон сайта Российского союза автостраховщиков.

Задачей Банка России — Службы по защите прав потребителей финансовых услуг и миноритарных акционеров, а также Департамента страхового рынка Банка России — является обеспечение непрерывности деятельности сайтов страховщиков, через которые потребитель может эту услугу приобрести. Совместные действия с участниками рынка позволили оперативно заблокировать деятельность упомянутого мошеннического интернет-ресурса. Но ясно, что требуется постоянный мониторинг интернета и готовность к блокировке новых попыток подобных мошенничеств.

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ФИНАНСОВОГО РЫНКА РФ НА ПЕРИОД 2016–2018 ГОДОВ

Цели Направления развития	Повышение уровня и качества жизни граждан Российской Федерации за счет использования инструментов финансового рынка	Содействие экономическому росту за счет предоставления конкурентного доступа субъектам российской экономики к долговому и долевым финансированию, инструментам страхования рисков	Создание условий для роста финансовой индустрии
Обеспечение защиты прав потребителей финансовых услуг и повышение финансовой грамотности населения Российской Федерации			
Повышение доступности финансовых услуг для населения и субъектов малого и среднего предпринимательства			
Дестимулирование недобросовестного поведения на финансовом рынке			
Повышение привлекательности для инвесторов долевого финансирования публичных компаний за счет улучшения корпоративного управления			
Развитие рынка облигаций и синдицированного кредитования			
Совершенствование регулирования финансового рынка, в том числе применение пропорционального регулирования, оптимизация регуляторной нагрузки на участников финансового рынка			
Повышение квалификации лиц, профессиональная деятельность которых связана с финансовым рынком			
Стимулирование применения механизмов электронного взаимодействия на финансовом рынке			
Международное взаимодействие в области выработки и внедрения правил регулирования глобального финансового рынка			
Совершенствование инструментария по обеспечению финансовой стабильности финансового рынка			

влияет на реализацию стратегической цели, но незначительно

значительно влияет на реализацию стратегической цели

прямо влияет на реализацию стратегической цели

Опубликована Межведомственная дорожная карта на 2016-2018 годы

Опубликована Ежегодная дорожная карта Банка России на 2016 год

Создана Рабочая группа для разработки перечня дополнительных показателей оценки эффективности реализации ОНРФР

Запущен проект по оценке состояния и уровня конкурентоспособности российского финансового рынка на основе панели индикаторов с использованием опыта международных рейтингов

Следующий риск — высокая убыточность реализации электронных полисов страхования недобросовестным клиентам, скрывающим предыдущие страховые случаи. Необходима процедура оперативной дистанционной проверки «страховой истории» покупателя электронного полиса ОСАГО.

Ещё один риск — нестыковка баз данных автостраховщиков и дорожной полиции. По закону, купив электронный полис, достаточно предъявить его распечатку. Были случаи, когда сотрудники дорожной полиции не принимали такие распечатки, а требовали предоставить полис на бланке. Чтобы потребитель доверял электронным полисам ОСАГО, федеральные органы исполнительной власти, включая Банк России, должны навести порядок в этой процедуре.

В целом реализация электронных полисов ОСАГО стартовала удовлетворительно, сняв ряд проблем в регионах. За первые полтора месяца 2017 года было продано около 300 000 полисов — очень много. Это столько же, сколько за весь прошлый год, когда страховые компании предлагали этот продукт не в обязательном, а в добровольном порядке. Теперь вопрос в том, насколько хорошо — удобно для потребителей работают сайты страховщиков.

Для контроля продажи электронных полисов ОСАГО Банком России созданы специальные алгоритмы проверки, с использованием автоматизированного мониторинга и анализа. Есть процедура запроса у страховой компании журналов электронных событий, в том числе сведений, кто, когда заходил на сайт, сколько времени там провёл т.п. Для того, чтобы выявить факты проблем с покупками, установить сторону ответственности — покупателя или продавца, выяснить причины не предоставления услуги.

ПЕНСИОННОЙ ПРИВАТНОСТИ — НЕПРИСТУПНОСТЬ

Ещё один пример — задача обеспечить информационную безопасность процесса **инновации системы обязательных накоплений, использования индивидуального пенсионного капитала**. Предполагается создание **единого пенсионного администратора — специализированной организации**, которая будет вести базу данных, предоставлять информацию гражданам и негосударственным пенсионным фондам о наличии, принадлежности и характере пенсионных прав, операциях с ними. Такой оператор-администратор может быть создан на базе федерального органа исполнительной власти или государственной корпорации, возможно, как отдельное юридическое лицо.

Очевидно, что такой единый пенсионный администратор может эффективно работать только посредством электронных технологий. Множество проблем Пенсионного фонда России, пока ведущего учёт пенсионных прав граждан, связано с большой долей бумажного документооборота, недостаточным использованием автоматизированных информационных систем. Многие из тех, которые уже работают, устарели, децентрализованы.

Бумажный век уходит в прошлое. Создаваемый пенсионный администратор должен работать посредством больших

баз данных, самыми передовыми информационными технологиями. Востребован высокий уровень защиты от несанкционированного вмешательства, способного привести к нарушениям функционирования, искажению данных, кражам информации и другому ущербу. Вопросы киберрисков встают остро и выходят на передний план.

Один из таких вопросов — **безопасность личных кабинетов клиентов**. На смену бумажному документообороту всё больше приходит электронный, а почтовому адресу офиса или квартиры — личный кабинет. Сегодня предписание должно в электронном виде помещаться в личный кабинет, и, согласно действующим общим правилам, профессиональным участникам рынка — страховой компании, пенсионному фонду, другой некредитной финансовой организациям — даётся 24 часа на ознакомление. Предполагается, что в течение этого срока отправленное будет доставлено адресату.

С одной стороны, такой порядок упрощает всем жизнь. Сокращаются организационно-административные расходы, расходы государственных регуляторов и профессиональных участников рынка. С другой стороны, серьёзно встаёт вопрос о поддержании личных кабинетов в нормальном рабочем состоянии, об обеспечении их непрерывной деятельности. Банк России со своей стороны должен обеспечить информационную безопасность этих сервисов, и необходимая для этого работа ведётся.

ГОТОВИТЬ НОВЫХ ПРОФЕССИОНАЛОВ

Противодействие киберпреступности — отдельное направление в рамках развития финансовых рынков. Порой к операционным рискам относятся как к чему-то второстепенному по отношению к финансовым рискам. Риски операционные редко делят на различные детализированные «подриски», каждый из которых должен специально обрабатываться. Наверное, это именно тот случай, когда подход и государственного регулятора, и участников рынка заслуживает коренного пересмотра.

Благодаря повышению ответственности к регулированию операционных рисков, в том числе используя механизмы саморегулирования, можно заметно повысить эффективность противодействия киберпреступности. У Банка России уже есть неплохие наработки, нужно активизировать и работу отраслевых саморегулируемых организаций в этом направлении.

Развивая нормативно-правовую базу, контрольно-надзорную деятельности, мы можем вывести нашу работу на новый уровень. А именно, **ориентируя профессиональных участников финансового рынка на целенаправленное формирование политик и процедур управления операционных рисков — киберрисков**. Тех, что существуют по причине активности киберпреступников, «высокотехнологичных» мошенников.

Рассмотрим подробнее вопрос **программы обучения специалистов**. Точно так же, как в компаниях действуют подразделения и специалисты по информационной безопасности, должны работать и сотрудники, занимающиеся противодействием киберпреступности, кибермошенничествам.

Это новая специализация, но некоторое время назад на финансовом рынке не было и таких профессий, как актуарий — страховой математик или специалист по финансовому моделированию. Сегодня без таких сотрудников немислима нормальная работа банков, страховых компаний, пенсионных фондов. Востребованы специалисты, которые умеют создавать внутренние рейтинговые модели, необходимые для управления рисками, включая киберриски.

Однако к такой профессии пока целенаправленно не готовят! Впрочем, таким же образом государственному регулятору до сих пор не хватает профессиональных специалистов по надзору. А страховым компаниям — специалистов по медицинскому страхованию, которые бы обладали компетенциями и в страховом деле, и в медицине. Организация подготовки профессионалов востребованных на рынке профилей — актуальная задача, её решение — вопрос времени.

Хотелось бы, чтобы специалистов по такому направлению кибербезопасности, как киберриски, начали готовить по возможности скорее, начиная с программ профессиональной переподготовки. В текущем 2017 году Банк России будет участвовать в разработке профессионального стандарта «Специалист по информационной безопасности». Эту работу ведёт Комиссия по банкам и банковской деятельности Российского союза промышленников и предпринимателей, с участием представителей финансового рынка.

«ВСЕОБУЧ» ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Следующее важное направление обеспечения стратегии развития финансового рынка — повышение финансовой грамотности его участников, пользователей и клиентов. За происходящими изменениями, не во всём успевают не только граждане, но и корпорации, не в полной мере осознавая новые финансовые инструменты и процедуры. Возникают конфликты, связанные с продажами профессиональными участниками рынка ценных бумаг сложных финансовых продуктов предпринимателям. Дело доходит до судебных разбирательств, в ходе которых выясняется, что продавцы не полностью раскрыли покупателям информацию, не объяснили всю сложность продукта, его функционирования.

Подчёркиваю, что покупатели — это юридические лица, сотрудники которых являются профессионалами. Что же тогда говорить о потребителях финансовых услуг — физических лицах? Очевидно, что они — «слабое звено», в том числе в вопросах безопасности. Имеет смысл на определённое время административно ограничить их доступ к сложным, структурированным финансовым продуктам. До тех пор, пока не будет создан эффективный механизм информирования потребителей обо всех главных особенностях новых финансовых продуктов, а также механизм повышения их финансовой грамотности, включая вопросы безопасности.

Эти вопросы с точки зрения защиты прав потребителей подведомственны Банку России, так называемому поведенческому надзору. Краеугольным камнем является защита прав потребителей: оказание качественных услуг, раскры-

тие полной существенной информации о продукте. В доступной, понятной форме, чтобы такие сведения не нужно было долго-долго искать и вчитываться в пресловутый «мелкий шрифт».

Такая задача несколько отличается от классического надзора за банками, страховыми компаниями, пенсионными фондами, у которого другая задача — обеспечить устойчивость финансовую и бизнес-процессов в целом, чтобы они могли должным образом исполнять свои обязательства. Поведенческий надзор государственного регулятора имеет другую цель — чтобы юридические лица оказывали потребителям качественные финансовые услуги, что предполагает раскрытие важной информации. В наши дни не стремиться к этому считается не меньшим риском, чем не обеспечить устойчивость бизнес-процессов.

В 9–11 классах средних образовательных школ внедряется учебный курс финансовой грамотности, подготовленный Банком России совместно с Министерством образования и науки РФ. Пилотный проект был выполнен успешно, и к 2019 году этот курс будет преподаваться во всех школах, в разделе «Экономика» предмета «Обществознание».

Уже сегодня понятно, как дальше должна развиваться образовательная работа в финансовой сфере. Школьный курс финансовой грамотности посвящён чисто финансовым инструментам: вкладам, облигациям, ценным бумагам. Уже ясно, что не меньше внимания должно быть уделено вопросу, как их использовать.

Пока что в школьном учебнике, — не в методическом комплексе для учителей, а в самом учебнике, — про киберриски информационных технологий практически не говорится. Очевидно, что применение информационных технологий в финансовой сфере становится практически всеобъемлющим, а значит, школьный курс финансовой грамотности должен рассказывать о том, как они работают, о киберрисках, о мерах информационной безопасности. Далее, следующий шаг — распространение такого курса на высшие учебные заведения. И на взрослых, включая «ликбез» информационной безопасности для пенсионеров.

* * *

Общая задача участников отрасли двуединая. С одной стороны — развивать финансовый рынок на базе информационных технологий, предоставляя новые широчайшие возможности профессиональным участникам и клиентам — гражданам. С другой стороны — делать всё возможное, чтобы максимально обеспечить информационную безопасность, нейтрализовать киберпреступность в финансовой сфере.

Статья подготовлена на основании доклада Владимира Чистюхина, прочитанного 16 февраля 2017 года на IX Уральском форуме «Информационная безопасность финансовой сферы».



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



КИБЕРУСТОЙЧИВОСТЬ ФИНАНСОВОЙ СФЕРЫ: ЧТО ЭТО ТАКОЕ?

НЕОБХОДИМО УМЕТЬ
ПРЕДВИДЕТЬ КИБЕРАТАКИ,
ЭФФЕКТИВНО ЗАЩИЩАТЬСЯ
ОТ НИХ И БЫСТРО
ВОССТАНАВЛИВАТЬ
ПОЛНОЦЕННУЮ РАБОТУ

В чём заключается актуальность проблемы киберустойчивости для информационной безопасности финансовой сферы, не только в России, но и во всём мире? Пример — серьёзное обсуждение этого предмета, которое ведут руководители центральных банков стран «большой двадцатки». Разработан документ рамочного характера, посвящённый подходам к обеспечению киберустойчивости. Согласно обязательствам международного сотрудничества, принятым Российской Федерацией, предстоит выработать и аргументированно сформулировать своё отношение к этому вопросу.

РАДИ УСТОЙЧИВОСТИ БИЗНЕСА

Понятие киберустойчивости в финансовой сфере подразумевает, прежде всего, способность предвидеть кибератаки, защищаться от них и потом быстро восстанавливать полноценную работу. В нашей отрасли кибератаки относятся к операционным рискам, косвенно влияя на другие риски — ликвидности и кредитные. Согласно принципу окончательности, ликвидность финансовых институтов и их клиентов зависит от достоверности предположений о завершённости транзакций. Критериями оценки киберустойчивости в финансовой сфере служат возможности, во-первых, обеспечить проведение расчётов в сроки, отведённые на погашение обязательств, во-вторых — возобновить операции в течение двух часов после инцидента.

Следует помнить, что наша основная задача остаётся прежней: прежде всего, обеспечение устойчивости бизнеса, с учётом влияния различных факторов, в том числе технического характера. Киберустойчивость является подзадачей, включающей, в частности, противодействие кибератакам, минимизацию и скорейшее преодоление их последствий. Для решения этой частной задачи осуществляются обнаружение и идентификация атак, защита от них и последующее восстановление штатного функционирования системы. К основополагающим компонентам обеспечения киберустойчивости относятся тестирование, ситуационная осведомлённость, накопление знаний и развитие.

Вместе с тем обеспечение киберустойчивости обладает и новыми аспектами. Киберустойчивость является системным понятием, оно охватывает в целом информационную инфраструктуру финансового рынка, её значимых институтов, находящихся в юрисдикции Российской Федерации. Это Банк России, Национальная система платёжных карт как системно-значимая на рынке платёжных услуг, ряд ключевых банков, бирж.

Согласно классическому принципу информационной безопасности, общий уровень защиты информации зависит от слабого звена. Слабым звеном в единой цепочке могут оказаться организации, которые не уделяют должного внимания киберустойчивости, но непосредственно взаимодействуют с информационными инфраструктурами ключевых участников отрасли. Такими «слабыми звеньями» могут оказаться кредитные организации, а также производители продукции и поставщики услуг для них. В поле зрения, таким образом, оказывается практически весь финансовый рынок страны, а также провайдеры телекоммуникационных услуг, некоторые производители программного обеспечения и другие его участники.

**СЛЕДУЕТ ПОМНИТЬ, ЧТО
НАША ОСНОВНАЯ ЗАДАЧА
ОСТАЁТСЯ ПРЕЖНЕЙ: ПРЕЖДЕ
ВСЕГО, ОБЕСПЕЧЕНИЕ
УСТОЙЧИВОСТИ БИЗНЕСА**

Особое внимание киберустойчивости программного обеспечения начало уделяться в ходе общения с его производителем с прошлого 2016 года. Перенос электронной подписи документов непосредственно в автоматизированную банковскую систему, использование криптографии требовали обсуждения с разработчиками программного обеспечения, формулирования им мотивированного «технического задания».

Что и было сделано на рабочей встрече с двумя десятками разработчиков программного обеспечения, проведённой несколькими подразделениями центрального аппарата Банка России. На встрече была представлена позиция государственного регулятора в вопросе реализации переноса электронной подписи на сторону банка, план действий с просьбой сделать замечания, дать встречные предложения. Однако таковых, к нашему удивлению, не последовало. По всей видимости потому, что предложенные им сроки организации переноса подписей возражений не вызвали.

РЕНОВАЦИЯ НОРМАТИВНОЙ БАЗЫ

Для обеспечения киберустойчивости важно решение не только технических вопросов, но и создание организационно-правовых условий, наделение субъектов необходимыми полномочиями. На уровне федерального законодательства такая работа ведётся: соответствующий законопроект получил положительное заключение Правительства России и готовится к внесению на рассмотрение Государственной Думы РФ. Развитие законодательства позволит участникам отрасли не ограничиваться защитой только платёжных механизмов, но и полноценно заниматься обеспечением безопасности всей информационной инфраструктуры кредитных организаций.

Нужно правильно оценивать важность этих новых реалий. Можно привести простой пример, один из недавних инцидентов — хищение денег у кредитной организации. Её сотрудник получил мошенническое электронное «письмо счастья» с вредоносным программным обеспечением. Заранее разосланное предупреждение о возможности такого типа атак было проигнорировано.

В результате атаки злоумышленники получили несанкционированный доступ к управлению инфраструктурой кредитной организации и похитили денежные средства. В данной схеме злоумышленники использовали не платёжную инфраструктуру, а не относящиеся к ней сегменты финансового блока. Новые нормы федерального законодательства позволят предотвращать подобные инциденты, отражать информационные атаки такого типа.

Ещё одно направление совершенствования нашей нормативно-правовой базы — дальнейшее развитие стандартизации, государственной (ГОСТ) и корпоративной, организаций (СТО). Разрабатывается проект нормативов стандартизации аутсорсинга как защиты информации, так и информационной безопасности как таковой. Это важное направление, которое, с большой степенью вероятности, также обретёт форму ГОСТ.

Ряд технических деталей из ведомственных нормативных документов предполагается перенести в следующие стандарты:

- ♦ ГОСТ Р «Безопасность финансовых (банковских) операций. Базовый состав организационных и технических мер защиты информации» (вводится в 2017 году);
- ♦ СТО БР ИБСС / ГОСТ «Обеспечение защиты информации для цели непрерывности деятельности финансовых организаций»;
- ♦ СТО БР ИБСС / ГОСТ «Аутсорсинг защиты информации и взаимодействие с поставщиками информационных услуг» (название предварительное).

В пользу такого решения говорит мировой опыт. Информационная безопасность и защита информации в финансовой сфере волнует не только нас, но и наших коллег за рубежом. Интересный опыт есть в Сингапуре, где целенаправленно проработаны требования регулятора к аутсорсингу не только для кредитных организаций, но и для их поставщиков продуктов и услуг. По всей видимости, для повышения киберустойчивости и нам предстоит усилить взаимодействие не только с кредитными организациями, но и с теми, кто поставляет им информационные продукты и услуги.

ПРОГНОЗИРОВАТЬ, ОТСЛЕЖИВАТЬ, НЕЙТРАЛИЗОВАТЬ

К настоящему времени в отраслевом обмене данными в сфере информационной безопасности участвуют порядка 330 организаций. Наверное, на сегодняшний момент это редкий случай такого взаимодействия, в котором активно участвуют, кроме государственного регулятора в лице Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) ГУБ и ЗИ Банка России, также большое количество различных участников отрасли. Новые нормы будут обосновывать и развитие информационных сервисов ФинЦЕРТ, и достоверный контроль государственного регулятора за подведомственными организациями.

Такое взаимовыгодное сотрудничество плодотворно, оно даёт ощутимые результаты. Удаётся своевременно выявлять новые типы информационных атак, получать неординарные схемы компрометации разных банков — и своевременно предупреждать о новых угрозах коллег, помогая уберечь от попыток хищений финансовые средства. Что подтверждает известный принцип: вовремя предупреждён — значит, вооружён.

На сегодняшний момент в комплексе документов Банка России в области стандартизации информационной безопасности есть практически все, что необходимо банкам для обеспечения киберустойчивости. Пока что, возможно, не хватает дополнения — документов, определяющих подход к обеспечению отказоустойчивости и непрерывности бизнеса. Этот пробел в обозримом будущем должен быть восполнен.

ПО ВСЕЙ ВИДИМОСТИ, ДЛЯ ПОВЫШЕНИЯ КИБЕРУСТОЙЧИВОСТИ И НАМ ПРЕДСТОИТ УСИЛИТЬ ВЗАИМОДЕЙСТВИЕ НЕ ТОЛЬКО С КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ, НО И С ТЕМИ, КТО ПОСТАВЛЯЕТ ИМ ИНФОРМАЦИОННЫЕ ПРОДУКТЫ И УСЛУГИ

Следует отметить, что регулярное наблюдение зафиксировало увеличение количества кибератак в финансовой сфере практически вдвое за прошлый 2016 год. С каждым месяцем всё больше рассылок электронных писем, содержащих различное вредоносное программное обеспечение с элементами социальной инженерии. Характер уловок злоумышленников крайне разнообразен. Мошеннические SMS-рассылки множатся просто в геометрической прогрессии: ежедневно поступает по пять-десять заявлений от сознательных граждан, а сколько получателей никуда не обращаются.

С другой стороны, есть и положительная тенденция. Хотя количество и разнообразие кибератак в финансовом секторе растут, их результативность снижается. Ряд информационных атак, зафиксированных нами в конце прошлого и в начале этого года, не принесли существенных осложнений ни одной кредитной организации. Кроме отдельных временных неудобств, не был нарушен ни один сервис.

Среди угроз нового типа — попытки злоумышленников использовать «умные вещи». Становятся возможными криминальные инструменты, которых прежде не было, например, создание бот-сети из смарт-телевизоров. Для своевременного отслеживания и нейтрализации таких прогнозируемых информационных угроз нужно усиление взаимодействия с Минкомсвязи РФ и Федеральным агентством связи — Россвязью.

* * *

Киберустойчивость действительно важна и нужна, её актуальность возрастает с каждым годом. Банк России, модернизируя свои информационные системы, в том числе платёжную систему, старается заложить в них достаточно высокую надёжность. Что означает устойчивое бесперебойное предоставление сервисов, несмотря на проблемы, которые могут возникнуть. Такой подход к киберустойчивости должен быть положен в основу бизнес-процессов организаций финансовой сферы.



ПАРТНЕРСТВО С БИЗНЕСОМ И AGILE

НОВЫЕ ИНСТРУМЕНТЫ КИБЕРБЕЗОПАСНОСТИ

Продолжаем публикацию цикла материалов об изменениях в работе Службы кибербезопасности ПАО «Сбербанк России». На вопросы BIS Journal отвечает Иван Янсон, бизнес-партнер по информационной безопасности ПАО «Сбербанк России».

СБЕРБАНК — ЭТО МАСШТАБ

BIS Journal: Ваш большой опыт работы в сфере информационной безопасности банков дает Вам возможность и право сравнивать. Чем Служба кибербезопасности Сбербанка отличается от служб безопасности других финансовых структур?

И. Янсон: В первую очередь масштабностью, большим многообразием и высокой специализацией выполняемых функций. Следствием этого является наличие редких и даже уникальных подразделений в его составе. Наиболее заметные — это Центр киберзащиты (CDC), Дирекция по управлению программами кибербезопасности, а также Центр обеспечения взаимодействия с бизнесом, в котором работают бизнес-партнеры по информационной безопасности. Все эти подразделения по-своему уникальны, аналоги не часто встречаются, например, я не слышал о том, чтобы в каком-то банке было подразделение, похожее на Центр взаимодействия с бизнесом.

МНОГО НОВОГО

Наименования других подразделений Службы более привычны для уха безопасника, но это не означает, что за этими названиями не стоит ничего нового. Например, отдел информационной безопасности в ИТ-проектах. Подобные подразделения или, по крайней мере, отдельные специалисты такой направленности, есть во многих банках, но мало где это подразделение участвует в обеспечении ИБ почти на всех стадиях жизненного цикла автоматизированных банковских систем (АБС). В Сбербанке же отдел ИБ в ИТ-проектах участвует и при проектировании, и при разработке, и на стадии приемки в эксплуатацию — на приемо-сдаточных испытаниях АБС. Свыше 30 сотрудников закладывают элементы подсистемы ИБ в многочисленные АБС Банка, участвуя в сотнях ИТ-проектов в течение года. Они закладывают требования ИБ в бизнес-требования, концептуальные архитектуры, проверяют выполнение этих требований в спецификациях и технических заданиях, контролируют реализацию при приемке систем в эксплуатацию. В каком-то смысле, это фабрика информационной безопасности, как в плане непрерывного участия в ИТ-проектах, так и в плане масштабности работы.

BIS Journal: Расскажите, пожалуйста, подробнее о структуре, которая занимается взаимодействием с бизнесом...

И. Янсон: Сотрудники, работающие в Центре обеспечения взаимодействия с бизнесом, называются бизнес-партнерами по информационной безопасности. Их основная функция — быть своего рода коннекторами между бизнесом и подразделениями ИБ, причем, коннекторами, призванными ускорять, улучшать это взаимодействие в обоих направлениях, как от безопасности к бизнесу, так и от бизнеса к безопасности.

БИЗНЕС-ПАРТНЕР — НЕ ПЕРЕВОДЧИК

Что это означает? Многие, когда слышат слова «бизнес-партнер», думают, что речь идет о сотрудниках, которые должны переводить требования безопасности с языка безопасности на язык бизнеса. На самом деле, переводить никому ничего не нужно. Бизнес-подразделения и ИТ-подразделения, внедряющие бизнес-продукты, как правило, достаточно хорошо понимают необходимость обеспечения безопасности и неплохо разбираются в способах и средствах ее обеспечения. Конечно, иногда приходится выполнять и роль «переводчика», но это не основная функция бизнес-партнера. Основная — ускорение взаимодействия безопасности и бизнеса.

Как уже говорилось, в Сбербанке ведутся сотни проектов, требующих доработок ИТ-систем. Есть бизнес-подразделения и ИТ-подразделения, которые вовлечены в такие проекты. Есть линейные подразделения ИБ, которые обеспечивают наличие подсистемы безопасности в рамках таких доработок. Во взаимодействии указанных подразделений иногда возникают сложности, например, с очередностью участия специалистов Службы кибербезопасности в ИТ-проектах. И тут бизнес-партнер, хорошо понимая потребности бизнеса,



Иван ЯНСОН
бизнес-партнер
по информационной
безопасности Службы
кибербезопасности
ПАО «Сбербанк России»

МНОГИЕ, КОГДА СЛЫШАТ СЛОВА «БИЗНЕС-ПАРТНЕР», ДУМАЮТ, ЧТО РЕЧЬ ИДЕТ О СОТРУДНИКАХ, КОТОРЫЕ ДОЛЖНЫ ПЕРЕВОДИТЬ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ С ЯЗЫКА БЕЗОПАСНОСТИ НА ЯЗЫК БИЗНЕСА. НА САМОМ ДЕЛЕ, ПЕРЕВОДИТЬ НИКОМУ НИЧЕГО НЕ НУЖНО

выстраивает приоритеты при решении соответствующих задач, помогает выполнить их более оперативно. Приоритет запросов может определяться плановыми датами открытия проектов, датами включения доработок в плановые интеграционные релизы, сроками запуска банковских услуг и продуктов, которые могут быть не известны сотрудникам безопасности. Чтобы повысить приоритет того или иного запроса, необходимо согласовать его с заказчиками других доработок, с которыми приходится меняться местами, что бывает не просто в ситуации недостаточного ресурса.

Сложности могут возникать не только с медленной обработкой запросов. Время от времени возникает ситуация, когда требования моих коллег вызывают неполное понимание со стороны заказчиков. Эти требования могут быть или сложно выполнимыми, или затрудняющими быстрый ввод в эксплуатацию продуктов, или вовсе запретительными по отношению к внедряемым бизнес-продуктам. В таких случаях бизнес-партнер погружается в суть проекта, разбирается в том, что же требуют его коллеги из безопасности, и что мешает, вызывает проблемы у бизнеса. Для устранения проблемы бизнес-партнер может предложить постоянные или временные альтернативные решения, организовать совместный поиск таких решений силами безопасности и бизнеса. Иногда приходится вести и разъяснительную работу, чтобы коллеги поняли, почему нельзя не внедрять те или иные защитные меры и механизмы, чем чревато их отсутствие.

Кроме того, важной задачей бизнес-партнера является оказание помощи коллегам-безопасникам в продвижении решений информационной безопасности и в эскалации проблем. Чаще всего это бывает при необходимости устранения тех или иных уязвимостей. Необходимо донести до бизнес-подразделений сигнал об угрозах, реализовавшихся или возможных инцидентах, объяснить, какие это может иметь последствия для клиентов, Банка, договориться о выделе-

нии ресурса разработчиков, ускорении внедрения защитных мер. Линейным подразделениям кибербезопасности может быть сложно, а подчас просто некогда заниматься эскалацией проблем на руководителей бизнес-подразделений, и в этом мы, бизнес-партнеры, помогаем своим коллегам.

АЛЬТЕРНАТИВНЫЕ РЕШЕНИЯ

BIS Journal: Можете привести пример поиска альтернативных решений?

И. Янсон: При разработке онлайн-сервиса может возникнуть задача его функционального тестирования из сети Интернет. Конечно, при вводе в эксплуатацию он должен быть проверен на уязвимости, и уязвимости должны быть устранены, поэтому при тестировании специалисты безопасности могут предложить запретить доступ к ресурсу из сети Интернет до устранения уязвимостей. Но можно предложить компромиссный вариант: временно, не устраняя уязвимостей, разрешить только ограниченный доступ к такому тестовому ресурсу из сети Интернет, например, только с определенных адресов, защитив его с помощью сетевых средств защиты и поставив на адресный мониторинг в центре киберзащиты. Такое решение позволит быстрее осуществить тестирование, а значит и внедрение ресурса и связанного с ним бизнес-продукта или услуги. В другом случае требование безопасности говорит о необходимости автоматизированной проверки электронной подписи под поступающими электронными документами. Но на период опытной эксплуатации на ограниченных объемах можно предложить использовать проверку ЭП силами клиентских менеджеров на их компьютерах, либо применить автоматизированную проверку, но не в целевой системе. А автоматизированную проверку в самой целевой системе реализовать на втором этапе при переходе к промышленной эксплуатации.

Отмечу, что часто для того, чтобы найти подходящее постоянное или временное альтернативное условие, бывает достаточно собрать частных специалистов разных подразделений для совместного обсуждения вопроса. И здесь как раз роль бизнес-партнера состоит в том, чтобы, рассмотрев задачу в целом, созвать достаточный для коллегиальной выработки решения консилиум, состоящий из сотрудников ИБ разных специальностей. Кстати, даже при штатной работе это тоже бывает полезно, так как позволяет быстрее получить сводный результат в случаях, когда задействованы специалисты разных направлений ИБ.

**ИНОГДА ПРИХОДИТСЯ ВЕСТИ
И РАЗЪЯСНИТЕЛЬНУЮ РАБОТУ,
ЧТОБЫ КОЛЛЕГИ ПОНЯЛИ, ПОЧЕМУ
НЕЛЬЗЯ НЕ ВНЕДРЯТЬ ТЕ ИЛИ ИНЫЕ
ЗАЩИТНЫЕ МЕРЫ И МЕХАНИЗМЫ,
ЧЕМ ЧРЕВАТО ИХ ОТСУТСТВИЕ**



BIS Journal: Вы говорили о сотнях ИТ-проектов. То есть у вас происходят какие-то серьезные изменения внутри банка?

И. Янсон: Количество ИТ-проектов не говорит о том, что происходят какие-то специальные изменения, просто Сбербанк живет очень динамичной жизнью. В каждом бизнес-блоке есть проектный офис, который ведет несколько десятков, а в крупных блоках даже более сотни проектов по автоматизации в год. Каждый проект по автоматизации означает, что либо внедряется новый бизнес-продукт, либо меняется существующий. Перед бизнесом стоят весьма амбициозные задачи, его главный тренд — это всеобщая дигитализация продуктов, перевод их в дистанционные каналы. Очень активно все происходит, очень масштабно.

ПЕРЕХОД НА AGILE

Количество проектов по автоматизации, сроки ввода в эксплуатацию продуктов и сервисов продиктовали банку необходимость внедрения нового подхода по ведению доработок. Раньше доработки велись классическим проектным путем,

В БЛИЖАЙШИЕ ГОДЫ БАНКИ БУДУТ КОНКУРИРОВАТЬ НЕ МЕЖДУ СОБОЙ, А С ТАКИМИ СОВРЕМЕННЫМИ ИТ-КОМПАНИЯМИ, КАК GOOGLE, AMAZONE, КОТОРЫЕ УМЕЮТ ОЧЕНЬ БЫСТРО ВНЕДРЯТЬ ИЗМЕНЕНИЯ В СВОИ ИТ-ПЛАТФОРМЫ

который в Сбербанке носит название сквозного производственного процесса. Это, безусловно, хороший путь, но он не позволяет вносить много изменений в продукты. В ближайшие же годы банки будут конкурировать не между собой, а с такими современными ИТ-компаниями, как Google, Amazone, которые умеют очень быстро внедрять изменения в свои ИТ-платформы. Соответственно, мы должны идти с ними, как минимум, в ногу. Руководством Сбербанка был взят курс на внедрение гибкой методологии разработки — Agile.

ОТ МНОГОУРОВНЕВОЙ ИЕРАРХИЧЕСКОЙ ОРГАНИЗАЦИИ И СОГЛАСОВАНИЙ МНОГИХ РЕШЕНИЙ ЧЕРЕЗ РУКОВОДСТВО СБЕРБАНК ПЕРЕХОДИТ К ПЛОСКОЙ СТРУКТУРЕ С ТРЕМЯ УРОВНЯМИ ИЕРАРХИИ ОТ ПРАВЛЕНИЯ БАНКА

BIS Journal: Методология управления проектами Agile стала трендом во многих сферах, и не везде ее понимают одинаково. Давайте уточним, что такое Agile в сфере ИБ?

И. Янсон: Agile в ИБ (да и в любой другой сфере) — это прежде всего эффективная практика организации труда, которая подразумевает гибкость организации команд, переход к коллаборативности (сотрудничеству и самоорганизации) сотрудников.

Внедряя методы Agile, Сбербанк преследует такие цели, как максимальная удовлетворенность клиентов, лучший клиентский опыт, непрерывные и быстрые улучшения продуктов и процессов за счет внешних и внутренних инноваций, уменьшение времени выхода продукта (Time-to-Market), добавление новой функциональности в продукт каждые две недели, повышение эффективности и продуктивности, а также удовлетворенности и вовлеченности персонала и т.д.

ИЗМЕНЕНИЯ

В рамках Agile-трансформации будут проведены масштабные изменения. От многоуровневой иерархической организации и согласований многих решений через руководство Сбербанк переходит к плоской структуре с тремя уровнями иерархии от Правления банка. Изменения становятся основой повседневной деятельности, они становятся децентрализованными, построенными на доверии, делегировании полномочий.

От организационно-функциональных колодцев банк переходит к применению кросс-функциональных команд и трайбов. От частичного вовлечения сотрудников в разные проекты к Full time работе в одной команде/над одной задачей, от так называемой водопадной модели работы и глобальных изменений с длительным процессом их подготовки к разработке Minimum Viable Product (MVP) — минимальной версии продукта либо новой крупной функциональности в нем, внедряемой для ранней обратной связи от клиентов. Созда-

ние MVP можно перефразировать так: «Не надо все и сразу, создавайте продукт инкрементально!».

СТРУКТУРА

В основе структуры Agile-организации Сбербанка лежат такие организационные единицы, как трайбы, команды и чаптеры.

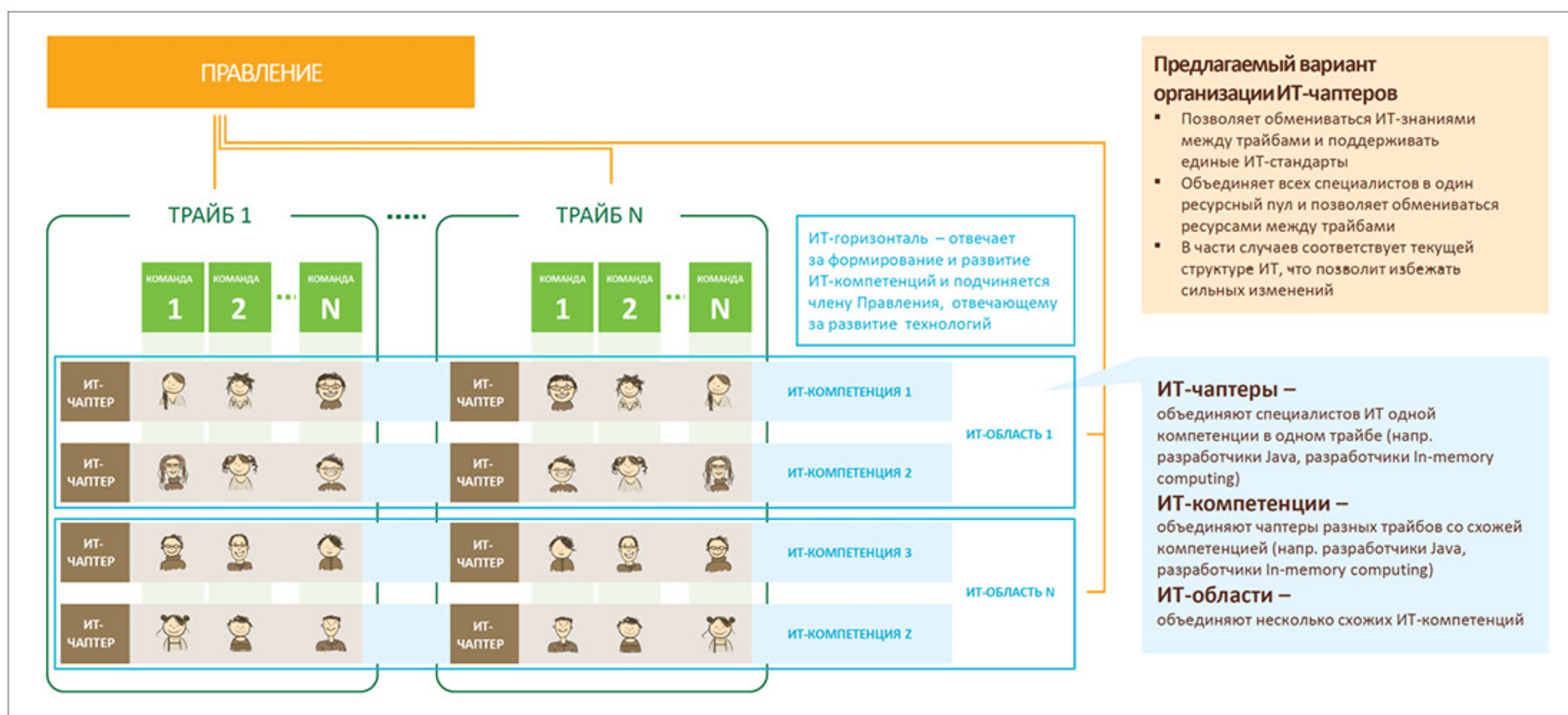
Команда — это кросс-функциональная совместно работающая группа специалистов, обладающая всеми навыками, инструментами и полномочиями, достаточными для самостоятельной разработки конечного продукта. Численность команды — порядка 10 сотрудников. Трайб — это группа взаимосвязанных команд, сформированная вокруг определенного продукта/бизнес-цели и отвечающая за бизнес-результат. Численность трайба — не более 150 человек. Специалисты одной области компетенции из разных команд трайба объединяются в чаптеры.

Согласно типам решаемых задач, трайбы и команды в Сбербанке могут быть двух типов: клиенториентированные и платформенные. Первые реализуют элементы бизнес-задач и клиентского опыта, например, продукты или клиентские путешествия. Вторые создают базовые модули платформ, предоставляющих стандартные сервисы множеству других команд.

Основное преимущество работы в небольшой кросс-функциональной команде состоит в том, что все специалисты внутри команды общаются во время работы над продуктом или бизнес-целью, обсуждают возникшие проблемы, мгновенно получают ответы на возникшие вопросы. Все это позволяет чаще создавать новые версии продукта, чаще выпускать их на рынок и чаще оценивать эти версии клиентами.

Процесс работы над задачей или продуктом разбивается на спринты, которые длятся 2 недели. Спринты объединяются в суперспринты. Суперспринт длится ровно 12 недель и состоит из 6 спринтов.

Спринт — это такт работы команды, в ходе которого создается новая версия продукта, так называемый инкремент продукта, то есть приращение функциональности продукта, которое демонстрируется заказчику, но не обязательно клиентам. Супер-спринт — это такт работы трайба, в ходе которого создается главная версия продукта трайба, как совокупность результатов работы всех команд. В рамках супер-спринта выпускается и внедряется для использования клиентами, как минимум, один релиз продукта. При этом используется концепция MVP, то есть создается минимально необходимая версия продукта с приемлемым функ-



ционалом, которая может быть предоставлена клиентам, и по которой можно получить раннюю обратную связь от клиентов.

ОБРАТНАЯ СВЯЗЬ

Основная идея использования спринтов, суперспринтов и создания MVP состоит в том, что чем раньше мы получим обратную связь от клиентов, тем быстрее будет реализована необходимая для клиентов функциональность, и тем раньше мы обнаружим и быстрее, и с меньшими затратами устраним ошибки реализации. При традиционной проектной разработке ошибки могут быть обнаружены слишком поздно и их устранение может очень дорого стоить.

Кроме команд, чаптеров, трайбов вводится такая сущность, как ИТ-горизонталь — один из инструментов обеспечения целостности ИТ-стандартов и подходов. ИТ-горизонталь состоит из ИТ-чаптеров, ИТ-компетенций и иногда ИТ-областей. ИТ-чаптер — это чаптер трайба, который состоит из ИТ-специалистов. ИТ-компетенция в свою очередь является объединением ИТ-специалистов из ИТ-чаптеров со схожей компетенцией (рис. 1).

Аналогичная горизонталь вводится для бизнеса. Целостность каналов и продуктов обеспечивается Бизнес-горизонталью.

РОЛЬ БЕЗОПАСНИКОВ В AGILE

Agile также потребует от безопасности более гибкого участия в создании продуктов и услуг. Специалисты по ИБ выполняют роль экспертов предметной области. Они привлекаются к работе трайбов по мере необходимости получения экспертизы по вопросам информацион-

ной безопасности. Они могут привлекаться в команду, как временные участники с загрузкой 100% или с меньшей загрузкой. В первой волне Agile-трансформации, которая продолжалась до февраля этого года, участвовали 8 трайбов, сфокусированных на макропотребностях клиента, и 1 платформенный трайб. В эти трайбы входили сотрудники отдела информационной безопасности в ИТ-проектах. Часть своего времени они проводили в Agile-командах, а часть — работали по привычной схеме в офисе.

В перспективе большая часть ИБ-специалистов Сбербанка перейдет на такой режим работы. Участие с их стороны в работе команд требуется достаточно часто, так как изменения в продукт будут вноситься быстро (напомню, что инкремент продукта выпускается по окончании каждого спринта, MVP должен внедряться не реже одного раза в течение суперспринта). При этом появляется задача организации процесса поддержания уровня компетенции у сотрудников ИБ. То есть время от времени специалистов ИБ надо будет «выдергивать» из трайба и отправлять на внутреннюю или внешнюю учебу/инструктаж.

В целом, обеспечение требований ИБ на стадиях разработки АБС Банка, выполняемой по методологии Agile, — это довольно интересная задача для информационной безопасности, к решению которой мы уже приступили в ряде проектов Банка. По мере приобретения практического опыта мы готовы поделиться им с читателями BIS Journal.

Рисунок 1.
Организация
ИТ-чаптеров

SWIFT ПОВЫСИТ САМООЦЕНКУ БАНКОВ



Матвей ГЕРИНГ
руководитель SWIFT
по России, СНГ
и Монголии

Программа повышения информационной безопасности для клиентов системы SWIFT позволит банкам усилить меры безопасности и ужесточить контроль за межбанковскими платежами.

Во втором квартале 2017 г. Международная межбанковская система передачи информации и совершения платежей SWIFT вводит новые требования к информационной безопасности банков-клиентов. Поводом для беспокойства стал получивший широкую огласку случай вывода средств со счетов Центрального Банка Бангладеш. Инцидент произошел в начале 2016 г., он не затронул систему SWIFT, но оказался показательным для финансовых организаций.

АТАКА НА ЦБ БАНГЛАДЕШ

При помощи вредоносного программного обеспечения злоумышленники получили доступ к системам Центрального Банка страны. Используя достоверные логины и пароли, в четверг вечером, накануне долгих выходных в банке-отправителе и банке-получателе, когда время для проверки сократилось до минимума, хакеры запустили платежные поручения в общей сложности на \$1 млрд. Все параметры транзакций были легитимны с технической точки зрения, платежи прошли по цепочке международных корреспондентских отношений. Заключительный этап преступления — сокрытие сведений о платежах в системе реконсильации путем ее взлома и уничтожения сообщений о проводках из выписок, которые идут через систему SWIFT.

Этот случай подробно описан в многочисленных публикациях. Часть платежных поручений вызвала подозрения у служащих ФРБ Нью-Йорка, однако некоторые проводки были исполнены. И хотя Центробанку Бангладеш удалось вернуть часть средств, добычей хакеров стали \$81 млн.

РЕАКЦИЯ SWIFT

Как реагировала компания SWIFT на этот и подобные инциденты? В июне 2016 года она объявила о запуске программы SWIFT Customer Security Programme (CSP), которая направлена на повышение мер по обеспечению информационной безопасности в финансовой сфере.

Программа основывается на пяти стратегических целях:

- ♦ улучшение процессов обмена информацией среди мирового сообщества;
- ♦ улучшение инструментов SWIFT для клиентов;
- ♦ улучшение рекомендаций и предоставление методологической базы по аудиту безопасности;
- ♦ улучшение процессов по обнаружению мошеннических паттернов транзакций;
- ♦ улучшение поддержки третьими сторонами.

В августе 2016 г. SWIFT объявила о запуске кампании повышения осведомленности о функциях безопасности, имеющих в продуктах SWIFT. Мероприятия проходят в рамках CSP. Позднее был выпущен новый инструмент Daily Validation Reports, который дополняет уже существующий инструментарий и позволяет быстро обнаружить мошеннические действия в системе, если злоумышленник пытается скрыть свою активность в сети банка путем изменения или уничтожения сведений о платежных сообщениях или данных реконсильации, как это было в случае взлома ЦБ Бангладеш. Отчеты предоставляются через закрытый канал, что дает возможность получать проверенную информацию даже в случаях, когда клиентская часть ПО SWIFT была скомпрометирована, в инциденте замешаны сотрудники банка, а локальные данные изменены.

Также компания SWIFT объявила о введении основных стандартов безопасности и методологической базы по аудиту для клиентов системы. Стандарты обязательны для всех клиентов SWIFT и начнут действовать со второго квартала 2017 г.

ЦЕЛИ И ПРИНЦИПЫ CSP

Ранее представленная общественности программа Customer Security Programme (CSP) преследует 3 цели, они сформулированы предельно кратко: защити свое окружение; знай и ограничь доступ; обнаруживай и реагируй. Исходя из этих целей, определены 8 принципов ИБ. Каждый банк должен нести ответственность за собственную безопасность путем соблюдения следующих требований:



Рисунок 1.
Customer Security
Programme (CSP)

- ♦ ограничение доступа в Интернет;
- ♦ разделение критически важных систем от общих IT-систем;
- ♦ устранение уязвимостей системы и сокращение возможностей для атак хакеров;
- ♦ обеспечение физической защиты систем;
- ♦ предотвращение компрометации учетных данных;
- ♦ управление пользовательскими привилегиями;
- ♦ обнаружение аномальной активности в сети;
- ♦ совместное использование методов разведки и разработка процедур реагирования в случае инцидентов.

САМООЦЕНКА ПО 27 ПУНКТАМ

Согласно новым требованиям SWIFT, со второго квартала текущего года клиенты компании обязаны осуществлять и ежегодно предоставлять результаты самооценки по 27 пунктам контроля. После официального выхода требований и до конца текущего года все банки России и мира, работающие с компанией SWIFT, должны будут провести самостоятельную оценку информационной безопасности финансовой организации на соответствие требованиям международной системы.

27 пунктов контроля основаны на упомянутых выше трех целях и 8 принципах, которые

в том или ином виде ранее были прописаны в нормативных документах (NIST, PCIDSS и ISO 27002). На практике — это 16 обязательных и 11 рекомендуемых правил. Все 27 принципов контроля сформированы на базе обратной связи пользователей, с учетом национальных особенностей и мнений крупных и мелких финансовых организаций.

В России со SWIFT работают 90% всех банков, и стоит подчеркнуть, что в августе 2016 г., когда принципы CSP были впервые опубликованы на сайте компании SWIFT, Банк России и другие национальные регуляторы на следующий же день известили своих корреспондентов о необходимости следовать рекомендациям SWIFT по ИБ. Это свидетельствует о тесной совместной работе системы и регуляторов.

После официальной публикации программы CSP, 95–98% банков в мире должны будут провести самооценку с помощью защищенно-

СО ВТОРОГО КВАРТАЛА ТЕКУЩЕГО ГОДА КЛИЕНТЫ КОМПАНИИ ОБЯЗАНЫ ОСУЩЕСТВЛЯТЬ И ЕЖЕГОДНО ПРЕДОСТАВЛЯТЬ РЕЗУЛЬТАТЫ САМООЦЕНКИ ПО 27 ПУНКТАМ КОНТРОЛЯ

SWIFT ОБЕСПЕЧИВАЕТ ЕДИНУЮ ПЛАТФОРМУ, ЕДИНЫЙ СТАНДАРТ, ЕДИНЫЙ ПРОТОКОЛ ДЛЯ МЕЖДУНАРОДНОГО ПЕРЕВОДА ДЕНЕГ. СО ВРЕМЕНЕМ К ЭТИМ ТРЕБОВАНИЯМ ДОБАВИЛИСЬ ЕЩЕ И СТАНДАРТЫ ИБ

го и распространяемого бесплатно инструмента системы SWIFT. Некоторым банкам придется сделать не только саму оценку, но и инспекцию на базе статистического образца. Это значит, что служба внутреннего аудита должна будет соблюсти и подчиниться все тем же 27 принципам контроля. Некоторым пользователям системы потребуется аудит третьей стороны, которая проведет инспекцию и укажет, внедрены ли 16 обязательных и 11 рекомендованных правил.

АУДИТ ТРЕТЬЕЙ СТОРОНЫ

Организации, нуждающиеся в оценке третьей стороны, — это сервис-бюро и другие пункты коллективного доступа. Классический пример сервис-бюро — пункт коллективного доступа к SWIFT Центрального Банка Беларуси, через который работают почти все банки страны. В России действует 5 сервис-бюро, им также потребуется инспекция третьей стороны. Оценка их безопасности должна быть произведена до конца 2017 г.

Начиная с января 2018 г., компания SWIFT будет сообщать обо всех не соблюдающих стандарты клиентах, выбирать случайным образом клиентов, которые должны будут предоставить дополнительное подтверждение или от своих внутренних, или от внешних аудиторов. Также клиенты системы могут сообщать о своих соответствиях 11 рекомендательным пунктам контроля в дополнение к 16 обязательным.

Полная документация по контролю доступна в базе знаний — Knowledge Base tip 5020786. на сайте компании.

SOC ОТ КОМПАНИИ SWIFT

Одна из целей и задач системы SWIFT, сформулированная при создании компании 40 лет назад, — непосредственная помощь банкам — участникам системы при работе между собой и со своими контрагентами. SWIFT обеспечивает единую платформу, единый стандарт, единый протокол для международного перевода денег. Со временем к этим требованиям добавились еще и стандарты ИБ.

У компании SWIFT, как у многих организаций, есть своя служба ИБ. Она работает напрямую с разными FinCERT в мире, в том числе с ФинЦЕРТ Банка России. Мы получаем тысячи сообщений о попытках компрометации от финансовых организаций и, как и другие подобные нам организации, обрабатываем эту информацию и предоставляем ее пользователям, чтобы исключить повторение подобных инцидентов в мире. Информация о попытках или случаях компрометации, которая становится известна SWIFT, распространяется среди наших пользователей анонимно, без указания на место происхождения.

На фоне хакерских атак мировое финансовое сообщество потребовало от SWIFT разработать собственный центр информационной безопасности и сбора информации (SOC), который откроется в этом или следующем году. Мы работаем с опытной командой киберразведки, стандартизируем формат отчетности, которому будут следовать наши пользователи, тесно работаем с вендорами.

ПАТЧИ И ИНТЕРФЕЙСЫ

Еще одна задача программы CSP — помочь банкам стать более устойчивыми к кибератакам. По итогам известных инцидентов, мы провели аудит систем ИБ вместе с национальными банками. Исследование показало, что сама сеть системы SWIFT, служба транспорта финансовых сообщений, не были скомпрометированы. Мы регулярно сообщаем о проводимых работах по усилению мер информационной безопасности системы и контролю их работы.

Как пример положительной работы можно упомянуть установку обновлений систем ИБ. Сегодня, выпуская патч Monitory Upgrade, касающийся обновления системы безопасности, мы связываемся с регулятором конкретной страны и ставим сроки обязательного внедрения обновления. Как показывает практика, рекомендации SWIFT, подкрепленные указаниями национальных регуляторов, идут на пользу ИБ банков конкретной страны. С 2016 г., когда мы начали взаимодействовать с Банком России и еще 212 центробанками разных стран, финансовые организации стали чаще устанавливать патчи на программное обеспечение.

Мы прилагаем все усилия, чтобы обеспечить максимальную безопасность интерфейсов системы, т.е. пунктов доступа к системе. SWIFT-интерфейсы всех уровней доступа к системе, которые предоставляем мы или третьей стороны, сертифицируются самой компанией. Еще одна, третья категория интерфейсов, — пункты коллективного доступа к системе SWIFT, которыми в России пользуются 2/3 банков. Собствен-

ное подключение банка к системе предполагает наличие у пользователя сложной технической инфраструктуры, специализированных каналов связи, квалифицированного персонала для осуществления целого ряда регламентных процедур обслуживания, а также лицензий, связанных с использованием шифровальных средств. Все это требует от финансовой организации больших материальных затрат.

Коллективный доступ к системе предоставляется через сервис-бюро, прошедшее сертификацию в SWIFT, и обходится банкам намного дешевле индивидуального. SWIFT работает со всеми тремя уровнями доступа к системе.

SWIFT В РОССИИ

Система SWIFT существует 40 лет и 26 из них она работает в России, где функционирует 500 банков и 450 из них работает с международной системой.

В России, как и других странах, мы работаем через ассоциацию пользователей. В РФ ассоциацию представляет РуСвифт, в котором есть технический комитет, его возглавляет CEO Национального Расчетного Депозитария (НРД).

Готовя программу CSP, которая состоит из 27 пунктов контроля, мы разослали ее для обсуждения национальным группам всех 212 стран — пользователей SWIFT. Россия оказалось одной из 90 стран, которые очень подробно ответили и высказали свое мнение по поводу этого документа. В российском ответе были выражены мнения как крупнейших финансовых организаций, так и средних и мелких банков.

Представители компании SWIFT очень плотно сотрудничают в сфере ИБ на уровне руководства программы CSP и руководства РуСвифт. Рабочие встречи проходят раз в квартал и потому у российского представительства есть возможность получать больше информации. Стоит отметить, что благодаря сотрудничеству российских банков с компанией SWIFT, подавляющее большинство нормативных документов SWIFT переведено на русский язык.

ПРЕДУПРЕЖДЕН — ЗНАЧИТ ВООРУЖЕН

В перспективе CSP пополнится еще рядом сервисов, которые разрабатываются компанией SWIFT. Один из них позволяет через независимый канал получить файл отчета Risk Report в формате.pdf с предупреждениями о необычных действиях, нехарактерных для данного банка: очень крупных сумм денег, денежных переводах в валюту некой страны или в банк некой страны, с которой ранее не было взаимоотношений. Такой файл с предупреждением минимизирует риск финансовых потерь, даже если кто-то скомпрометировал пункт доступа в систему SWIFT и уничтожил следы самого платежа, как это было в том же центробанке Бангладеш.

Еще один сервис находится на стадии обсуждения Советом директоров SWIFT, в котором участвует и Россия. Многие банки, как крупные, так и мелкие, просят установить промежуточную систему контроля платежей, хотя такая система контроля не входит в изначальные задачи системы SWIFT. Поэтому сейчас надо точно определить, что и как мы должны контролировать внутри системы. Надеюсь, что подобные предложения будут представлены Советом директоров в течение первой половины года и поступят на всеобщее обсуждение.

* * *

Также SWIFT продолжит работу над сертификацией третьих сторон, поскольку компания, выдвинув 27 правил контроля, не сможет одновременно и отслеживать их выполнение банками-клиентами системы, и проводить внешний аудит. Поэтому SWIFT сертифицирует третьи стороны, чтобы они были независимыми экспертами при организации проверок банков на соблюдение требований международной платежной системы SWIFT.

СПРАВКА

Международная межбанковская система передачи информации и совершения платежей SWIFT объединяет примерно 10 тысяч пользователей в мире и еще порядка 1000 корпораций, в т.ч. более 150 центральных банков. Контроль за системой SWIFT осуществляет Национальный банк Бельгии, который координирует работу 20 центральных банков, в т.ч. Банка России. В день через SWIFT проходит более 1 млн транзакций — денежные переводы, межбанковские платежи, ценные бумаги. Ежегодно через SWIFT проходит 2,5 млрд платежных поручений.

Статья подготовлена на основании доклада Матвея Геринга, прочитанного 14 февраля 2017 года на IX Уральском форуме «Информационная безопасность финансовой сферы».



Сергей ДЕМИДОВ
директор департамента
операционных рисков,
ИБ и непрерывности
бизнеса Московской
биржи

РАЗНООБРАЗИЕ ОТТЕНКОВ КИБЕРУСТОЙЧИВОСТИ

КАК ОБЕСПЕЧИВАЕТСЯ БЕЗОПАСНОСТЬ
ИНФРАСТРУКТУРЫ МОСКОВСКОЙ БИРЖИ

90 000

транзакций
в секунду способен
обращивать
каждый узел
торговых систем
Московской биржи

Московская биржа предоставляет полный цикл торговых и пост-трейдинговых операций на фондовом, валютном, срочном и товарном рынках, начиная с заключения сделок и заканчивая расчётами и депозитарными операциями. Все взаимодействия с клиентами — высокоскоростные электронные транзакции, массовая обработка которых возможна только при использовании современных высоких технологий и средств коммуникаций. Узлы торговых систем Московской биржи способны обрабатывать до 90 000 транзакций в секунду каждый, с задержкой менее 400 микросекунд, что ставит нас в ряд с крупнейшими биржами мира, а технологии расчета риска в реальном времени — не имеют аналогов.

Вместе с тем это очень высокая ответственность. В данном случае киберустойчивость —

это сервис, который мы должны предоставлять всем без исключения участникам торгов и Банку России, осуществляющему, в том числе, с помощью биржевых инструментов денежно-кредитную политику.

В масштабах Международной ассоциации бирж, куда Московская биржа входит на правах участника, фиксируется устойчивый интерес злоумышленников к торговым площадкам. Соответственно, для этих бирж и для нас киберустойчивость не просто важна, но носит схожие задачи с одинаковым профилем угроз.

«ПЛАН В» И ДАЛЕЕ...

Нам удалось воплотить мечту всех инфорбезопасников — мы создали отчасти закрытую систему. Все торговые системы биржи функционируют в рамках замкнутого контура. Для подключения участников торгов мы использу-

ем нашу частную сеть, которая практически не имеет стыков с внешними сетями. Для организации доступа используется семь операторов связи, что также позволяет не зависеть от перебоев в работе одного или нескольких из них. Есть услуги колокации, когда оператора связи просто нет, а участник торгов имеет прямую связь с системами биржи.

На пути возможного проникновения расположены порядка 80 серверов доступа, их функция в том числе в создании буферной зоны между ядром торговых систем и участниками торгов.

Сложность кроется и в двухуровневой структуре рынка. Есть профессиональные участники торгов, регулируемые Банком России, а есть их клиенты, и у всех могут быть разные инфраструктуры, часто менее защищенные, чем у лицензируемого участника.

Вместе с Банком России мы разрабатываем единый стандарт информационной безопасности, который могли бы применять профессиональные участники торгов и их клиенты. По мере завершения разработки нам предстоит еще и большая работа по его внедрению. Также нам должен помочь информационный обмен, который сейчас организован Банком России в рамках работы ФинЦЕРТ. Надеюсь, что удастся подключить к этому обмену и профессиональных участников торгов.

БОЛЬШИЕ ДАННЫЕ

В нашем торгово-клиринговом комплексе несколько десятков тысяч сетевых устройств и порядка нескольких тысяч серверов. Соответственно, помимо непосредственно торговых событий, число которых достигает до 60 млн транзакций в день, они производят достаточно большое количество и других событий.

В основе комплекса информационной безопасности биржи находятся аналитические системы, которые анализируют и выявляют аномалии в большом объеме данных. Мы обучаем системы знать разрешенный трафик, его стандартное поведение и диагностировать отклонения. Каждая обнаруженная аномалия подлежит исследованию.

В перспективе, с развитием технологий, нам хотелось бы сделать систему анализа событий и обнаружения аномалий проактивной: выявлять с её помощью не только атаки на инфраструктуру, но и нештатные ситуации. У нас нулевая толерантность к нештатным ситуациям, которые происходят по нашим ошибкам. Но, к сожалению, в рамках сверхсложной торговой системы не удастся их полностью избежать.

Что касается «плана В», то он подразумевает использование других сегментов в случае на-

ВМЕСТЕ С БАНКОМ РОССИИ МЫ РАЗРАБАТЫВАЕМ ЕДИНЫЙ СТАНДАРТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КОТОРЫЙ МОГЛИ БЫ ПРИМЕНЯТЬ ПРОФЕССИОНАЛЬНЫЕ УЧАСТНИКИ ТОРГОВ И ИХ КЛИЕНТЫ

ступления инцидента. Для этого мы одновременно поддерживаем несколько различных контуров, которые при необходимости можем оперативно перевести в «боевой режим». Сейчас их не менее десяти. При этом важно, чтобы альтернативные контуры имели другие версии систем, которые, мы считаем, не будут скомпрометированы в тот же момент, что и основная система. Поэтому многие действующие тестовые контуры биржи созданы с расчётом на возможную боевую нагрузку.

У нас есть «план С». Но не стоит полностью раскрывать информацию о том, какие у нас есть ещё планы. Важна задача взаимоотношений с вендорами. Мы используем мультивендорный подход и выстраиваем основные торговые системы на оборудовании разных поставщиков.

КУДА МЫ ДВИЖЕМСЯ?

Пять лет назад мы обсуждали возможность перехода на web-платформы и отказа от частной сети. Однако концепция частной сети по-прежнему остается актуальной. При этом, разрабатывая web-сервисы, мы планируем предоставлять их через наши частные сети. То есть в нормальной ситуации они смотрят наружу через Интернет. А в случае негативного развития событий эти сервисы мы можем спрятать внутрь наших частных сетей и продолжать оказывать участникам торгов полный спектр наших услуг.

* * *

Мы продолжаем инвестировать в усиление наших средств защиты. До трети бюджета IT уходит на вопросы, связанные с информационной безопасностью. Основным направлением для нас остается работа с участниками торгов и их клиентами, чтобы их меры безопасности соответствовали принятым на рынке стандартам с целью защиты общей инфраструктуры финансового рынка. С ростом числа инвесторов и российского рынка в целом актуальность этой задачи будет только увеличиваться.

МИРОВЫЕ ТРЕНДЫ ИБ НА СЛУЖБЕ ФИНТЕХА



Кирилл ЕРМАКОВ
технический директор
QIWI

Сотрудники QIWI создали Vulners — бесплатную поисковую систему по источникам информации, связанным с анализом защищенности компьютерных систем. Она позволяет быстро, эффективно и, главное, объективно выявить тренды и основные тенденции в сфере ИБ.

Как с годами меняется ситуация с хакерскими угрозами? Достаточно посмотреть на график роста угроз и уязвимостей за последние 20 лет, чтобы сделать прогноз на 2017 г. (рис. 1). На этом фоне очевидно, что отследить все тысячи существующих уязвимостей и выявить среди них реально важные — сложно. Что такое современные информационные системы? Это миллионы строк чужого кода, всевозможные библиотеки, разнообразное программное обеспечение, это десятки разновидностей аппаратно-программных комплексов, на каждом из которых стоит своя операционная система и программное обеспечение различных версий. Как в такой ситуации проследить за всеми уязвимостями, принимая во внимание многочисленные источники? Возникла идея создать поисковую систему, которая позволит отделить зерна от плевел и интегрировать в нее систему обмена информацией, какую использует любой CERT. Создатели БД Vulners решили изучить поисковые запросы и проанализировать поведение большой массы людей, интересующихся вопросами ИБ, чтобы выявить, что им реально важно, а что нет.

Vulners.com — это большая и непрерывно обновляемая база данных ИБ-контента, своеобразный технологический стартап, созданный

сотрудниками компании QIWI в свободное от основной работы время. Это приложение позволяет искать уязвимости, эксплойты, патчи, результаты bug bounty и многое другое так же, как обычный поисковик ищет сайты. Vulners изначально задумывался как внутренний инструмент для QIWI — база данных уязвимостей, которая бы позволила быстро отслеживать появление новых угроз.

Созданная поисковая система Vulners агрегирует и представляет в удобном виде основные типы данных:

- ◆ бюллетени безопасности вендоров, в которых указаны выявленные уязвимости в поставляемых ими продуктах;
- ◆ эксплойты из Exploit-DB, Metasploit и других крупных источников;
- ◆ nessus-плагины — компоненты сканера для обнаружения уязвимостей;
- ◆ сведения об исправленных ошибках в программах с сайтов bug bounty программ;
- ◆ публикации на тематических ресурсах.

Таким образом, создатели Vulners объединили 69 различных источников информации об уязвимостях и эксплоитах. База данных Vulners содержит более 600 тыс. бюллетеней безопасности и является одним из крупнейших в мире хранилищ подобной информации с обновлениями в режиме реального времени. Физический объем БД небольшой для хранилища, компактность достигается за счет дедупликации и упаковывания. Vulners написан на Python с применением собственной оболочки поверх популярного фреймворка Django, для поиска используется база данных Elasticsearch, данные хранятся в формализованном виде, связи между ними устанавливаются автоматически. Vulners защищается WAF Wallarm, работающем в блокирующем режиме.

Нужна ли такая база данных уязвимостей? Как показывает статистика, в день фиксируется порядка 6 тыс. обращений об уязвимостях и патчах к ним, половина трафика идет из запросов поисковой системы Google. Как работает поисковая система в ее классическом виде? Пользователь заходит в поисковик, что-то ищет, просматривает и тем самым меняет метрики искомого контента внутри хранилища. Поисковая система корректирует поисковую выдачу. Получается замкнутый цикл оценки релевантности информации.

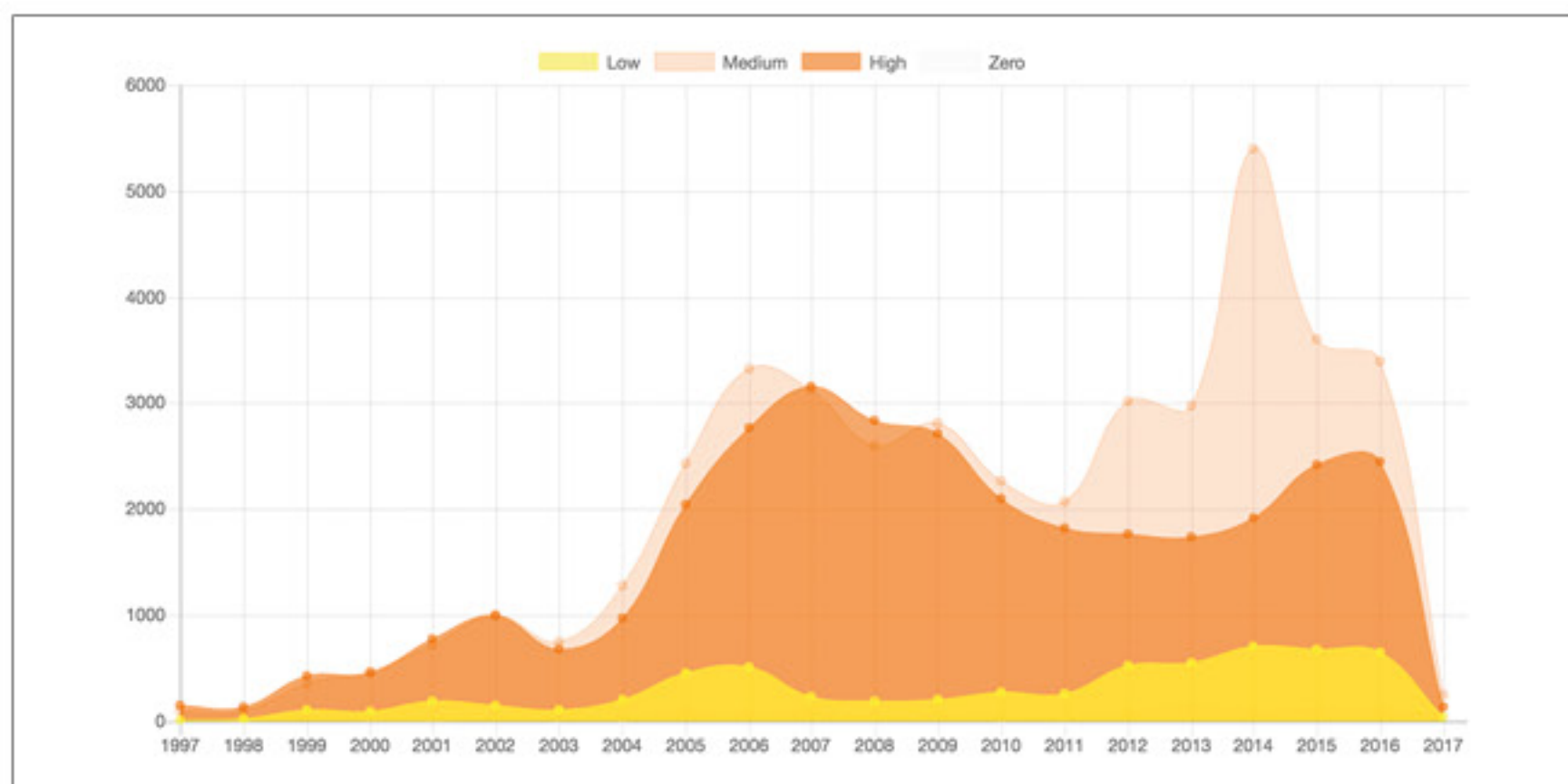


Рисунок 1. График роста угроз и уязвимостей за последние 20 лет

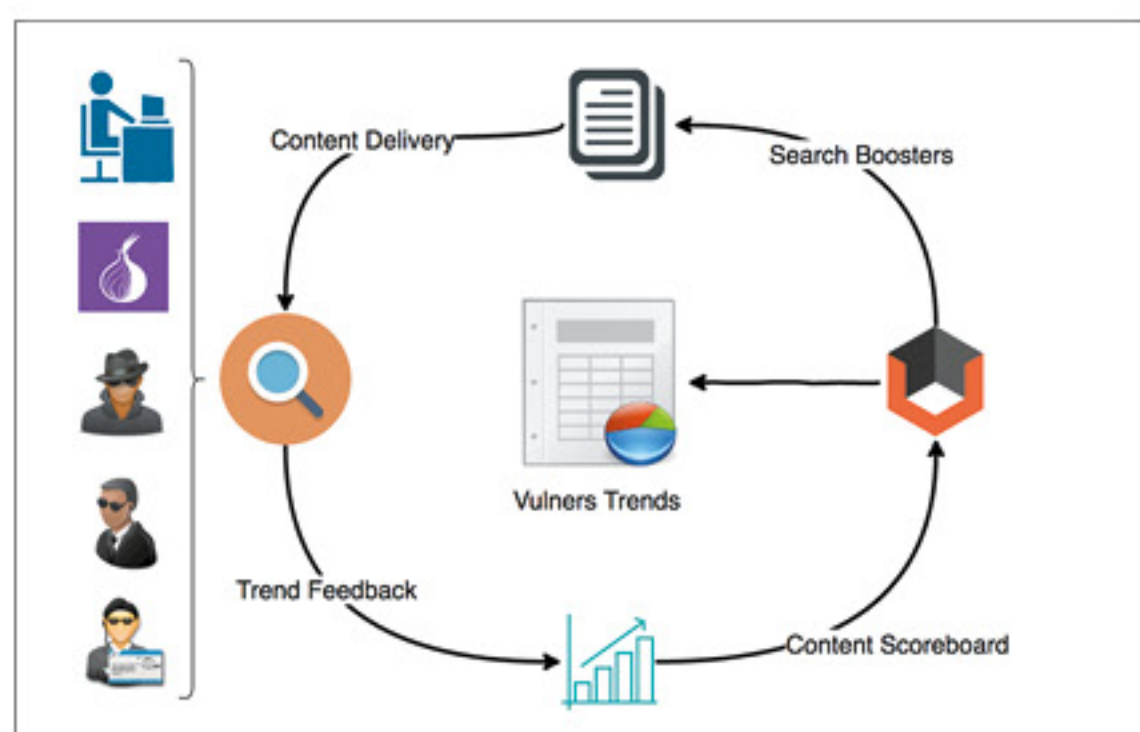


Рисунок 2. Система с замкнутым циклом

Создатели Vulners собирают математическую статистику на основе поисковых запросов, учитывают контент, переходы по ссылкам, просмотры... Все эти сведения, собранные и проанализированные в одном месте, формируют скоринг. Фактически, Vulners учитывает интерес пользователей своего сервиса, а также данные внешних ресурсов, например, TheHackerNews, которые ведут собственные рейтинги контента.

Кто пользуется базой данных уязвимостей? Все те, кому интересна и нужна информация об уязвимостях и эксплоитах. Около четверти всех запросов приходит из России, пятая часть — из США, еще 7% — из Индии. Все это видно на трендах. Построив систему замкнутой — аналогично Google, разработчики поисковика смогли увидеть, что на сегодня действительно интересно, а что — всего лишь информационный шум (рис. 2).

Предложенная разработчиками система анализа позволяет отслеживать действительно важные вещи. Всплеск популярности новости может быть кратковременным, однако если применить методы машинного обучения и анализа данных, то можно понять ее реальную ценность. Например, в октябре прошлого года вышел опасный эксплойт на уязвимость 2013 г. Своими силами отследить факт его появления можно, если тратить все время на чтение бюллетеней обновлений. Однако, используя методы математического анализа, можно определить, что вышло действительно важное обновление или пример использования уязвимости: его обнаружили и начали эксплуатировать множество пользователей.

На рис. 3 приведен пример специального интерфейса на Vulners. Разработчики системы получают трендовую аналитику за последние 7 дней. По ней видно то, что действительно важно и на что нужно обратить внимание, а что — малозначительные события (рис. 4). Итоговый отчет формируется в файл pdf.

Как отмечают специалисты в области ИБ, инструменты, подобные системе информирования и раннего оповещения Vulners, удобны в каче-

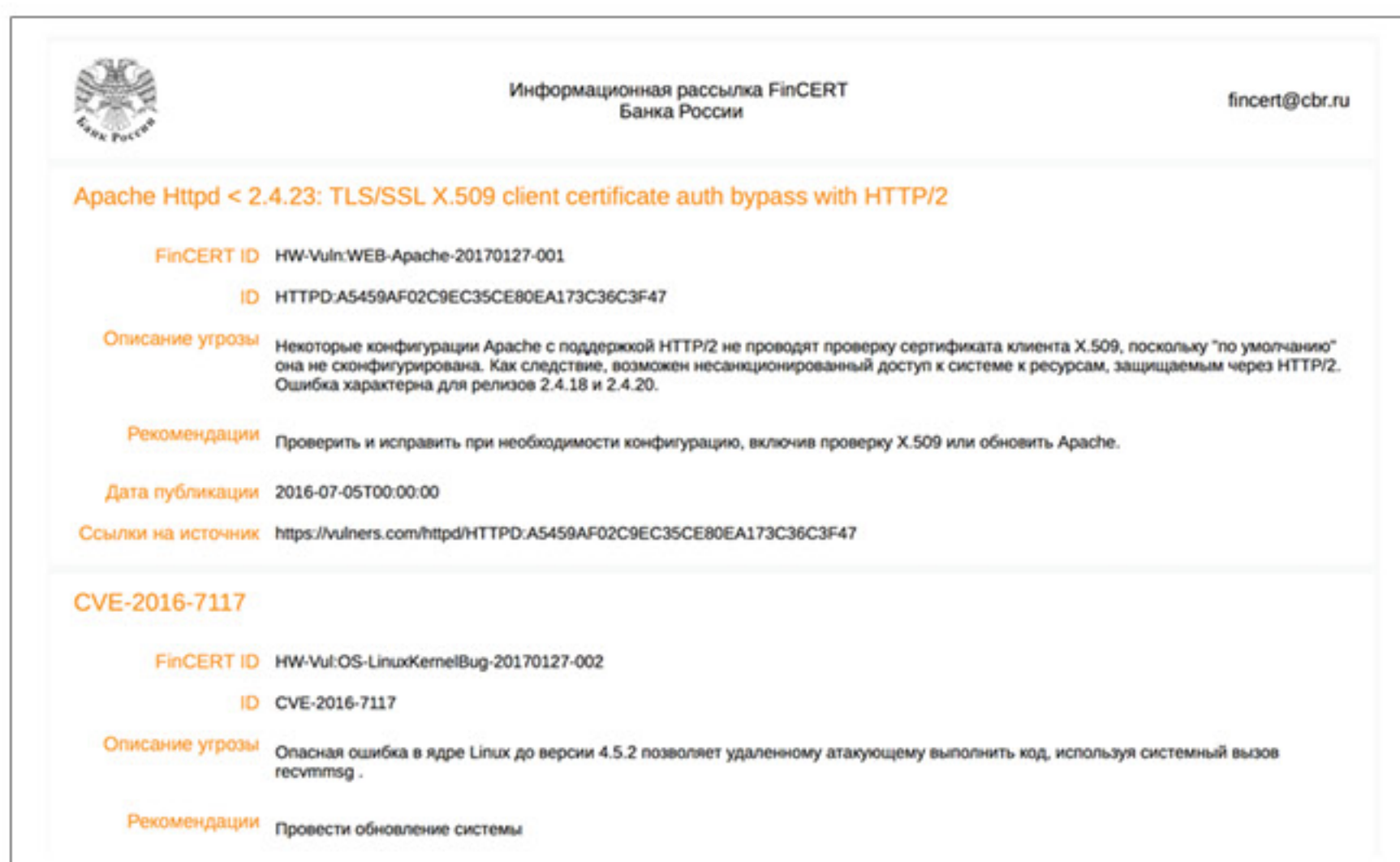


Рисунок 3. Специальный интерфейс на Vulners

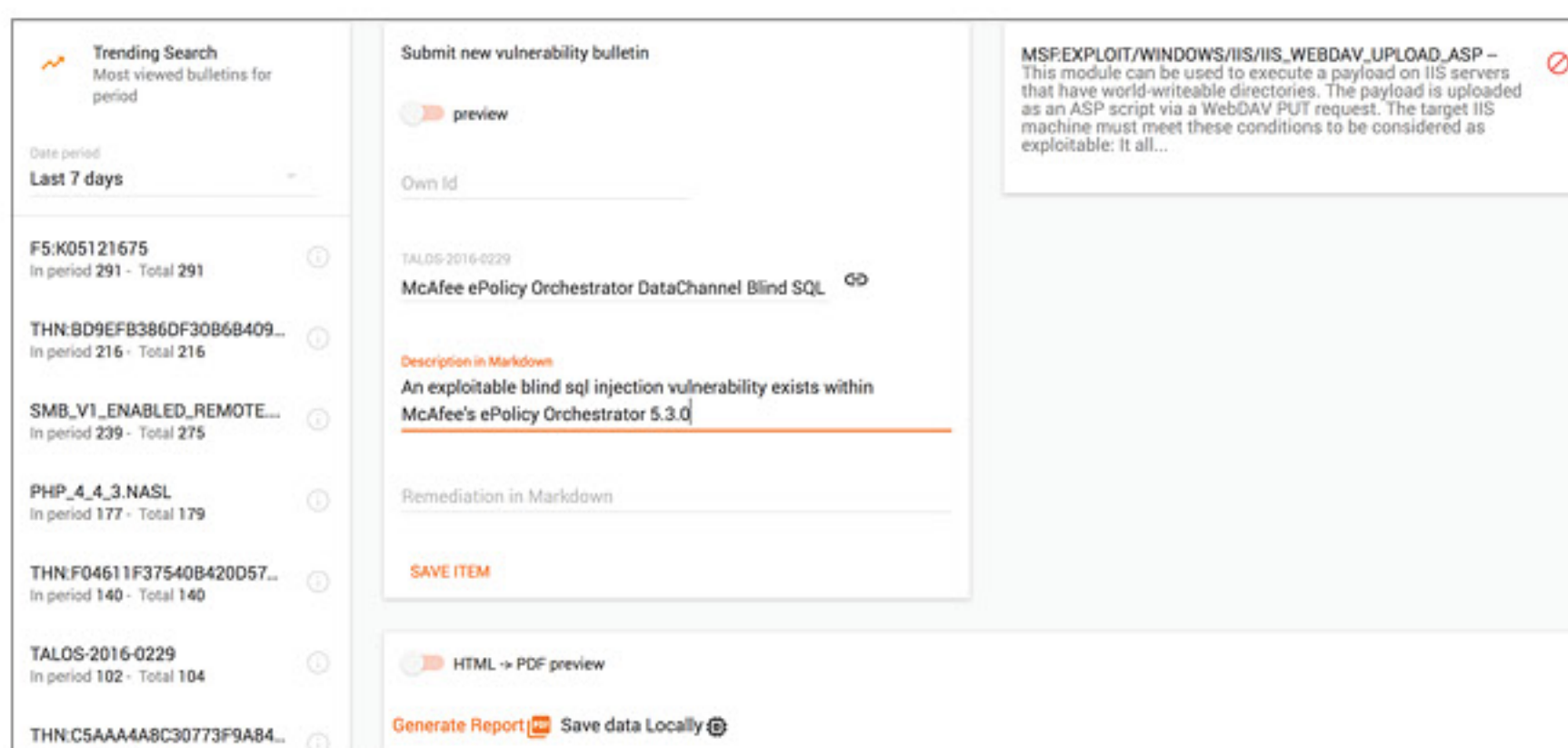


Рисунок 4. Взгляд изнутри. Слева — тот контент, который предлагается как трендовый. Справа — расшифровка уязвимости

стве бесплатного сервиса для финансовых организаций. Унифицированный контент и встроенные сервисы, которые предоставляет Vulners, намного удобнее многочисленных сканеров информационной безопасности, так как позволяет получать моментальную реакцию на обновления данных.

* * *

Несмотря на то, что проект молодой — недавно ему исполнился год — он уже привлек свою немаленькую аудиторию. Среди наших пользователей, например, такие гиганты как Adobe и Wargaming. Благодаря тому, что этот инструмент экономит время при исследовании и эксплуатации сложных векторов атак, он становится все более популярным у сотрудников отделов информационной безопасности всего мира, в т.ч. в России и США. Инструмент Vulners продолжает развиваться, и я, как один из создателей этого поисковика, утверждаю: база данных всегда будет открытой и бесплатной для пользователей.

КЛЮЧ ДЛЯ ДБО

ПРАКТИКА ЗАЩИТЫ ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ В СБЕРБАНКЕ



**Анатолий
МОРОЗОВ**
начальник отдела
сопровождения средств
защиты ЦОД и защиты
от DDOS Операционного
центра информационной
безопасности
ПАО «Сбербанк России»



**Александр
БОНДАРЕНКО**
главный инженер отдела
сопровождения средств
защиты ЦОД и защиты
от DDOS Операционного
центра информационной
безопасности
ПАО «Сбербанк России»

В ноябре 1982 г. Nottingham Building Society совместно с Банком Шотландии и британской телефонной компанией British Telecom внедрила систему Homelink. Теперь клиенты Ноттингемской строительной компании стали переводить деньги, не выходя из дома, — с помощью телефона и телевизора. Так появилось дистанционное банковское обслуживание.

С тех пор, благодаря распространению интернета, каналы ДБО перестали быть дополнительным сервисом для особо требовательных клиентов и превратились в популярную услугу.

ДБО ШАГАЕТ ПО СТРАНЕ

Эту тенденцию подтверждают различные исследования. По данным ЦБ РФ, в 2015 г. число банковских отделений на единицу населения в России сократилось на 15%. Удалённое обслуживание клиентов за пределами банковских офисов стало обычным делом. Ожидания пользователей растут.

Исследование аналитического агентства Marksw Webb Rank & Report, проведённое в конце 2015 года, показывает, что число потребителей банковских интернет-услуг в России составляет 35,3 млн человек — это 64,5% всех российских интернет-пользователей.

28 млн человек — 82% всех клиентов интернет-банкинга в России пользуется интернет-банком «Сбербанк Онлайн».

Мобильные банковские приложения для смартфонов и планшетов в России применяет 18,1 млн человек (33% всей российской интернет-аудитории). Как и в случае с интернет-банкингом, доминирующий по числу клиентов мобильный банк — мобильные приложения

Сбербанка: ими пользуется 14 млн человек (78% всей аудитории мобильного банкинга).

Почему же банковские сервисы дистанционного обслуживания Сбербанка так популярны?

БЕЗОПАСНОСТЬ — КОНКУРЕНТНОЕ ПРЕИМУЩЕСТВО

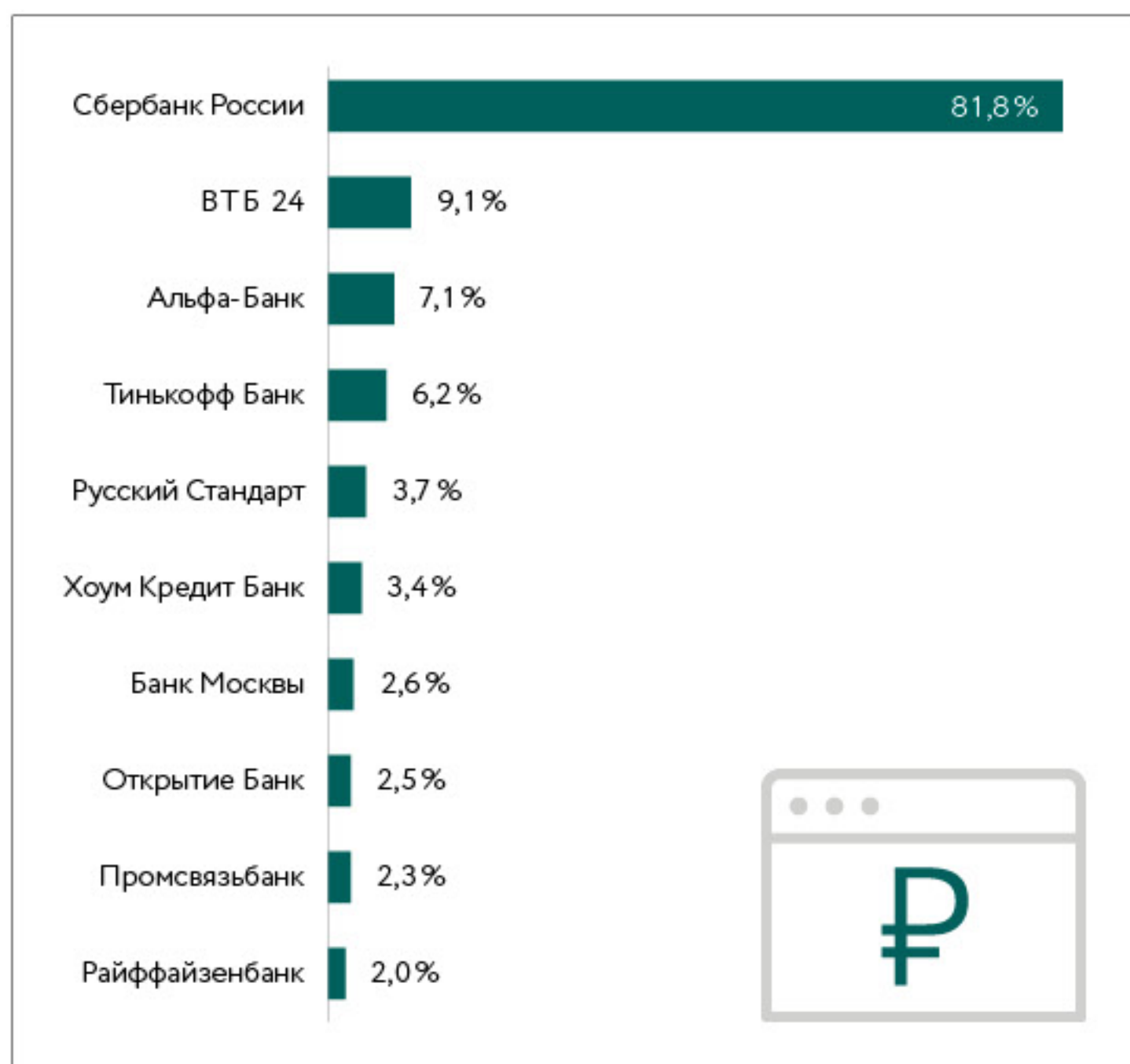
Вопрос защиты удалённых каналов обслуживания остаётся одним из самых острых в банковской отрасли. Статистика говорит об экспоненциальном росте мошенничества в системах ДБО. В 2015 году Банк России получил сведения о 32,5 тысячах попыток осуществления несанкционированных операций в системах ДБО на общую сумму 5,13 млрд руб.

Если обратиться к статистике Сбербанка, то с ноября 2015 года по август 2016 года доля предотвращённых попыток краж в системах ДБО выросла до 95%. Так, за прошлый год Сбербанк сохранил клиентам 8 млрд рублей. Это притом, что число пользователей за год выросло в два раза, а количество транзакций, проходящих через каналы дистанционного банковского обслуживания, — в 2,5 раза.

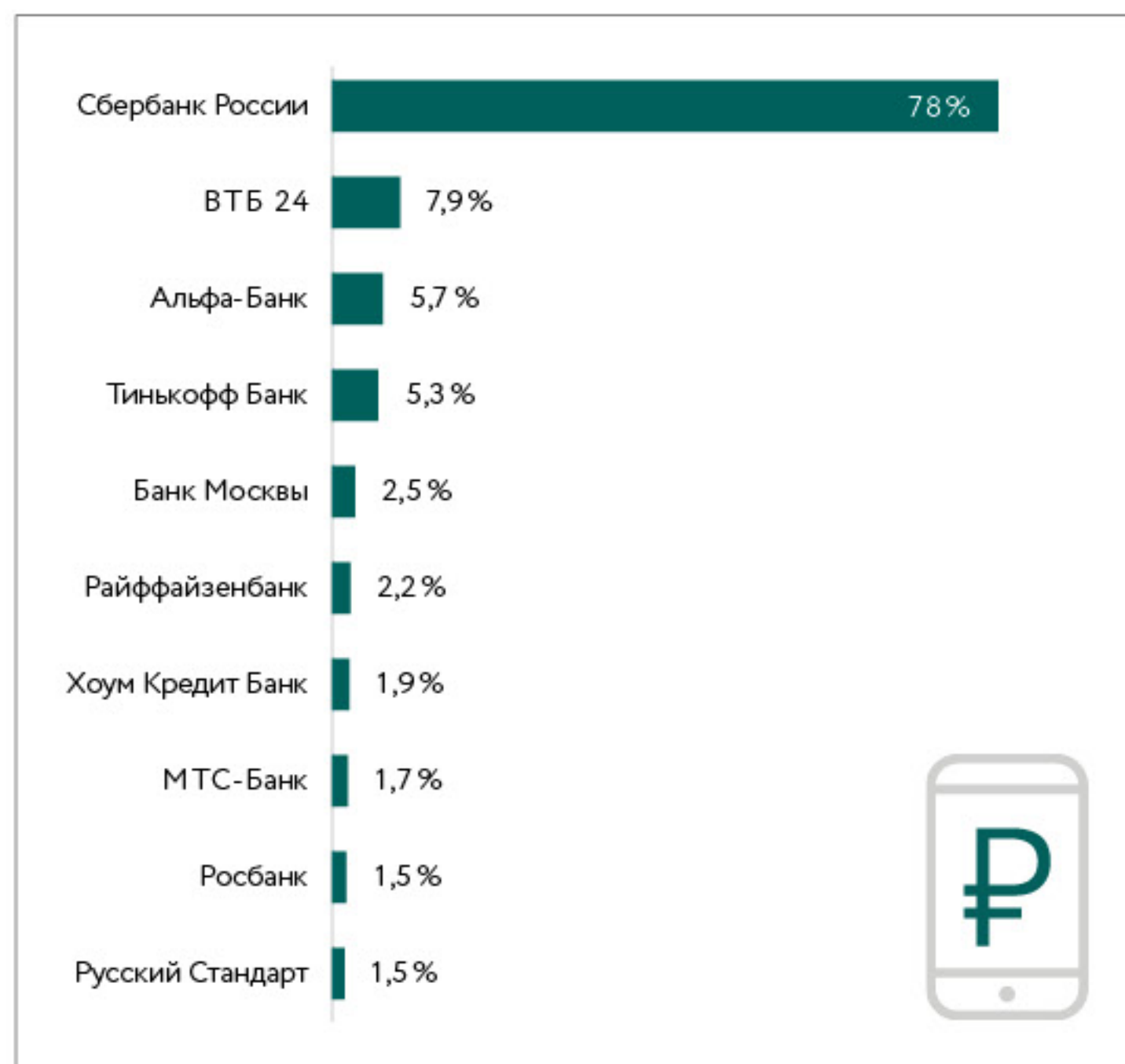
В условиях жёсткой конкуренции Сбербанк предлагает безопасность как одно из ключевых преимуществ: сервис не может быть удобным, если он не защищён и у клиента крадут деньги. Эффективное решение для обеспечения безопасности ДБО возможно только при условии создания системы, защищённой не только со стороны банка, но и со стороны клиента.

КОМПЛЕКСНАЯ ЗАЩИТА

Автоматизированная система «Сбербанк Бизнес Онлайн» — одна из самых популярных си-



Топ-10 интернет-банков по количеству пользователей (относительно всей аудитории интернет-банкинга)



Топ-10 мобильных банков по количеству пользователей (относительно всей аудитории мобильного банкинга)

стем ДБО в Сбербанке. Её используют порядка 1,4 млн юридических лиц. Каждую неделю к услуге подключается до 10 000 новых организаций. Система предназначена для дистанционного банковского обслуживания бизнеса — индивидуальных предпринимателей и юридических лиц. В «Сбербанк Бизнес Онлайн» можно через стандартный интернет-браузер создавать, подписывать, отправлять в банк платёжные документы, получать выписки по счетам, производить переписку с банком, отправлять зарплатные реестры и многое другое.

Аутентификация пользователей и обеспечения достоверности (аутентичности) документов в системе может происходить с помощью одноразовых СМС-паролей. При этом на телефон клиента высылается сообщение с деталями транзакции и одноразовым кодом для её подтверждения. Однако у специалистов по информационной безопасности Сбербанка есть причины считать этот метод подходящим только для единичных транзакций.

СМС могут перехватить мошенники. Они устанавливают «троян» не только на компьютер с интернет-банком, но и на телефон клиента (в основном это касается платформы Android). Юридическое лицо для такого метода мошенничества — лакомый кусок: можно украсть сразу большую сумму, а пропажу клиент заметит не сразу.

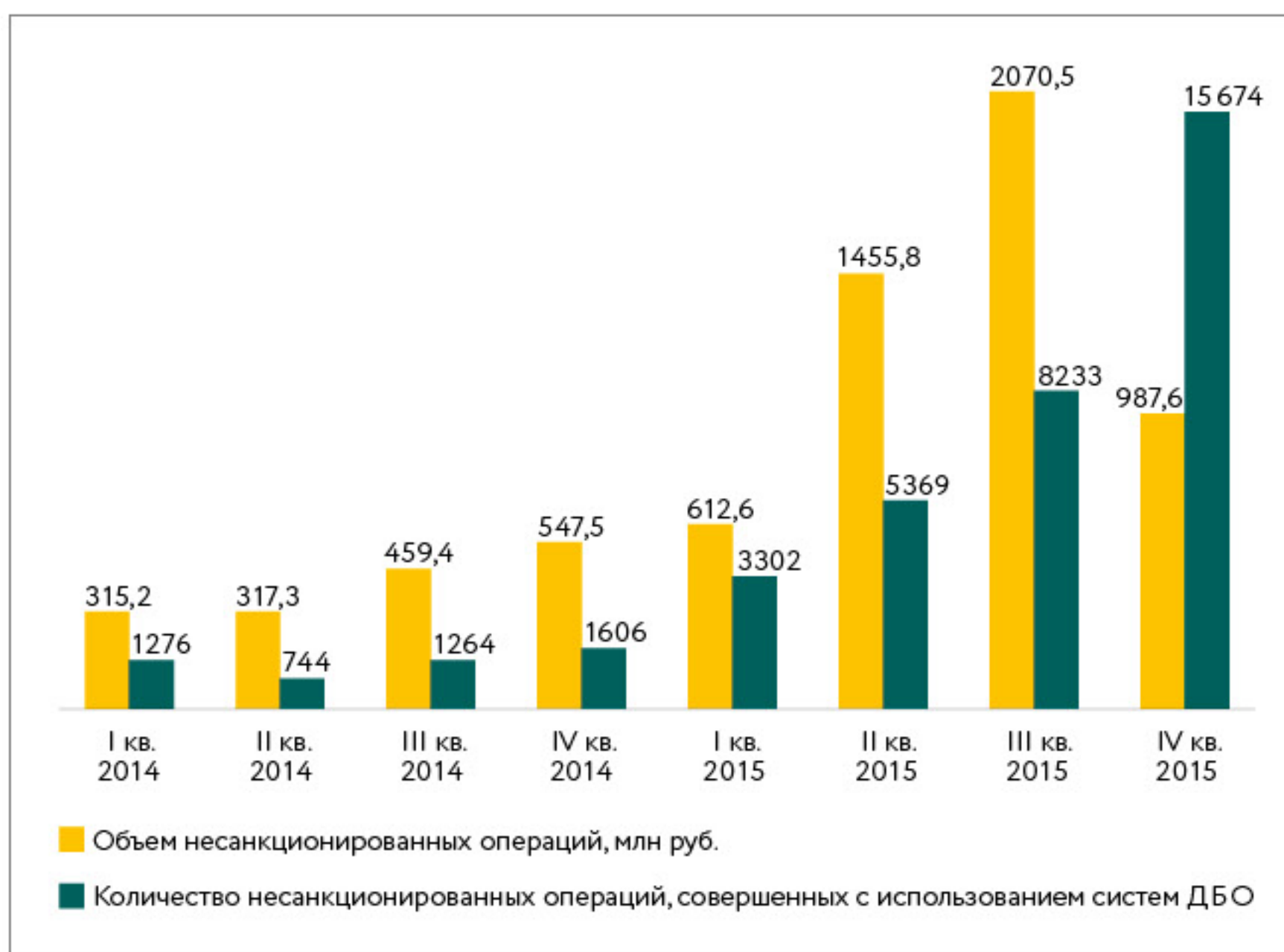
Известны случаи перевыпусков SIM-карт по поддельным паспортам. Проконтролировать принадлежность номера телефона клиенту, отследить замену SIM-карт, чтобы исключить си-

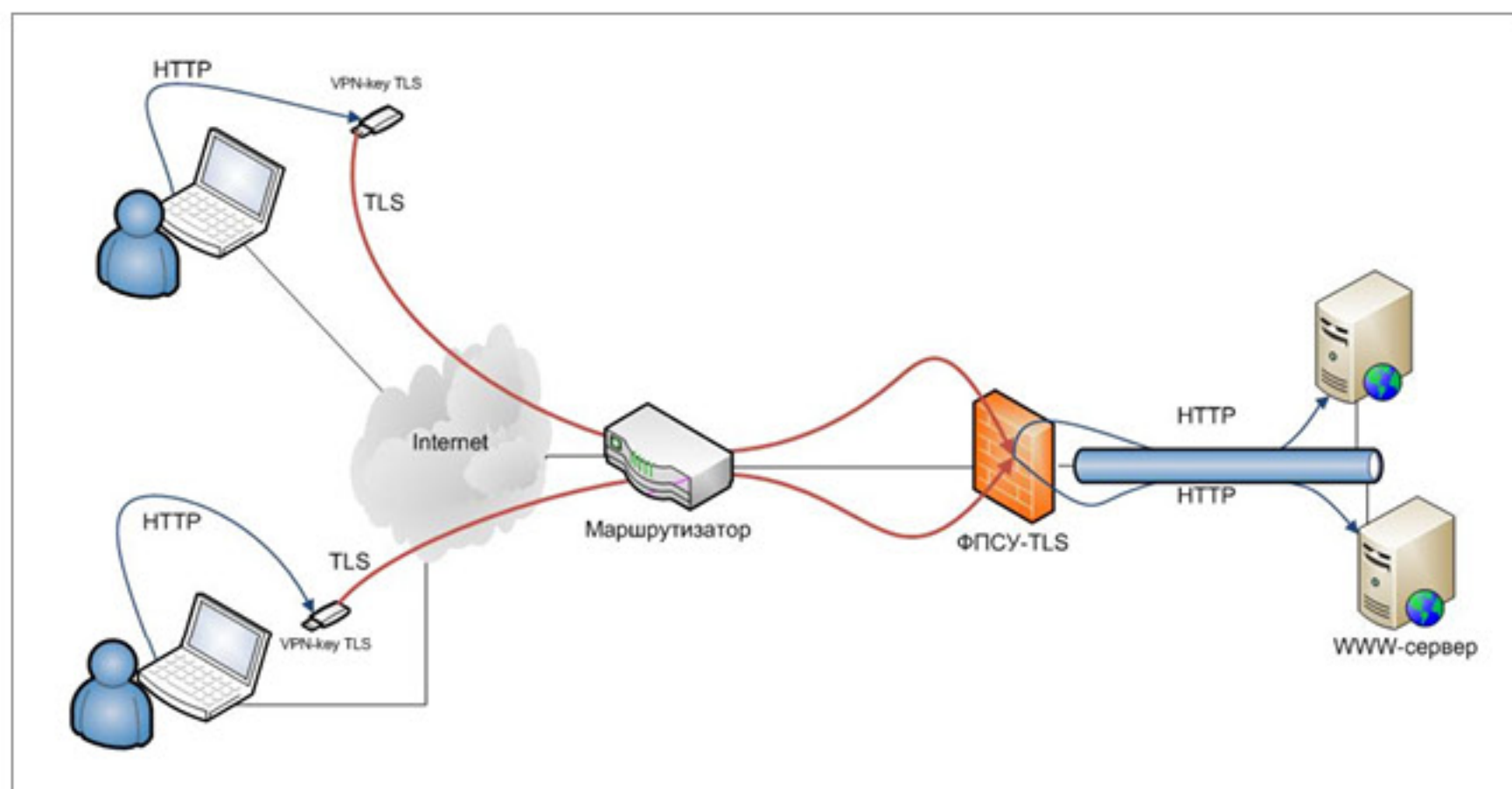
туации по отправке сообщений на телефон мошенника, можно не всегда.

И, наконец, рассылка СМС — это достаточно затратно для банков.

РЕКОМЕНДУЕТСЯ «ТОКЕН»

Постоянную работу с крупными денежными потоками Сбербанк рекомендует проводить с помощью «токена». Этот механизм защищает максимально и комплексно и пользователя, и банк. USB-ключ используется для аутентификации клиента в системе и создания защищённого TLS-соединения с банком в концепции «тонкого» клиента. Все криптографические





преобразования, включая квалифицированную электронно-цифровую подпись и шифрование передаваемых по открытым каналам данных, происходят непосредственно внутри «токена». Основная система устройства полностью совместима с инфраструктурой открытых ключей (Public Key Infrastructure).

ОСОБЕННОСТИ ЗАЩИТЫ НА СТОРОНЕ БАНКА

Механизм безопасного доступа к веб-сервису построен на базе кластера SSL/TLS концентраторов «ФПСУ-TLS». В соответствии с ГОСТом 28147-89 средства защиты аппаратно-программного комплекса «ФПСУ-TLS» используют протокол TLS 1.2 с алгоритмом шифрования. При взаимодействии клиента с оконечными прикладными WWW-серверами системы ДБО ПАО Сбербанк «ФПСУ-TLS» обеспечивает аутентификацию пользователя и защиту HTTP-трафика.

TLS-концентраторы снижают загрузку процессорных ресурсов прикладных WWW-серверов, повышают возможности масштабирования и отказоустойчивости системы.

Практика Сбербанка показывает, что лучший эффект резервирования достигается, когда аппаратные элементы кластера распределяются по разным площадкам, то есть оборудование подключается в разных ЦОДах. Для бесперебойной работы системы в случае поломок необходимо обеспечить достаточное количество блоков (зависит от трафика) на каждой площадке, а в точках подключения оборудовать два независимых источника электропитания — по количеству блоков питания у аппаратных платформ «ФПСУ-TLS». Отказоустойчивость и масштабируемость решения реализуются посредством VRRP и IPVS.

Комплексы «ФПСУ-TLS» надёжно защищают систему. Они могут выполнять функцию защищённого прокси-сервера. Для этого специа-

листы Сбербанка рекомендуют устанавливать их в сети компании непосредственно между внешним межсетевым экраном и пулом прикладных WWW-серверов. При этом на кластере «ФПСУ-TLS» необходимо включить опцию X-Forwarded-For (XFF). Так, в заголовке пакета фиксируется реальный IP-адрес внешнего клиента, и при наличии соответствующей функциональности в прикладной автоматизированной системе именно этот IP-адрес будет отражаться в подсистеме аудита. Такой подход сокращает процесс получения и анализа файлов регистрации действий клиентов — в логе автоматизированной системы сразу присутствует реальный (а не транслированный при прохождении по сети организации) адрес клиента.

Подсистема логирования «ФПСУ-TLS» фиксирует события различного уровня. Она передаёт эту информацию по протоколу Syslog на внешний сервер либо сохраняет журналы на диске. Опыт показывает, что даже при включении режима логирования абсолютно всех событий утилизация вычислительных ресурсов программно-аппаратного комплекса увеличивается незначительно. Для дальнейшего анализа событий специалисты Сбербанка рекомендуют использовать внешнюю SIEM-систему с тонкой настройкой правил корреляции. Это позволит фиксировать любую, даже незначительную аномальную активность и оперативно реагировать на инциденты.

В современных комплексах «ФПСУ-TLS» встроен модуль защиты от DDoS-атак. Однако опыт Сбербанка показывает, что для эффективного противодействия распределённым атакам необходимо строить эшелонированную систему защиты с применением специализированного оборудования и технологий. Специалисты Банка считают, что защищать системы ДБО от атак типа «отказ в обслуживании» только с помощью механизмов «ФПСУ-TLS» малоэффективно.

95%

доля предотвращённых попыток краж в системах ДБО Сбербанка с ноября 2015 года по август 2016 года

Простота и надёжная защита — ключевые особенности функционала продуктов линейки VPN-Key-TLS и программно-аппаратного комплекса «ФПСУ-TLS». Благодаря им Сбербанку удалось внедрить простой для клиента и надёжный с точки зрения безопасности способ защиты ДБО. Опыт Банка показывает, что в условиях жёсткой конкуренции безопасность ДБО становится основным преимуществом и её успех зависит двух факторов — лёгкости в использовании и гарантии абсолютной защиты.



Центр мониторинга и реагирования на инциденты ИБ (SOC)



Повышение уровня защиты

Привлечение специализированных ресурсов и инструментов ИБ обеспечивает повышение общего уровня ИБ вашей организации



Перераспределение рисков

Часть вашей ответственности за обеспечение ИБ ложится на АМТ-ГРУП как на провайдера сервиса и фиксируется в договоре на сервисное обслуживание



Высвобождение человеческих ресурсов

Вам не требуется нанимать дополнительный персонал; снижается нагрузка на штатных сотрудников



Отсутствие капитальных затрат

Вам не требуется проводить закупку технических средств, аппаратных платформ, ПО



Повышение эффективности

Вы получаете доступ к компетенциям и экспертизе наших специалистов, с которыми можно проконсультироваться по вопросам обеспечения ИБ



Готовые процессы

Вы получаете уже готовые процессы по обеспечению ИБ



Алексей САБАНОВ
заместитель
генерального
директора компании
«Аладдин Р.Д.»

ТАКАЯ РАЗНАЯ...

ИДЕНТИФИКАЦИЯ КЛИЕНТОВ
И ТРЕБОВАНИЯ К ЕЕ ОРГАНИЗАЦИИ
ДОЛЖНЫ СООТВЕТСТВОВАТЬ РИСКАМ

Применительно к банковским услугам существуют две похожие, но совершенно разные по своим целям задачи идентификации клиентов: знать своего клиента (KYC — know your client) и при доступе в приложения, как модно сейчас говорить, цифровизации банковского обслуживания, т.е. в различных видах дистанционного банковского обслуживания (ДБО).

Цель KYC — отличить клиента от остальных для проявления к нему внимания и повышения его лояльности. Риск ошибки в данном случае минимален. Например, при внедрении идентификации по голосу на поступивший в Call-центр звонок девушка, назвавшая Ивана Ивановича Петром Степановичем, согласно инструкции извинится, и разговор продолжится.

Другое дело — ДБО. Риски в данном случае на порядок выше. Речь идет об ошибке идентификации, означающей несанкционированный доступ к счету клиента, результатом которого может быть разбирательство, утрата доверия клиента и возможная его потеря. Целью идентификации в данном случае является не просто отличие клиента от других, а определение личности клиента с заданным уровнем достоверности для предоставления ему доступа к услугам банка. Для корректного управления доступом клиент должен пройти обязательную процедуру регистрации в конкретной информационной системе (ИС). Процесс идентификации клиента во время регистрации в ИС называется первичной идентификацией.

ПЕРВИЧНАЯ ИДЕНТИФИКАЦИЯ

Целью первичной идентификации является присвоение заявителю идентификатора доступа, обеспечивающего уникальность каждого субъекта доступа при каждой попытке авторизации в системе ДБО. При этом осуществляется получение от заявителя и регистрация идентификационной информации, достаточной для последующей идентификации претендента на доступ, а также обеспечение отсутствия коллизий между идентификационной информацией, представленной заявителем, и уже зарегистрированной идентификационной информацией, принадлежащей другим субъектам доступа. Полнота и строгость проверки идентификационной информации определяется политикой безопасности оператора ДБО и существенно влияет на качество управления доступом.

Первичная идентификация заявителя должна завершаться регистрацией (присвоением идентификатора доступа, уникального в конкретной информационной системе) или обоснованным отказом. Причиной отказа может являться недостаточный объем представленной информации или невозможность (нежелание) ее подтверждения заявителем. В итоге регистрации в системе ДБО появляется новая учетная запись, содержащая информацию о пользователе и секрет, с помощью которого пользователь будет подтверждать эту информацию и факт владения секретом в процессе аутентификации, который в обязательном порядке предшествует авторизации, то есть до-

ступу клиента к своим счетам. Идентификация клиента в последующих попытках доступа называется вторичной.

ВТОРИЧНАЯ ИДЕНТИФИКАЦИЯ

Целью вторичной идентификации является проверка соответствия (верификация) предъявленного претендентом идентификатора занесенному ранее в базу данных ИС. Процесс вторичной идентификации прост, как гвоздик: если предъявленный идентификатор совпал с зарегистрированным в системе, то вторичная идентификация считается успешно пройденной. Если речь идет о запросе на доступ к системе ДБО, то за идентификацией следует процесс аутентификации. По сути, аутентификация является идентификацией с подтверждением. Однако в силу сложности безопасной проверки подлинности предъявленного идентификатора и принадлежности идентификатора и секрета конкретному пользователю в условиях небезопасной среды, проводимой с помощью специально разработанных протоколов, системы аутентификации относят к классу одних из самых сложных интеллектуальных систем. Качество аутентификации существенно зависит от качества первичной идентификации, поскольку в отличие от идентификации целью аутентификации является доказательство того, что претендент на доступ является именно тем, за кого себя выдает. Стопроцентной уверенности в результатах аутентификации для систем с большим количеством пользователей в удаленном режиме достичь даже теоретически не-

возможно, поэтому международными стандартами введены уровни доверия.

УРОВНИ ДОВЕРИЯ К ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

В зависимости от используемого вида аутентификации устанавливается четыре уровня доверия к ее результатам. При использовании простой анонимной аутентификации нет никакой уверенности в том, что претендент на доступ является тем, за кого себя выдает («аноним»). Данная аутентификация обеспечивает первый (низкий) уровень доверия.

При использовании простой аутентификации (однофакторной аутентификации с организацией одностороннего обмена аутентификационной информацией) имеется некоторая доля уверенности в том, что претендент на доступ является тем, за кого себя выдает. Второй (средний) уровень доверия.

При использовании усиленной аутентификации (многофакторной или однофакторной OTP — аутентификации с организацией одностороннего обмена аутентификационной информацией) появляется высокая доля уверенности в том, что претендент на доступ является тем, за кого себя выдает. Третий (высокий) уровень доверия.

При использовании строгой аутентификации (многофакторной с организацией двухстороннего или многостороннего обмена информацией и применением криптографических протоколов аутентификации) уверенность в том, что претендент на доступ является тем, за кого себя выдает, является очень высокой. Такая аутентификация обеспечивает четвертый (очень высокий) уровень доверия.

Поясним генезис уровней доверия. Идентификация граждан проводится ежедневно с разной степенью тщательности. Например, при входе в театр достаточно предъявить билет. Или вы зашли в обменный пункт обменять 100 долларов на рубли. Достаточно протя-

нуть деньги, и вам их поменяют. Это — примеры анонимной идентификации. Естественно, доверие к такой идентификации граждан нулевое.

Для доступа в информационную систему надо предъявить персональный идентификатор — уникальную метку, которая должна отличать Вас от других пользователей данной системы. Существуют информационные системы, где вы можете иметь псевдоним, абсолютно не связанный с вашим ФИО и другими персональными данными, зарегистрированными в уполномоченных государственных органах. Примеров такого анонимного доступа достаточно во многих приложениях Интернета, так как эта технология изначально предназначена для использования безымянного (при желании) пользователя. Однако при появлении рисков нежелательного доступа к информации даже в приложениях Интернета требуется некий начальный уровень уверенности в том, что пользователь — именно тот, за кого себя выдает. На начальном уровне такой уверенности (уровне доверия) достаточно сетевого имени пользователя, отличающего его от других — например, адреса электронной почты. Для подтверждения подлинности информации даже на этом уровне доверия требуется ввод некоего секрета (пароля).

При увеличении рисков несанкционированного доступа к информации требования к идентификации пользователя и ее достоверности также растут. На третьем уровне доверия, кроме требования того, что пользователь зарегистрирован в ИС, для него согласован способ согласования одноразовых паролей (OTP) и, чаще всего, выдано определенное устройство генерации OTP.

При использовании строгой аутентификации уверенность в том, что претендент на доступ является тем, за кого себя выдает, является очень высокой. Применение строгой аутентификации рекомендуется международными стандартами и проектом национального

ГОСТ Р «Идентификация и аутентификация. Основные положения» для высокорисковых операций.

БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ В СИСТЕМАХ ДБО

Биометрическая идентификация клиентов может служить дополнительным (не основным) фактором идентификации и аутентификации в части доказательства принадлежности смарт-карты или токена, содержащих аутентификационную информацию, конкретному физическому лицу. Стандарт США FIPS PUB 201-2 рекомендует применять биометрию только для разблокирования смарт-карты, содержащей сертификат доступа и закрытый ключ. Служить основным средством идентификации ни одна биометрическая характеристика не способна по своей природе. Биометрическая идентификация граждан основана на методах математической статистики и характеризуется ошибками первого (FAR — False Accept Rate, злоумышленник идентифицирован вместо легального пользователя) и второго (FRR — False Reject Rate, отказ в идентификации легальному пользователю) рода. Согласно научным исследованиям из десятиmillionной выборки (аналог — население Москвы), по крайней мере 10 тысяч человек имеют схожие параметры при применении одного из самых точных механизмов — анализа радужной оболочки глаза. Другие методы дают значительно больше ошибок или стоимость их внедрения не вписывается в бюджет даже самых крупных банков.

* * *

Таким образом, идентификация клиентов и требования к ее организации в банках должна соответствовать рискам. Для операций с низким уровнем рисков применение идентификации с низким уровнем доверия, к которой относится и биометрия, возможно. При этом модели трансляции идентификации, обсуждаемые в последнее время, требуют внимательного рассмотрения с точки зрения неизбежных потерь доверия при передаче от одного кредитно-финансового учреждения другому.

**СЛУЖИТЬ ОСНОВНЫМ СРЕДСТВОМ
ИДЕНТИФИКАЦИИ НИ ОДНА
БИОМЕТРИЧЕСКАЯ ХАРАКТЕРИСТИКА
НЕ СПОСОБНА ПО СВОЕЙ ПРИРОДЕ**



Сергей
ВАХОНИН
директор по решениям
АО «Смарт Лайн Инк»

БАНК РОССИИ ПОДНИМАЕТ ТРЕБОВАНИЯ ПО БОРЬБЕ С УТЕЧКАМИ ИНФОРМАЦИИ НА УРОВЕНЬ ОТРАСЛЕВОГО СТАНДАРТА

ПРОГРАММНЫЙ КОМПЛЕКС DEVICESLOCK DLP ПОЗВОЛЯЕТ
РЕАЛИЗОВАТЬ ЦЕЛИ, ПОСТАВЛЕННЫЕ РС БР ИББС-2.9-2016

Защита информации в банковском бизнесе регулируется целым рядом нормативных актов и надзорных органов. Наиболее важными нормативами, регулирующими информационную безопасность в российской банковской отрасли, являются Стандарты Банка России группы «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». Весной 2016 года эти стандарты были существенно расширены новыми рекомендациями по предотвращению утечек информации.

Несмотря на то, что стандарты Банка России группы СТО БР ИББС носят рекомендательный характер, де-факто многими действующими в России банками они рассматриваются как обязательные. Некоторые финансовые организации уже реализовали соответствие требованиям Стандартов, другие — находятся в начале этого пути.

Весной 2016 г. Банк России выпустил новый ключевой документ, также имеющий рекомендательный характер — «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации» (РС БР ИББС-2.9-2016), где прямо указано, что организациям банковской системы РФ следует принимать меры по обеспечению конфиденциальности обрабатываемой информации. Наибольшими возможностями для нанесения ущерба, в том числе неумышленного, организации БС РФ и ее кли-

ентам в части возможного нарушения конфиденциальности обрабатываемой информации обладают работники организации БС РФ и (или) иные лица, обладающие легальным доступом к информации, — возможные внутренние нарушители информационной безопасности. При этом утечка информации является одной из наиболее актуальных угроз нарушения информационной безопасности, которую могут реализовать внутренние нарушители ИБ.

Собственно, утечкой информации Банк России именует несанкционированное предоставление или распространение информации конфиденциального характера, не контролируемое организацией. При этом подразумевается, что пользователь обладает правами доступа

к информации. Другой важный термин, именованный в документе — защита информации от утечки. Таковой признается деятельность, направленная на предотвращение неконтролируемого предоставления или распространения информации конфиденциального характера.

Среди рекомендаций, указанных Банком России, выделяются следующие:

- ♦ определение потенциальных каналов утечки информации конфиденциального характера;
- ♦ выполнение процессов системы обеспечения ИБ, которые обеспечивают непосредственный мониторинг и контроль информационных потоков, т.е. потенциальных каналов утечки информации конфиденциального характера (информационных потоков).

Организациям БС РФ рекомендуется рассматривать следующие значимые потенциальные каналы утечки информации:

- ♦ передача информации за пределы контролируемой информационной инфраструктуры с применением электронной почты;
- ♦ передача информации с применением сервисов сети Интернет, в том числе социальных сетей и форумов;
- ♦ размещение информации конфиденциального характера на объекте информационной инфраструктуры организации, не предназначенном для ее хранения;
- ♦ удаленный доступ к информационной инфраструктуре организации с использованием сети Интернет;
- ♦ копирование информации на переносные носители информации;
- ♦ печать и (или) копирование информации на бумажные носители;
- ♦ использование и (или) утеря переносных носителей информации;
- ♦ визуальное (включая фотографирование и видеосъемку) и слуховое ознакомление с информацией.

Особая ценность Рекомендаций заключается в том, что помимо перечисления категорий нарушителей и потенциальных каналов утечки информации Банк России приводит также Перечень угроз утечки информации конфиденциального характера, где в табличной форме увязывает потенциальные каналы утечки с категориями нарушителей, актуальные для различных типов объектов среды — от серверного оборудования до бумажных носителей информации.

Кроме того, в документе приводится широкий перечень действий, рекомендуемых для обеспечения необходимого и достаточного уровня предотвращения утечек информации. В частности, организациям рекомендуется обеспечить мониторинг и контроль использования различных сервисов и каналов электронных (сетевых) коммуникаций, канала печати, а также мониторинг, контроль, блокирование копирования информации на переносные носители информации.

Особо отмечается, что режим блокирования возможности использования потенциальных каналов утечки информации или режим их непрерывного мониторинга и контроля рекомендуется определять в зависимости от правил доступа для различных категорий потенциальных внутренних нарушителей. При этом применение режима блокирования возможности использования потенциальных каналов утечки информации не отменяет целесообразность проведения службой информационной безопасности организации БС РФ регулярного контроля, направленного на корректность реализации процессов мониторинга и контроля потенциальных каналов утечки информации.

Кроме того, Рекомендации указывают, что для большей эффективности в решении задачи предотвращения утечки информации рекомендуется реализация автоматизированного протоколирования и (или) блокирования передачи информации на основе контентного анализа передаваемой (переносимой) информации — в частности, при передаче информации на внешние адреса электронной почты, публикации в сети Интернет, вклю-

ЧТО ВАЖНО, КОНТЕНТНЫЙ АНАЛИЗ РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ ИМЕННО И НЕПОСРЕДСТВЕННО ДЛЯ РЕАЛИЗАЦИИ ПРОЦЕССОВ МОНИТОРИНГА, КОНТРОЛЯ, БЛОКИРОВАНИЯ ИСПОЛЬЗОВАНИЯ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ

чая социальные сети и форумы; при печати, сохранении на переносные носители информации и др. Что важно, контентный анализ рекомендуется использовать именно и непосредственно для реализации процессов мониторинга, контроля, блокирования использования каналов передачи информации — а не только для анализа архива электронных сообщений и файлов.

ВОЗМОЖНОСТИ DEVICELOCK DLP ПРИМЕНИТЕЛЬНО К РС БР ИББС-2.9—2016

Согласно ключевой парадигме Стандартов, наибольшие угрозы ИБ исходят от собственных сотрудников компаний. Программный комплекс DeviceLock DLP ориентирован на предотвращение утечек данных, связанных с нарушениями со стороны именно внутренних пользователей корпоративных ИС и потому является необходимым инструментом обеспечения информационной безопасности организаций, желающих успешно реализовать требования и пройти аудит соответствия Стандартам Банка России.

DeviceLock DLP контролирует перемещение (передачу) данных через локальные порты рабочей станции, съемные носители и каналы сетевых коммуникаций на основе гибких, персонализированных политик с использованием технологий контентной фильтрации. Каждый раз решение о том, чтобы разрешить или запретить доступ к устройству или сетевому протоколу, чтобы разрешить, запретить или сделать теневую копию передаваемо-

го файла или документа, принимается автоматически на основании контекстных параметров и, при необходимости, анализа содержимого перемещаемых данных.

Использование DeviceLock DLP позволяет обеспечить комплексный контроль действий пользователей непосредственно на их рабочих станциях, что в свою очередь существенно упрощает моделирование угроз и действий нарушителей. Например, если политика безопасности компании запрещает копирование информации на съемные устройства, использование DeviceLock DLP минимизирует риск утечки через данный канал в рамках общей модели угроз. Благодаря использованию DeviceLock DLP предотвращаются хищения информации внутренними нарушителями через порты рабочих станций, беспроводные сети, принтеры, мобильные устройства, а также электронную почту, мессенджеры, файлообменные сервисы и другие каналы сетевых коммуникаций. Кроме того, поддержка DeviceLock DLP событийного протоколирования и теневого копирования обеспечивает юридическую документированность и доказательность фактов попыток доступа и копирования конкретных данных.

* * *

Внедрение разработанного компанией Смарт Лайн Инк программного комплекса DeviceLock DLP помогает организациям БС РФ обеспечить соответствие их информационных систем отраслевым Стандартам СТО БР ИББС.

SIEM

В ФИНАНСОВОЙ СФЕРЕ

ИСПОЛЬЗУЕМ СТАРЫЕ СРЕДСТВА
ДЛЯ РЕШЕНИЯ НОВЫХ ПРОБЛЕМ



Андрей БИРЮКОВ
ведущий инженер
Департамента
информационной
безопасности АМТ-ГРУП

Обеспечение защитных мер в финансовых организациях, как правило, связано с серьезными расходами, на что в наше кризисное время готовы пойти далеко не все заказчики. Однако, иногда у заказчиков уже имеются все нужные средства, необходимо лишь их настроить. Поговорим об одном из таких средств.

SIEM И ДРУГИЕ СРЕДСТВА ЗАЩИТЫ

Системы обеспечения ИБ состоят из различных компонентов, обеспечивающих защиту информационных ресурсов как на сетевом, так и на прикладном уровнях, защищающих как от внутренних, так и от внешних угроз. При этом все эти сложные и дорогие средства могут работать гораздо более эффективно, если информация об обнаруженных ими инцидентах будет централизованно собираться и обрабатываться. Так, например, атаки на внутреннюю инфраструктуру банка можно своевременно обнаружить, если сопоставлять события от сетевых средств безопасности, сканеров уязвимостей и антивирусных систем. Также подозрительные действия в онлайн банкинге можно обнаруживать при помощи корреляции и анализа событий от платежных систем.

Для централизованного сбора и обработки событий ИБ используются решения класса SIEM (Security Information and Event Management). Данные комплексы осуществляют сбор, нормализацию (то есть разбиение по значащим полям), хранение и корреляцию информации о событиях. Наиболее

распространенными решениями класса SIEM на рынке являются HP ArcSight, IBM QRadar, MaxPatrol SIEM и другие. Данные продукты, как правило, представляют собой программные или программно-аппаратные комплексы, собирающие события со всех критичных элементов инфраструктуры и средств защиты. Совокупная стоимость их внедрения даже для средних организаций исчисляется десятками миллионов рублей, что делает проблематичным внедрение подобных систем «с нуля». Также здесь следует отметить, что существуют решения, предназначенные только для сбора и хранения событий и не осуществляющие их корреляцию. Обычно их используют для соответствия нормативным требованиям. Они не являются SIEM и в дальнейшем в статье не рассматриваются.

ХОРОШО ЗАБЫТОЕ СТАРОЕ

При этом во многих средних и крупных банках за прошедшие годы уже были внедрены различные средства защиты, и, как правило, среди них уже имеется решение класса SIEM. Эти продукты могут использоваться по-разному. В одних организациях SIEM используются лишь в качестве хранилищ событий ИБ, которые анализируют только постфактум, при расследовании инцидентов. В других SIEM уже не толь-

ко собирают, но и коррелируют события безопасности. Но, при этом ведется мониторинг исключительно со средств защиты и каталога Active Directory. Из приложений могут собираться только события неудачного входа-выхода. При этом никак не учитывается логика работы приложений. Например, если злоумышленник пытается подобрать пароль к онлайн банкингу, SIEM система это перехватит. А вот если хакеру уже удалось заразить машину бухгалтера трояном и он переводит в нерабочее время деньги на свои счета, такая активность не будет обнаружена SIEM.

И наконец, в организациях третьего типа SIEM используют «на всю катушку». Здесь собирают и анализируют не только события от средств защиты, но погружаются глубже в логику работы приложений, отслеживая подозрительные активности и мошеннические действия легальных пользователей в самих целевых системах. В приведенном выше случае, с зараженным трояном компьютером бухгалтера, правильно настроенная SIEM система получит сообщения о попытке перевода в то время, когда обычно платежи не проводятся, и на те счета, на которые ранее переводы не проводились, и на основании данной информации создаст инцидент.

Также с помощью гибкой настройки SIEM системы можно автоматизи-

**ПОДОЗРИТЕЛЬНЫЕ ДЕЙСТВИЯ
В ОНЛАЙН БАНКИНГЕ МОЖНО
ОБНАРУЖИВАТЬ ПРИ ПОМОЩИ
КОРРЕЛЯЦИИ И АНАЛИЗА СОБЫТИЙ
ОТ ПЛАТЕЖНЫХ СИСТЕМ**



ровать процесс блокировки подозрительных транзакций. Такая настройка требует кропотливой, непрерывной работы, однако она позволяет существенно повысить эффективность работы SIEM системы и службы ИБ в целом.

ПРИЧИНЫ И ПОСЛЕДСТВИЯ

Но вернемся к нашим трем типам организаций. Напомним, что организации первого типа лишь хранят собранные события, второго типа — анализируют только события со средств защиты, а третьи — коррелируют события как со средств защиты, так и с приложений. Очевидно, что первые две используют SIEM систему не полностью: у одних она лишь собирает и хранит события, у других коррелирует, но не все возможные. При этом во всех трех организациях может использоваться одно и то же решение SIEM. Только первые, например, когда-то внедрили SIEM, однако для того, чтобы его изучить и настроить корреляции, не нашлось времени. Ну а вторые внедрили, настроили базовые корреляции и им этого вполне достаточно. Либо, опять-таки, не хватает времени на дальнейшее развитие.

Еще одной причиной, по которой SIEM системы оказываются «забыты», является то, что с ними работают люди, не обладающие достаточной компетенцией. Например, система SIEM находится в ведении ИТ-отдела. Так как ИТ-специалисты не обладают достаточными знаниями о том, для чего нужна эта система, то они и не используют

ее как нужно. Аналогично и в случаях, когда система обслуживается специалистами ИБ, не прошедшими необходимого обучения и не знакомыми с возможностями системы.

Так или иначе, во многих организациях развернуты дорогостоящие средства SIEM, используемые не на полную мощность.

НОВЫЕ ВЫЗОВЫ

Однако жизнь не стоит на месте, появляются новые угрозы, внедряются новые банковские системы, выходят новые нормативные акты, и все это требует реакции от ИБ-специалистов. В банковской сфере проблемы информационной безопасности стоят острее, чем в других отраслях, ведь здесь злоумышленники посягают непосредственно на деньги. С активным развитием платежных систем и онлайн банкинга возросли и требования к их защите и, прежде всего, к борьбе с мошенничествами — антифроду. При проведении банковской транзакции самое главное — удостовериться в том, что она является легитимной, то есть, что ее не осуществляет злоумышленник.

Для обнаружения банковского фрода (мошенничества) существуют специализированные решения, однако они обладают рядом существенных недостатков: они преимущественно иностранные и стоят существенно дороже, кроме того, они не учитывают российскую специфику, что приводит к большому количеству ложных срабатываний,

ЭКСПЕРТ, ПРОРАБОТАВШИЙ МНОГО ЛЕТ В БАНКОВСКОЙ СФЕРЕ, ЗНАЕТ ДЕСЯТКИ, ЕСЛИ НЕ СОТНИ РАЗЛИЧНЫХ СПОСОБОВ ФРОДА И ИХ ПРИЗНАКИ

и, наконец, они работают по принципу «черного ящика», то есть в них мало что можно настроить без обращения за помощью к производителю решения.

Однако для обнаружения фактов фрода можно использовать SIEM. В этом случае необходимо передавать в данную систему информацию о событиях с признаками транзакций (время, банковские реквизиты, IP-адреса и т.д.). Далее данные события сопоставляются с другими, проверяются на соответствие определенным признакам (черные, белые списки, пороговые значения и т.д.), и на основании этой информации подается сигнал о подозрительной транзакции.

При этом у аналитиков ИБ, занимающихся антифродом, всегда есть возможность составить свои правила корреляции, ведь эксперт, проработавший много лет в банковской сфере, знает десятки, если не сотни различных способов фрода и их признаки.

* * *

Таким образом, в наше непростое время совершенно необязательно тратить деньги на покупку новых решений, вместо этого можно постараться получить максимум возможностей от уже имеющихся. Понятно, что более тонкая настройка и модернизация SIEM требуют высокой квалификации от выполняющих ее специалистов, и здесь лучше всего обратиться к профессионалам. Однако, экономический эффект, получаемый от модернизации SIEM, позволит достаточно быстро окупить все затраты и существенно повысить уровень защищенности ресурсов.

СТАРАЯ СКАЗКА НА НОВЫЙ ЛАД



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



ДА С ПРИСКАЗКАМИ ОТ «С-ТЕРРА»

Жили-были три поросенка. Три брата. Звали их, как вы уже догадались, Ниф-Ниф, Нуф-Нуф и Наф-Наф. Это были продвинутые, современные поросята. Жили они в хороших, крепких домиках, с компьютерами и Интернетом. У каждого была построена целая информационная система, объединяющая их с друзьями.

Весь год занимались они разными важными и необходимыми, как они считали, делами и не задумывались о безопасности своих сетей. Зачем? Ведь вокруг только друзья! Совсем забыли они про злого волка (который мог и данные украсть и их самих съесть) и про строгого медведя (который следил за порядком в лесу и за соблюдением законов).

И вот наступила осень, подул холодный ветер... Да-да, вот такие совпадения. Именно осенью пришли сообще-

ния, что совсем скоро нужно проводить аттестацию систем и для этого приедет с проверкой суровый Топтыгин, а также, что коварный волк поживился информацией в соседнем лесу.

Собрались братья на совет.

— Пора нам подумать об информационной безопасности, — сказал Наф-Наф своим братьям. — Я весь дрожу от страха перед грядущей аттестацией. Давайте построим себе системы защиты и будем спать спокойно.

Но его братья не хотели браться за работу.

— Успеется! Волку наши данные не нужны, а до проверки еще далеко. Мы еще тестированием виртуализации занимаемся, — сказал Ниф-Ниф и приказал виртуалкам мигрировать в резервный ЦОД.

— Когда нужно будет, я сам построю себе систему защиты, — сказал Нуф-Нуф, открыл ленту новостей в фейсбу-

ке и отлайкал там посты популярного блогера.

— Я тоже, — добавил Ниф-Ниф и вернул виртуалки обратно.

— Ну, как хотите. Тогда я буду один строить себе систему защиты, — сказал Наф-Наф.

Ниф-Ниф и Нуф-Нуф не торопились. Они только и делали, что читали новости и занимались «текучкой».

— Сегодня мы доделаем все «срочные» задачки, — говорили они, — а завтра с утра возьмемся за дело. Но и на следующий день они говорили то же самое. И только когда до приезда медведя остался месяц, ленивые братья взялись, наконец, за работу.

Ниф-Ниф решил, что проще и быстрее всего купить какое-нибудь одно средство защиты. Ни с кем не посоветовавшись, он так и сделал — приобрел антивирус. Очень довольный своей «системой», он направился к Нуф-Нуфу.

Нуф-Нуф тоже очень своеобразно озабочился безопасностью своей инфраструктуры. Он старался скорее покончить с этим скучным и неинтересным делом. Сначала, также как и брат, он хотел просто купить себе антивирус. Но потом вспомнил, что необходим комплексный подход, и добавил в корзину интернет-магазина межсетевой экран с VPN-шлюзом. Пока Нуф-Нуф восхищался своей абсолютной защищенностью, к нему пришел Ниф-Ниф, и они пошли посмотреть — как обстоят дела у Наф-Нафа.

Наф-Наф уже давно был занят постройкой системы безопасности. Он провел обследование, составил модель угроз и техническое задание и теперь не спеша строил себе надежную, современную систему защиты, которая может оградить и от атак злоумышленника, и от штрафов проверяющего. Он обеспечил двухфакторную аутентификацию пользователей, разделил информационную систему на сегменты, реализовал удаленный доступ через внешние сети, не забыв и про регистрацию событий безопасности и реагирование на них. Теперь волк не сможет нарушить конфиденциальность и целостность передаваемой информации. Ниф-Ниф и Нуф-Нуф застали брата за работой.

— Что ты делаешь? — в один голос закричали удивленные Ниф-Ниф и Нуф-Нуф.

А Наф-Наф, как ни в чем не бывало, продолжал настраивать централизованный мониторинг через SIEM систему. Они хотели подразнить Наф-Нафа, но тот даже не обернулся.

— Пойдем, Нуф-Нуф, — сказал тогда Ниф-Ниф. — Нам тут нечего делать!

И два храбрых, но беспечных брата пошли на очередную конференцию.

На ней они так громко рассказывали, как сэкономили на системе защиты время и деньги, что привлекли внимание волка, который оказался среди слушателей и был не прочь поживиться их информацией.

Ниф-Ниф стал первой жертвой. Пока поросенок работал через удаленный доступ, волк перехватил незащищенный трафик, и данные потекли в его лапы. Ниф-Ниф заметил это и помчался за советом к Нуф-Нуфу.

Едва успели братья обсудить необходимость защиты сетевого трафика, как волк добрался и до Нуф-Нуфа. Но его трафик был защищен VPN-шлюзом, совмещенным с межсетевым экраном, и волк не смог нарушить конфиденциальность информации. А вот для обеспечения целостности использовался алгоритм sha-1 (как недавно выяснилось — не самый надежный). Тут волк пошел на хитрость — изменил передаваемый поросенком трафик, и атака успешно прошла!

Ниф-Ниф и Нуф-Нуф побежали к Наф-Нафу. Они были так напуганы, что ничего не могли сказать. Наф-Наф сразу догадался, что на системы братьев напали. Но ему нечего было бояться со своей суперзащитой. После проверки работоспособности всех компонентов своей системы, он был уверен, что всё в безопасности.

Волк перехватывал и пытался расшифровать трафик, искал уязвимости алгоритма — все напрасно, система выдержала.

Голодному до чужой информации волку ничего не оставалось делать, как убираться восвояси.

И он решил попробовать обойти систему защиты физически — решил украсть устройство, на котором удаленно работал Наф-Наф. Как волк это сделал — до сих пор остается для всех загадкой, но у него в лапах оказался вожделенный тонкий клиент. Но, к огромному его разочарованию, данных на нем не было, так как Наф-Наф использовал специальный загрузочный носитель с встроенным VPN-клиентом, который всегда носил с собой.

Собрав информацию обо всех трех атаках, братья передали её сотрудникам полиции. Волка нашли и арестовали, а поросята глядели ему вслед и радовались, что они так ловко проучили злого разбойника.

Система Наф-Нафа не только стойко выдержала атаку волка, но и успешно прошла аттестацию. А Ниф-Ниф и Нуф-Нуф сделали себе полноценные системы защиты по примеру брата.



ПРИСКАЗКА 1

В системе Наф-Нафа для защиты удаленного доступа использовались продукты С-Терра:

- ♦ Многократно проверенный стандартный протокол IPsec — волк не нашел уязвимостей,
- ♦ Криптоалгоритмы ГОСТ — волк не нарушил ни конфиденциальность, ни целостность,
- ♦ Сертификаты регуляторов — пригодились при аттестации.

ПРИСКАЗКА 2

У Наф-Нафа был не просто VPN-клиент, а специальный загрузочный носитель — С-Терра Пост, работающий по технологии среды построения доверенного сеанса.

- ♦ Дополнительная аутентификация — носитель используется как токен,
- ♦ Изолированная среда — система рабочего места изолирована от системы для удаленного подключения,
- ♦ Нет данных на устройстве пользователя — все хранится на сервере.



КОМПАС ДЛЯ БЕЗОПАСНИКА

ДНЕВНИК IX УРАЛЬСКОГО ФОРУМА

13–17 февраля 2017 года в ДЦ «Юбилейный» (Республика Башкортостан) Медиа Группа «Авангард» при официальной поддержке Банка России и Ассоциации российских банков провела ключевое мероприятие отрасли информационной безопасности финансовой сферы — IX Уральский форум.

«Уральский форум является ведущей площадкой по обмену опытом в сфере обеспечения информационной безопасности финансовых организаций»

Эльвира Набиуллина, Председатель Центрального банка Российской Федерации

14 ФЕВРАЛЯ

Открывая Форум, Георгий Лунтовский, первый заместитель председателя Банка России, отметил беспрецедентный рост масштабов главного события отрасли информационной безопасности и сообщил, что благодаря ФинЦЕРТ объем несанкционированных операций со счетов сократился вдвое — с 3,8 млрд руб. в 2015 г. до 1,9 млрд руб. в 2016 г. Сумма мошеннических операций по платежным карточкам составила 1,08 млрд.

При этом удельный вес несанкционированных переводов с платежных карт в России не превышает 0,002%, в то время как по стандартам в международных платежных системах доля несанкционированных транзакций может достигать 0,009%. Поставлена цель — удерживать этот показатель в пределах 0,005%.

Кроме того, он сообщил, что Банк России в 2016 г. выявил девять попыток хищения средств с корсчетов банков на общую сумму 2,18 млрд руб., из которых 1,5 млрд руб. были не санкционированно переведены. «Тем не менее прогноз, который делался на декабрь, о массированных атаках на нашу финансовую кредитную сферу с целью дискредитации не оправдался, и те атаки, которые были, мы успешно отразили. Но в целом проблема остается», — подчеркнул он. Также Георгий Иванович подробно рассказал о направлениях и специфике работы Банка России в 2017 г. В частности, в 4 квартале 2017 г. планируется внедрение национального стандарта (ГОСТ Р) по защите информации финансовых ор-



Георгий Лунтовский, первый заместитель председателя Банка России

ганизаций, в котором будет определен базовый набор организационных и технических мер защиты. В документах Банка России предполагается давать ссылки на этот стандарт и, таким образом, сделать обязательным соблюдение его положений, включая требования по защите информации на этапах жизненного цикла автоматизированных систем и приложений.

Стоит отметить, что первый деловой день Форума оказался богатым на инициативы и предложения.

Первую инициативу выдвинул Гарегин Тосунян, президент Ассоциации российских банков.

Он рассказал, что Комитет АРБ по банковской безопасности проанализировал все действующие законы, ука-

зы, стратегии, постановления и другие нормативно-правовые документы, в которых прописана «правовая ответственность» подразделений информационной безопасности банков. Выяснилось, что таких документов около 130. Из них:

- ♦ федеральных законов — порядка 50;
- ♦ указов Президента и постановлений Правительства — более 20;
- ♦ актов федеральных органов исполнительной власти — около 15;
- ♦ нормативных документов Банка России — порядка 25;
- ♦ стандартов и нормативных документов по международным и российским платежным системам, а также по системе СВИФТ — более 20.

Президент АРБ уверен, что назрела необходимость в упорядочении этих документов и в создании единого отраслевого документа. В связи с этим он предложил создать Стратегию развития информационной безопасности организаций кредитно-финансовой сферы, которая объединит все вышеназванные документы.

Другая инициатива, выдвинутая банковским сообществом, касается отсут-



450 специалистов
из 20 городов
России



Гарегин Тосунян, президент Ассоциации российских банков



Алексей Новиков, сотрудник ФСБ России

Роман Шередин,
заместитель руководителя Россвязи

ствия механизма срочной блокировки мошеннических сайтов с иностранными доменами. Мошеннические сайты используются в основном для сбора персональных данных и кражи денег с банковских карт. Участники форума согласились с актуальностью проблемы и тем, что необходимо в срочном порядке создать Межведомственную рабочую группу, в состав которой, кроме специалистов банковского сообщества и сферы информационной безопасности, должны войти представители силовых ведомств, Минкомсвязи, Роскомнадзор, а также все заинтересованные организации.

Целый ряд инициатив выдвинул Роман Шередин, заместитель руководителя Россвязи. Он подчеркнул, что участие Россвязи в IX Уральском форуме обусловлено в первую очередь тем, что задача обеспечения информационной безопасности — это комплексная задача, решение которой неразрывно связано с обеспечением целостности, устойчивости и безопасности Единой сети электросвязи Российской Федерации. И озвучил предложения по противодействию

угрозам для финансовой сферы. Наряду с оригинальными методами противодействия фроду и идентификации клиентов, участники Форума оценили инициативу в сфере высшего образования — предложение использовать 4 вуза Россвязи (в состав которых входят 8 филиалов и 4 колледжа) как площадку для реализации образовательных программ на стыке сфер связи, безопасности и финансов.

Начальник управления Роскомнадзора Юрий Контемиров в свою очередь представил своеобразный результат деятельности Уральского форума — Стратегию информационно-публичной деятельности до 2020 года. Дело в том, что на предыдущих форумах тема информационно-просветительской деятельности среди населения поднималась постоянно. Теперь, применительно к персональным данным, она оформлена в четкую программу действий, которая уже воплощается на практике. По крайней мере, по словам выступающего, уже сегодня можно окунуться в увлекательный мир портала «Персональные данные. Дети».

Всеобщий интерес вызвал доклад начальника управления ФСТЭК Дмитрия Шевцова, рассказавшего о новых требованиях к средствам защиты информации, которые будут приняты в 2017 году. В частности о ТБИ к системам управления базами данных, к средствам управления потоками информации, к средствам виртуализации, к межсетевым экранам и др.

Сотрудник ФСБ Алексей Новиков рассказал о перспективах развития Национального координационного центра по компьютерным инцидентам, подчеркнув, что скоро аббревиатуру НКЦКИ будет знать весь мир. Задачи НКЦКИ простые, но принципиально важные: помощь в реагировании, пресечение вредоносной активности, уведомление об угрозах, методическая помощь в создании центров ГосСОПКА.

Артем Сычев, заместитель начальника ГУБиЗИ Банка России, рассказал, что все DDoS-атаки, которые были проведены в конце прошлого года и в начале этого, не принесли никаких су-



Артём Сычёв, заместитель начальника ГУ БиЗ И Банка России

ществленных осложнений ни одной из кредитных организаций.

«Да, действительно, они были, да, действительно, доставляют какие-то неприятности, но они не носили критический характер и не нарушили ни одного сервиса», — сказал он. «Вместе с тем, хочу обратить внимание, что на рынок таких проблем вышла новая история, когда для атак стали активно использовать интернет вещей», — добавил Сычев. По его словам, Банк России проводит по этому вопросу консультации с Минкомсвязью и Россвязью.

В выступлении Матвея Геринга, представителя СВИФТ, было анонсировано взаимодействие Банка России и СВИФТ в части обеспечения информационной безопасности, рассказано об имевших место атаках. Банк России поддерживает необходимость выполнения требований по информационной безопасности разработанных СВИФТ. Обсуждалась возможность построения систем антифрода для денежных переводов СВИФТ.

15 ФЕВРАЛЯ

Второй рабочий день Форума открылся дискуссией «Повышение культуры кибербезопасности». «Жидкая тема», — охарактеризовал ее, не подумав, один из журналистов. И ошибся. Разделенная надвое — «Культура профессионалов ИБ» и «Культура пользователей» — «жидкая тема» в устах неглупых людей спиралью поднялась до высоких обобщений и вернулась в зал конкретными примерами и практическими рекомендациями.

Неожиданный поворот дискуссия получила при обсуждении места белых хакеров в сфере ИБ. Сбербанк делает ставку на создание своей собственной команды «белых хакеров», а ВТБ привлекает внешние компании по мере необходимости. И еще большего накала дискуссия достигла, когда добралась до животрепещущей «культуры пользователей». Примеры из практики Сбербанка, ВТБ, Банка России звучали одновременно и убедительно, и противоречиво. Артём Сычев раскрыл страшную тайну этого противоречия — банальная про-

блема с деньгами. Культура, как известно, всегда финансировалась по остаточному принципу.

Следующая дискуссия — «Финтех и кибертех: вместе или врозь?» — по определению не могла быть «жидкой». Искусственный интеллект, интернет вещей, облака, блокчейн и т.д. — все это уже реальность, заполняющая нашу жизнь — работу и быт. Модератор Ольга Скоробогатова, заместитель председателя Банка России, сообщила, что время новых систем наступило, и рассказала о первом отечественном когнитивном продукте в сфере ИБ, который вот-вот поступит на рынок. Анастасия Масленникова, вице-президент Почта Банка, поделилась проблемой: без технологии удаленной идентификации ее банк уже терпит убытки. Сергей Солонин, генеральный директор QIWI plc, «пропел оду» блокчейну, что вызвало еще более бурное обсуждение... С развитием финтеха растут риски информационной безопасности. Вместе или врозь? — вопрос, оказалось, поставлен неправильно. Конечно, вместе!

После обеда открылась сессия «Возможности для атаки и практика защиты финансовых организаций». Началась она с серьезных, фундаментальных докладов со стороны регулятора: «Развитие платежных технологий: возможности и риски бизнеса, задачи регулятора» Олега Перестенко, Департамент платежной системы Банка России, и «Новые вызовы и защита прав потребителей финансовых услуг» Юрия Божора, Служба по защите прав потребителей и обеспечению доступности финансовых услуг Банка России. Профессионалам было безусловно интересно. Ведущий сессии Илья Медведовский прокомментировал так: «Банк России советуется с рынком и все делает адекватно».

Дмитрий Кузнецов, Positive Technologies, выступил с презентацией «Защита от кибератак на уровне платежного процесса», в которой рассказал, что до

45 компаний-партнеров

62 доклада

8 воркшопов, а также 4 дискуссии, 1 вечерние дебаты, 1 закрытая секция



Ольга Скоробогатова, заместитель председателя Банка России

2014 года банки больше защищали себя от клиентов, пока злоумышленники грабили не сами банки, а счета клиентов. В 2015 году ситуация изменилась — убытки стали терпеть непосредственно банки. И оказалось, что далеко не все они имеют возможность вкладываться в свою информационную безопасность. Дмитрий сказал: «Надо бороться!», и очень просто, почти на пальцах, показал, как защитить банк практически без затрат.

Всех встряхнуло эмоциональное выступление Кирилла Ермакова, QIWI. «Прекратите платить деньги за то, что бесплатно!» — заявил он. Стоит вспомнить, что в прошлом году его устный репортаж с места событий — захватывающее повествование о том, как в QIWI проводили жесткий тест на проникновение — стал хитом: BIS Journal позже опубликовал его почти дословно. В этом году Кирилл представил другой проект — информационный сервис трендов в сфере ИБ. Трендов подлинных (в смысле, не ложных, на которые клюют, засоряя свое сознание, тысячи безопасников), очищенных с помощью матанализа и других когнитивных методов. Зачем? — спросили его, — ведь это бесплатно! «Такая

вот у нас инициатива, — ответил он, — сделать хоть что-то для всех».

Еще больше ошарашил участников Форума Илья Медведовский, Диджитал Секьюрити. Как оказалось, это именно он по договоренности с Кириллом Ермаковым взломал в прошлом году QIWI. Но хвастать (в смысле, сильно хвастать) этим не стал. В своем выступлении «Блеск и нищета пентеста в режиме Read Team, или «Не нужна тебе, Вовка, такая машина» он в пух и прах разнес любителей поиграть в пейнтбол в стиле ИБ. Зачем? — задал он сакраментальный вопрос и подробно на него

ответил. Если вкратце, то это очень дорого, бесполезно и часто просто опасно.

Тем временем, в кулуарах журналисты терзали Артема Сычева, заместителя начальника ГУБиЗи Банка России, и Артема Сударенко, начальника отдела ФинЦЕРТ. Повод — выход в свет официального документа «Обзор несанкционированных переводов денежных средств за 2016 год». Стоит с гордостью заметить, что идея ФинЦЕРТа зародилась несколько лет назад именно на Уральском форуме, а сегодня, еще до пресс-конференции, на одной из дискуссий участники Форума пришли к общему выводу, что создание ФинЦЕРТа — одно из важнейших позитивных событий в сфере ИБ. Еще недооцененное.

Не менее интересной оказалась и сессия-дискуссия на тему «Аутсорсинг в ИБ». Достаточно сказать, что позиции ее соведущих Василия Окулесского, АО НСПК, и Игоря Ляпунова, Solar Security, оказались диаметрально противоположными. Что и стало пружиной долгого непростого разговора.

Вечерние дебаты на тему «Agile и безопасность. Практика безопасной разработки программного обеспечения в финансовом секторе» прервались далеко за полночь. Из необходимости немного поспать перед следующим рабочим днем.



Интересно, как представляют себе «профессионализм как часть цеховой культуры» известные в сфере ИБ люди:

**Андрей Акинин:**

«Профессионал ИБ — это прежде всего шериф, полицейский. Он охраняет хороших людей и не позволяет им стать плохими».

**Сергей Лебедь:**

«Профессионал информационной безопасности — прежде всего эксперт в IT».

16 ФЕВРАЛЯ

Сессию «Квалификационные требования и подготовка специалистов ИБ. Повышение осведомленности сотрудников финансовых организаций» открыл Андрей Выборнов (Банк России). В своей лапидарной манере он рассказал о планах по переработке РС «Квалификационные требования к специалистам по ИБ организаций КФС». В ближайших планах — в апреле — обсуждение и, возможно, утверждение «Примерной программы профессиональной переподготовки». Пора, давно пора, господа безопасники, подучиться, чтобы было легче работать в соответствии с требованиями регулятора.

Дальше разговор пошел об осведомленности сотрудников. Ведущий Лев Шумский (ГК «Связной») представил неутешительную статистику по антифишинговым проверкам. Так вот, открыли фишинговые письма, а затем и перешли по зловредным ссылкам 55% бухгалтеров, 50% сотрудников бэкофисов, 50% сотрудников ИТ. «С этим надо что-то делать», — покачал головой Шумский.

Оказалось, неплохой опыт есть в «Почта Банке» (докладчик Максим Лукин) и «ВымпелКоме» (Александр Голубев). Аудит осведомленности, точечное и массовое интерактивное обучение... Но оба сошлись во мнении, что разовые мероприятия не работают, повышение осведомленности — это постоянный процесс, комплексная программа. Александр Голубев привел интересный пример. В ВымпелКоме на каждом этаже на больших мониторах в режиме non-stop демонстрируют рекламные ролики, а между ними приятные девушки с угрозой произносят фразу из спецнабора, типа: «А ты поменял пароль?»

Ощущение, что повышение осведомленности персонала — дело почти безнадежное, сродни войне с ветряными



Владимир Чистюхин, заместитель председателя Банка России

мельницами, но делать его надо, терпенье и труд все перетрут, кое-что все-таки получается и т.д., разрушил Алексей Горелкин («Лаборатория Касперского»). Он заявил: «Надо превратить слабое звено в вашу сильную сторону!» А как? — молча спросил зал. Горелкин предъявил картину «Проповедь на селе», на которой тусклые прихожане уныло слушают бодрого проповедника и сообщил: «Сотрудники точно так же не воспринимают то, что им вдалбливают безопасники». И рассказал о подходах к обучению кибербезопасности, разработанных в его компании на самой что ни на есть современной основе: психология, педагогика, смена убеждений, метод непрерывного обучения...

— Проблема в том, — констатировал он, — что большинство программ повышения осведомленности работает только со знаниями. Но люди устроены иначе. Поведение — вот с чем надо работать в ходе тренингов!

«Да, есть все-таки свет в окошке», — подумал Шумский.

После кофе-паузы состоялось ключевое выступление дня. Владимир Викторович Чистюхин, заместитель пред-

седателя Банка России, рассказал об основных направлениях развития финансовых рынков и новых вызовах для безопасности. Главная мысль: в свете глобальной дигитализации все, что делает Банк России, он делает теперь сквозь призму информационной безопасности.

Развивая цифровые финансовые услуги, необходимо обеспечивать должный уровень защиты прав потребителей финансовых услуг, обеспечить соблюдение баланса между инновациями и рисками (необходимость выявления, оценки, мониторинга и управления рисками, возникающими в результате развития инноваций) и повышать уровень финансовой грамотности населения. Анонсировано введение оценки финансовых организаций с учетом жалоб, направляемых в Интернет-приемную Банка России.

Сразу после доклада неумолимые журналисты увели его на растерзание в пресс-рум. Вместе с Артемом Сычевым. Как обычно.

Следующая сессия называлась «Высокотехнологичное мошенничество. Что противопоставить?» Илья Кочетков (Банк России) рассказал о пробле-



Рустэм Хайретдинов:

«ИБ — это не профессия, а состояние, и мы в нашей компании поддерживаем его у сотрудников. ИБ у нас „размазана“ по всем ровным слоям».



Сергей Пазизин:

«Профессионализм в ИБ — это соответствие современным вызовам и умение решать поставленные задачи».



Артем Сычев:

«Профессионализм — это постоянный культурный и личностный рост, самостоятельность и умение работать в команде».



мах безопасности информационной среды в сфере микрофинансирования. Там осведомленность клиентов и пользователей на порядок ниже, чем среди сотрудников банков. В то же время, эта среда — просто райский сад, в котором вольно произрастают фишинговые сайты, а мошенники всегда счастливы. Одно их название чего стоит: псевдопосредники, агрегаторы, двойники, нелегальные кредиторы...

Дальше пошел разговор о технологиях ИБ. Александр Хегай («Кросс технологис») предъявил целый арсенал защиты от высокотехнологичного мошенничества, Алексей Сизов («Инфосистемы Джет») доказал теорему самообучаемости антифрода, Алексей Коняев («SAS») пропел осанну машинному обучению. Правда, в заключение на сцену поднялась гордая женщина Анна Гольдштейн («Информзащита») и безапелляционно развенчала это самое машинное обучение.

Самой насыщенной — от обеда до ужина (и все равно времени не хватило) — стала сессия «Проблема доверия к идентификации и аутенти-

фикации в финансовой среде». Тема ключевая, сложная, необходимая и... пока так и не разрешенная. Максим Григорьев (Банк России) рассказал о планах Банка России по построению удаленной идентификации клиентов финансовых организаций на основе Единой системы идентификации и аутентификации с привлечением банков, Иван Янсон (Сбербанк) также поддержал планку на уровне государственных решений. Сбербанк пытается решить задачу идентификации и аутентификации в рамках эксперимента по удаленной регистрации бизнесов и открытия счетов с использованием облачной подписи.



17 ФЕВРАЛЯ

Заключительную часть деловой программы составила сессия «Угрожающий» день практической безопасности», во время которой происходил обмен эффективными практиками расследования инцидентов информационной безопасности. А завершился форум стратегической бизнес-игрой. Четыре команды, включая команду ЦБ, в течение двух часов спасали «свои банки» от вполне серьезных нападений злоумышленников. Была продемонстрирована недюжинная эрудиция и часто феноменальная сообразительность.

Организовали и провели игру представители Сбербанка и «Лаборатории



31 мая в Москве состоится Летняя сессия Уральского форума. Среди основных тем — применение актуальных версий стандартов ИБ международных платёжных систем, взаимодействие организаций финансовой сферы в деле противодействия DDoS-атакам, вопросы идентификации и аутентификации в контексте использования ЕСИА.

Касперского». Каждой из команд предлагалось почувствовать себя на месте руководства службы информационной безопасности банка, получив под контроль IT-инфраструктуру, которую необходимо защитить от атак при ограниченном бюджете. Основная цель участников — закончить игру с максимальным доходом. Всё как в реальной жизни.

— Игра воспроизводит основные действия и процессы, с которыми в реальной жизни сталкиваются специалисты информационной безопасности кредитно-финансовых организаций, — рассказал один из организаторов игры, представитель Сбербанка Кирилл Мартыненко. — Такой подход отражает основные тенденции и культурные основы развития современной службы кибербезопасности. Сегодня специалист кибербезопасности осознает, что его задачи напрямую связаны с задачами бизнеса. Правильное распределение ресурсов, гибкий подход к конкретному случаю киберугрозы, атаки становятся залогом эффективной защиты банка, с одной стороны, и условием максимально допустимого дохода для бизнеса, с другой. И порой, став участником игры, специалист впервые осознает этот новый подход, и завершает игру уже с перевернутым сознанием.

Очень неоднозначно отношение к службе кибербезопасности других подразделений банка — увы, часто нас воспринимают как карателей и ограничителей. Игра позволяет сотрудникам банка попробовать себя в роли безопасника, и это в итоге помогает облегчить взаимопонимание со службой информационной безопасности, увидеть стоящие перед ней непростые задачи, сотрудничать с ней по доброй воле. Ну, и конечно в захватывающей форме каждый участник осваивает современный ландшафт компьютерных угроз, в котором все мы вынуждены жить. Игра провоцирует мыслить стратегически и работать в команде.

СПОРТИВНЫЕ ИГРЫ «БАНКОВСКИЕ БИТВЫ»

В день прибытия на Урал, 13 февраля 2017 года, на ледяном ринге встретились сборные команды банков «НАШИ» и интеграторов «ТОЖЕ НАШИ». Отважные спортсмены сошлись в матче по хоккею с шайбой «в валенках»



А по соседству заснеженная местность превратилась в поле боя для участников командного лазертаг-матча «Банковская зарница»



Остальные участники болели за команды и шумно подбадривать игроков. А также соревновались в различных подвижных играх

Подробная информация
и условия участия на сайте:

ural.ib-bank.ru

ГЕРОИ НАУЧНЫХ ГОРИЗОНТОВ

В марте в Математическом институте им. В.А. Стеклова Российской Академии Наук (МИАН) состоялось ежегодное награждение победителей интеллектуальных соревнований школьников в области защиты информации — Межрегиональной олимпиады по математике и криптографии и Межрегиональной олимпиады по информатике и компьютерной безопасности.

Олимпиада по криптографии проводится 26-й год подряд, Олимпиада по компьютерной безопасности — одиннадцатый. И если в первые годы в них принимали участие не более сотни ребят, то теперь статистика этих мероприятий не может не впечатлять: число участников приближается к 6000, а проведение очного тура охватывает около 50 городов — от Калининграда до Владивостока. Таким образом создаются предпосылки для решения важнейшей для каждой отрасли науки и техники задачи — заинтересовать в приходе в профессию наиболее подготовленных и способных школьников, создать условия для воспроизводства и развития накопленных знаний.

Учредители олимпиад — Академия криптографии РФ и Институт криптографии, связи и информатики Академии ФСБ России — провели за минувшие годы колоссальную организационную и методическую работу. Весомый вклад в становление межрегионального статуса олимпиад внесло федеральное учебно-методическое объединение «Информационная безопасность» и Общественный совет при ФСБ России. По результатам экспертной оценки олимпиады ежегодно включаются в перечень Министерства образования и науки России для предоставления их призерам предусмотренных законодательством особых прав при поступлении в вузы. При этом анализ результатов ЕГЭ подтверждает вы-

сокий уровень подготовки награжденных школьников.

По сложившейся многолетней традиции объявление итогов олимпиад и вручение дипломов проводится при участии ведущих учреждений науки, культуры или образования. В этом году мероприятие прошло в МИАН, а его организацию взял на себя Фонд содействия развитию безопасных информационных технологий.

После сообщения жюри об итогах решения задач, перед собравшимися школьниками, их учителями и родителями выступил руководитель лаборатории популяризации математики МИАН, кандидат физико-математических наук Николай Андреев. Его лекция «Математическая составляющая» сопровождалась наглядной демонстрацией удивительных фактов из мира геометрии и физики, при этом имеющих важное прикладное значение в различных областях техники.

Перед вручением дипломов к школьникам с вдохновляющей речью обратился председатель оргкомитета олимпиады, вице-президент Академии криптографии РФ Владимир Сачков: «Если вы выберете криптографию своей профессией, то никогда не будете разочарованы — столь многообразна

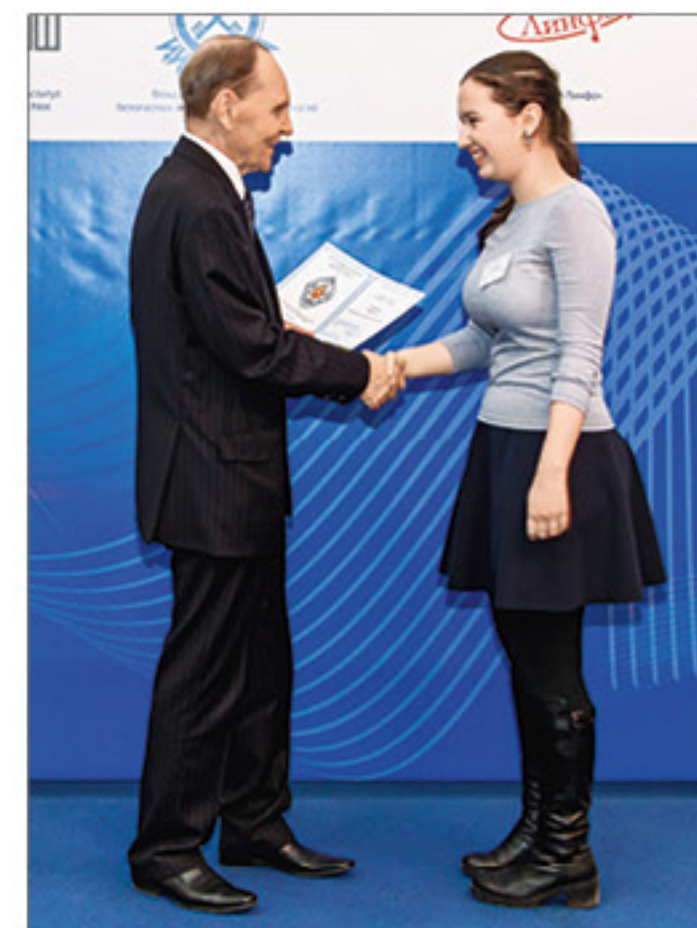
и интересна эта область знаний и умений. Нет деятельности более современной и идущей в ногу со временем! Когда проводились первые олимпиады по криптографии, никто не подозревал, что на наших глазах — и во многом силами тех, самых первых, победителей наших олимпиад — возникнет и получит мощное развитие асимметричная криптография, квантовая криптография, благодаря которым сегодня создаются новые направления в математике и физике. Также постоянно расширяется и сфера применения криптографии. Когда-то она использовалась исключительно в дипломатии и военном деле, а теперь это — финансы, банковское дело, информатика, компьютерные технологии...»

Действительно, будущее отрасли информационной безопасности формируется на наших глазах. Сегодня эти юные победители — всего лишь потенциал отрасли, ее «олимпийский резерв», а завтра — пионеры, творцы новых направлений, герои стремительно приближающихся научных горизонтов XXI века.

ИНТЕРВЬЮ С ЛАУРЕАТОМ

Вениамин Марков, призер III степени (11 класс, ГОУ СОШ № 6, Мытищи):

— Все началось с компьютерных игр. В 10 классе играл в СТФ, у нас хорошая команда, не раз побеждали в крупных соревнованиях. Увлёкся информационной безопасностью, стал хакером на белой стороне. Хожу на дополнительные занятия в школу программирования, но в основном занимаюсь сам, читаю книжки по криптографии — в школе такому не учат. Свой результат на Олимпиаде оцениваю как удовлетворительный. Мог бы и лучше, но сильно переволновался. В перспективе хотел бы посвятить себя интересным проектам: созданию банковских сервисов, социальных сетей, компьютерных игр. Люблю читать. Очень понравились «Мастер и Маргарита» Булгакова, «Отец Горио» Бальзака. Кино люблю про супергероев. Но книги и кино — это всего лишь разные истории, а мне больше по душе практика. Сложная практика.



ИНТЕРВЬЮ С ЛАУРЕАТОМ

Артур Яворски, призер I степени (11 класс, Лицей ЛИЕН, Саратов):

— В разных олимпиадах я участвую много лет. Получал разные дипломы, но первое место — это впервые. Увлекаюсь программированием. У нас хороший лицей, знания по математике и информатике довольно глубокие, но компьютерная безопасность потребовала дополнительных занятий. Большинство заданий выполнил легко, но были и такие, где сомневался до последнего. Даже не ожидал, что решил правильно. Учиться дальше буду по направлению «математика и программирование», где — еще не решил. Родители предлагают ехать в Питер. Мне собственно все равно, главное — чтобы было интересно... и связано с математикой и программированием.



Андрей ВЫБОРНОВ
начальник отдела
ГУБиЗИ Банка России

КАДРЫ ПО НОВЫМ СТАНДАРТАМ

В БАНКЕ РОССИИ ВПЕРВЫЕ РАЗРАБАТЫВАЮТСЯ
ПРИМЕРНЫЕ УЧЕБНЫЕ ПРОГРАММЫ ПО ПОДГОТОВКЕ
СПЕЦИАЛИСТОВ ИБ В ОРГАНИЗАЦИЯХ КРЕДИТНО-
ФИНАНСОВОЙ СФЕРЫ

Проблема нехватки кадров в области информационной безопасности характерна не только для коммерческих организаций. Даже Банк России испытывает определенные трудности в подборе квалифицированных сотрудников, которые могут работать по направлению обеспечения ИБ. С аналогичной проблемой сталкиваются и кредитно-финансовые организации. В связи с этим по инициативе и при участии Банка России создаются базовые программы для обучения и переподготовки специалистов в области обеспечения информационной безопасности организаций кредитно-финансовой сферы.

Социологические опросы показали, что проблема нехватки квалифицированных кадров в сфере информационной безопасности характерна для многих организаций кредитно-финансовой сферы (КФС). Перед Банком России встал вопрос, какие организационные мероприятия необходимо предпринять, чтобы создать условия для стабильного воспроизводства таких специалистов в нашей стране?

НЕОБХОДИМО, НО НЕДОСТАТОЧНО

В апреле 2016 г. подразделения Главного управления безопасности и защиты информации Банка России (ГУБиЗИ) начали разработку рекомендаций в области стандартизации, которые представляют собой квалификационные требования к специалистам по информационной безопасности организаций КФС. Эти рекомендации были разработаны и не раз рассматривались на подкомитете «Безопасность финансовых (банковских) операций» Технического комитета по стандартизации «Стандарты финансовых операций» (ТК 122).

Осенью прошлого года проект рекомендаций РС БР ИББС-2.X-20XX «Квалификационные требования к специалистам по информационной безопасности организаций кредитно-финансовой сферы Российской Федерации» был готов. Однако по итогам взаимодействия с разными сторонами, в т.ч. с уполномоченными органами в области образования, мы поняли, что этого документа для массового появления специалистов в области ИБ будет

МЫ ПОЛАГАЕМ, ЧТО УЧИТЬ СПЕЦИАЛИСТОВ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИБ СЛЕДУЕТ В РАМКАХ БИЗНЕС- И ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ОРГАНИЗАЦИЙ КФС

недостаточно. И было принято решение о разработке программы профессиональной переподготовки кадров на базе подготовленных ранее рекомендаций. Сейчас ведется активная работа по подготовке такой программы.

ПО СХЕМЕ ФСТЭК

Вопросы образования в области защиты информации курирует уполномоченный орган — Федеральная служба по техническому экспортному контролю (ФСТЭК). Указанный федеральный орган исполнительной власти разрабатывает примерные программы профессиональной переподготовки в определенной сфере, эти программы согласовываются, получают статус во ФСТЭК России, после чего на базе этих примерных программ конкретные учебные заведения разрабатывают свои программы профессиональной переподготовки. Которые в свою очередь проходят процесс согласования в ФСТЭК и, наконец, становятся основой для обучения слушателей.

Исходя из такой практики, мы решили сначала разработать «Примерную программу профессиональной переподготовки кадров», первая редакция которой будет готова в апреле этого года. После придания программе официального статуса мы планируем до конца 2017 г. (совместно с кадровым подразделением Банка России и при участии учебных заведений) организовать обучение слушателей на курсах, созданных на основе «Примерной программы профессиональной переподготовки кадров».

СПЕЦИФИКА КФС. СУТЬ ПРОГРАММЫ

При создании любой учебной программы возникает вопрос: чему учить будущих высококвалифицированных специалистов? Поскольку наша программа разрабатывается на базе рекомендательных документов ФСТЭК и в будущем должна быть согласована с этим

ведомством, мы, безусловно, следуем его рекомендациям.

Мы вводим новый вид профессиональной деятельности — «Обеспечение информационной безопасности в кредитно-финансовой сфере». Поскольку мы готовим программу переподготовки, ее продолжительность должна быть не менее 500 часов. Если говорить о содержательной части программы, то в рамках курса есть такое понятие — объекты профессиональной деятельности. Мы полагаем, что учить специалистов в сфере обеспечения ИБ следует в рамках бизнес- и технологических процессов организаций КФС. В том числе, в рамках процесса перевода денежных средств. Усилия специалистов, которые будут учиться по новой программе, должны быть направлены на объект информационной инфраструктуры организации КФС, включая автоматизированные системы и учитывая реализацию бизнес- и технологических процессов Банка России.

Работа специалиста по ИБ в КФС должна основываться на знании действующего законодательства и нормативно-правовых актов Российской Федерации, в т.ч. нормативных актов и требований Банка России, стандартов и других документов в области стандартизации. Прошедшие переподготовку специалисты должны обладать необходимыми навыками и умениями, чтобы обеспечить реализацию процессов обеспечения ИБ, обеспечить применение средств и систем защиты информации применительно к объекту информационной инфраструктуры.

КТО БУДЕТ УЧИТЬСЯ?

Любая переподготовка кадров ведется на основе базового образования. Кто те специалисты, которые, как я полагаю, могут обучаться по новой программе? Это люди, которые получили высшее профессиональное образование по следующим направлениям:

- ♦ специалисты в области защиты информации;
- ♦ специалисты в различных областях информационных технологий ИТ;
- ♦ обладатели военных специальностей, которые связаны с организацией мероприятий по защите информации или использованием вычислительных сетей.

ЧЕМУ? ДВА ПОДХОДА

Согласно регламентирующим документам ФСТЭК России, на которые опира-

ется ГУБиЗИ при создании программы переподготовки, все виды профессиональной деятельности делятся на организационно-управленческую, проектную и эксплуатационную. В документах Банка России, в т.ч. в рекомендациях по ресурсному обеспечению, используется несколько иной подход. Мы рассматриваем вопросы методологии, реализации сопровождения и контроля. Поэтому в программе переподготовки кадров мы попробуем совместить и отразить оба подхода.

В части организационно-управленческой методологической деятельности подготовленный специалист должен обладать знаниями, навыками и умениями в следующих областях:

- ♦ организация и контроль работы службы ИБ организации КФС;
- ♦ установление и контроль целей ИБ;
- ♦ управление рисками ИБ организации КФС;
- ♦ вопросы ресурсного обеспечения ИБ;
- ♦ управление проектами и договорная деятельность;
- ♦ планирование и реализация контроля совершенствования процессов обеспечения ИБ;
- ♦ организация взаимодействия с причастными сторонами (что очень важно с точки зрения обеспечения киберустойчивости);
- ♦ назначение и управление ролями, связанными с обеспечением ИБ, и повышение осведомленности персонала и причастных лиц и клиентов организаций КФС.

Следующий блок вопросов — проектная деятельность, которая в первую очередь решает вопросы реализации сопровождения и обеспечения ИБ. Сюда входят:

- ♦ концептуальное, архитектурное и техническое проектирование реализации процессов обеспечения ИБ в информационной инфраструктуре организаций КФС;
- ♦ установка функционально-технических требований к средствам систем обеспечения ИБ;
- ♦ выбор средств и систем обеспечения ИБ для применения в рамках процессов обеспечения ИБ;
- ♦ контроль реализации средств и систем обеспечения ИБ в информационной структуре организации КФС;
- ♦ контроль обеспечения информационной безопасности на этапах жизненного цикла автоматизированных систем.

И последний блок вопросов — эксплуатационная деятельность. В терминологии Банка России — это контроль и совершенствование обеспечения ИБ:

- ♦ обеспечение комплаенс-контроля, в первую очередь, на соответствие законодательству и отраслевым и перспективным национальным стандартам;
- ♦ организация и реализация контроля защищенности;
- ♦ оперативный мониторинг, обнаружение вторжений и сетевых атак;
- ♦ управление инцидентами ИБ, взаимодействие с подразделением ФинЦЕРТ Банка России, сбор и обработка технических данных, связанных с инцидентами, взаимодействие с правоохранительными органами (форензика);
- ♦ организация проведения самооценок и внешних аудитов ИБ.

КЛЮЧЕВЫЕ ПРОЦЕССЫ

Если говорить о тех ключевых процессах обеспечения ИБ, которым будут обучаться новые кадры, то это вопросы:

- ♦ обеспечения защиты информации при управлении доступом;
- ♦ обеспечения защиты вычислительных сетей;
- ♦ контроля целостности и защищенности информационной инфраструктуры;
- ♦ обеспечения защиты от воздействия вредоносного кода;
- ♦ предотвращения утечек информации, защита машинных носителей информации;
- ♦ менеджмента инцидентов защиты информации;
- ♦ защиты среды виртуализации;
- ♦ защиты информации при осуществлении логического доступа с использованием мобильных (переносных) устройств.

Эти процессы подробно отражены в новом национальном стандарте «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер защиты информации», который планируется ввести в действие в 2017 г.

Все ключевые процессы обеспечения ИБ мы предполагаем выстроить таким образом, чтобы они не были абстрактными категориями, а оказались четко привязаны к специфике деятельности кредитных организаций, к специфике реализации бизнес-процессов и технологических процессов кредитных организаций, а также к той инфраструктуре, которая эксплуатируется кредитными организациями.

* * *

Можно констатировать, что на сегодняшний день задача по созданию условий для воспроизводства необходимого и достаточного количества компетентных специалистов в области обеспечения ИБ в организациях КФС, поставленная перед ГУБиЗИ Банка России, успешно решается, и можно надеяться, будет решена в ближайшие годы.



Александр ГОЛУБЕВ
директор дирекции
по информационной
безопасности
ПАО «ВымпелКом»

ОСВЕДОМЛЕННЫЙ СОТРУДНИК — ЗАЩИЩЁННАЯ КОМПАНИЯ

ОПЫТ СОЗДАНИЯ КОРПОРАТИВНОЙ КУЛЬТУРЫ
В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как показывает практика, какая бы мощная система защиты ни стояла по периметру, всегда найдется слабое место. Чаще всего этим слабым местом оказывается человек. По статистике, больше 80% инцидентов в области информационной безопасности связаны именно с человеческим фактором. Причем угрозы возникают не из злого умысла сотрудников, а по причине их невнимательности, расслабленности, а чаще всего, банальной неосведомленности.

Корпоративная культура, как и театр, начинается с вешалки, то есть с отдела кадров. Поделюсь наблюдениями за практикой трудоустройства рядовых сотрудников. Традиционно при устройстве на работу человек получает в отделе кадров пачку бумаг, которую надо изучить, заполнить и подписать. Новички подписывают соглашение о неразглашении информации, дают своё согласие на обработку персональных данных, подписывают, не вникая из-за дефицита времени в содержание большого количества бумаг. Дальше идёт обустройство на новом месте: прохождение инструктажа на рабочем месте, получение компьютера, знакомство с обязанностями, соседями... О том, что следовало бы изучить некие положения, как правило, все успешно забывают.

В крупных компаниях на испытательный срок новичку назначается куратор. Он вводит в курс дела, в том числе знакомит с темой информационной безопасности — вне зависимости от того, в каком подразделении начал работать человек. Но и такой подход, оказывает-

ся, не является решением проблемы осведомленности в сфере ИБ. Эту проблему нужно решать постоянно.

Под повышением осведомленности в вопросах информационной безопасности обычно понимается:

- ♦ обучение сотрудников компании вопросам обеспечения ИБ;
- ♦ повышение осведомленности об актуальных угрозах ИБ, мерах и способах реализации атак, и средствах защиты;
- ♦ фокусировка внимания сотрудников на важности обеспечения ИБ и пр.

Какова программа повышения осведомленности? В нашей компании мы используем Цикл Деминга — PDCA (англ. Plan-Do-Check-Act — планирование — действие — проверка — корректировка) — циклически повторяющийся процесс принятия решения, который используется в управлении качеством. Мы применили этот цикл к системе обучения и тестирования персонала в области ИБ.

Все необходимые требования, действующие в компании, должны быть представлены сотруднику в доступной, понятной форме. Например, в силу специфики ВымпелКома у нас в офисе расставлены мониторы, на которых в режиме нон-стоп крутится реклама бренда. Периодически реклама прерывается, и очаровательная девушка строго спрашивает: «А ты не забыл сменить пароль?!», «А ты помнишь, что он должен быть не менее восьми буквенно-цифровых символов?» и т.д. Такая практика напоминания приносит свои практические плоды.

Процесс повышения осведомленности работников Компании в обла-

сти ИБ не должен быть разовой акцией: провели, отчитались и забыли. Это рутинная, порой монотонная работа, которую нужно проводить регулярно. Основной вопрос при внедрении программы повышения осведомленности — найти поддержку у руководителей компании, отвечающих за финансовую сторону бизнес-процессов. Для этого необходимо представить и защитить бизнес-план, в котором определены основные моменты программы, целевая аудитория, исполнители и заказчик.

При составлении плана работ мы выделили ответственных за создание и реализацию программы, определили цели и задачи проекта. Сложный момент — определение целевых аудиторий. В зависимости от занимаемых должностей и служебных обязанностей сотрудникам требуется разное обучение в разном объеме. Можно выделить финансовый блок, IT-персонал, менеджмент, внешних исполнителей и т.п.

Поскольку базовый стандарт квалификационных требований к подготовке специалистов ИБ для телекоммуникационных компаний пока не определен, за основу мы взяли стандарт Банка России СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности», стандарты безопасности индустрии платежных карт PCI Security Standards Council, пакет международных стандартов COBIT 5, наработки в области тренингов Национального института стандартов и технологий США, Европейского агентства по IT-безопасности ENISA. Также по-

лезно было изучить материалы вендоров, интеграторов, программы отечественных и зарубежных учебных центров.

Далее для каждой целевой аудитории определяется актуальный набор мероприятий. Способы донесения информации могут быть различные: семинары, тренинги, вебинары, мультимедиа-курсы, рассылки, бюллетени безопасности, постеры и пр.

Чтобы оценить результат, мы заранее подготовили метрики для анализа эффективности программы и подготовили мероприятия по проверке и тестированию полученных сотрудниками знаний.

Очень важен вопрос обратной связи. Какой бы замечательный лектор или именитый эксперт в области ИБ ни выступил перед вашей целевой аудиторией, вы не сможете оценить эффективность его выступления, если не имеете обратной связи. Отзывы сотрудников помогают понять, насколько им интересно и полезно то или иное мероприятие. Часто приглашенный эксперт, будучи отличным специалистом, оказывается плохим оратором, не способным донести свои знания до аудитории. А часто аудитории и не требуются глубокие знания в специфических областях ИБ — достаточно общего обзора, но изложенного понятно и увлекательно.

Важно также поддерживать связь с руководством — от его вовлеченности в процесс повышения корпоративной культуры зачастую зависит финансирование и дальнейшее развитие этого проекта.

Поскольку программа повышения осведомленности носит непрерывный, циклический характер, необходимо завершать каждый её этап полноценной проверкой знаний сотрудников и сбором их мнений о качестве проведенной работы. Иначе весь проект превратится в пустую формальность. Кроме того, необходимо постоянно анализировать ландшафт угроз, отслеживать новые требования регуляторов и дополнять программу обучения новыми материалами, учитывая стоящие перед компанией как оперативные, так и долгосрочные цели.

Среди тенденций в работе с персоналом стоит отметить свободный график

и отсутствие жесткой привязки к рабочему месту. Компания активно практикует модель работы сотрудников на «BeeFREE», т.е. возможность удаленной работы из любого места, без привязки сотрудника к рабочему месту в офисе. Причём с точки зрения повышения осведомленности работников в вопросах ИБ удаленная работа — хороший повод провести тестирование на практике.

Основные угрозы для рядовых сотрудников — это, как правило, фишинговые письма. По согласованию с руководством Компании мы провели собственную рассылку таких писем. Пошли по наиболее жизненному сценарию: сотрудникам отдела маркетинга мы разослали послания с предложением необычного продукта, в HR-службу — резюме от соискателя работы и т.д. Большинство писем содержали просьбу перейти по ссылке и ввести свою учетную запись.

Результат оказался ошеломляющим. Большинство сотрудников, не придав должного внимания, перешли по этим ссылкам и «поделились» данными своей корпоративной учётной записи. Появился повод как минимум задуматься о повышении осведомленности сотрудников и роли ИБ в Компании, а как максимум — организовать постоянное финансирование программы образования сотрудников в области ИБ.

Заручившись финансовой поддержкой, Дирекция по ИБ разработала программу и методику обучения по вопросам ИБ, которая была включена в общую корпоративную программу обучения «Билайн-университет». Обучение и тестирование в течение года работники Компании проходят на регулярной основе. Положение об ежемесячных проверках осведомленности персонала в ближайшее время будет внесено отдельным пунктом в «Политику информационной безопасности Компании».

Каждый месяц, готовя отчет, мы отмечаем сотрудников и структурные подразделения, которые попадают на те или иные уловки, и проводим с ними дополнительное обучение. Человека отправляют на курсы и тренинги в автоматизированном режиме. Сдал тест,

набрал определенное количество баллов — иди дальше. Не набрал — учись по второму кругу. Если после нескольких попыток проблема не решается, то стоит, как минимум, присмотреться к сотруднику.

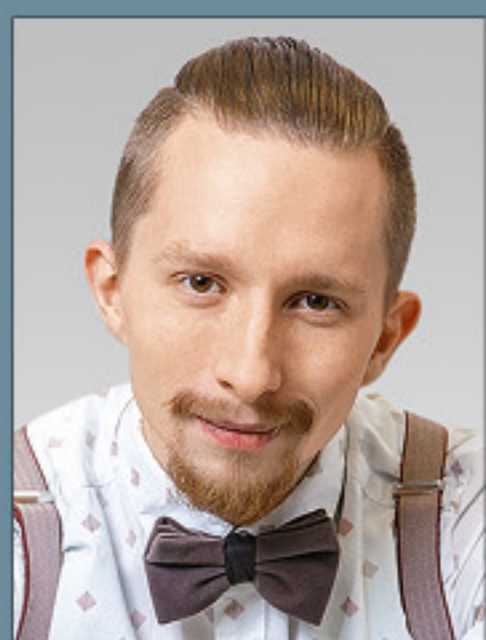
Как сделать обучение интересным? Можно использовать геймификацию и интерактивные техники, хорошо работают методы стимуляции и поощрения за высокие результаты в программе, привлечение успешных сотрудников к обучению коллег. Стоит обращать внимание персонала на то, что полученные знания и навыки полезно применять не только на работе, но и в личной жизни, дома.

Программа повышения осведомленности достаточно быстро принесла свои плоды. После проведенной рассылки «фишинговых» писем сотрудники стали задумываться, прежде чем открыть какое-то письмо. Первое время моему структурному подразделению пришлось особенно трудно — на нас обрушился шквал вопросов: отсылать его на проверку в «песочницу», стоит ли открывать то или иное письмо, фишинг это или это только повод попасть на обучение? Со временем такие наивные обращения сошли на нет, что говорит о пользе проведенного обучения.

* * *

Аналогичную программу повышения осведомленности в вопросах информационной безопасности можно реализовать на базе учебных центров, у которых есть своя программа-методика преподавания, аккредитации в данной области и необходимые лицензии регуляторов. Часто готовы обучать сотрудников организации вендоры, компании-интеграторы (партнёры), поставляющие оборудование и заинтересованные в его грамотной эксплуатации. Однако гораздо надежнее, спокойнее и проще собрать и подготовить специалистов в своей компании, иметь собственную необходимую экспертизу.

И тогда можно перевести самое слабое звено в цепи защиты от разного рода кибератак в надежный элемент ИБ.



Алексей ГОРЕЛКИН
инженер предпродажной
поддержки
АО «Лаборатория
Касперского»



ИГРА В БЕЗОПАСНОСТЬ

СОВРЕМЕННЫЕ ПОДХОДЫ К ОБУЧЕНИЮ ПОМОГАЮТ
РЕЗКО ПОВЫСИТЬ УРОВЕНЬ ОСВЕДОМЛЕННОСТИ
СОТРУДНИКОВ В ОБЛАСТИ ИБ

По данным IBM 2015 Cyber Security Intelligence Index, более 95% всех internal incidents (внутренних инцидентов) в сфере информационной безопасности компаний вызваны ошибками пользователей. При этом большинство организаций даже не задумываются о том, что пользователи являются очень уязвимой частью ИБ компании. В то время как департамент ИБ планирует вложить средства в защиту периметра компьютерной сети, покупку нового оборудования и программного обеспечения, вопросы обучения пользователей остаются за пределами его внимания.

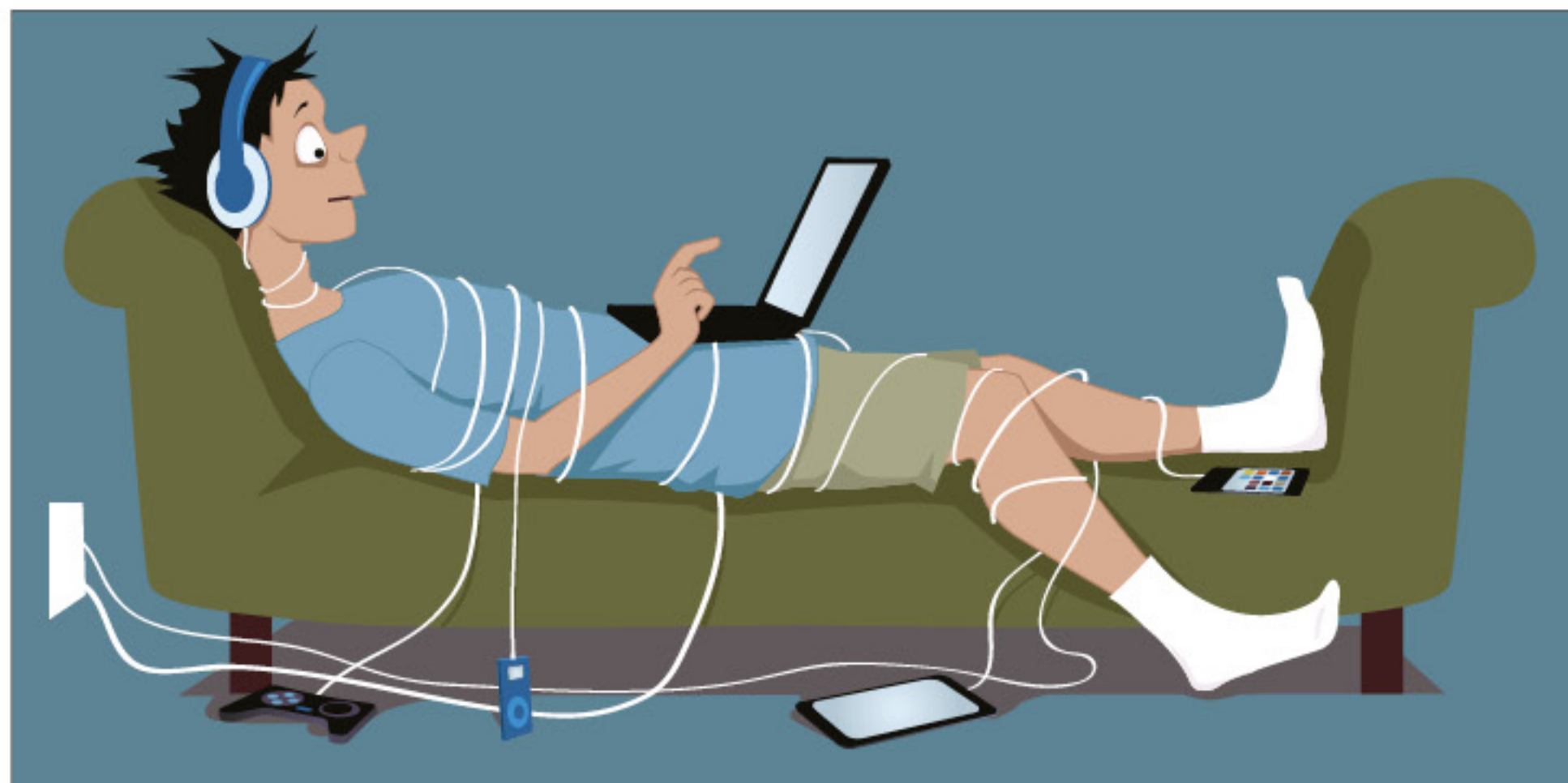
ЧТО ИМЕЕМ НА ПРАКТИКЕ?

Как уже не раз отмечалось многими специалистами в сфере ИБ, весь инструктаж сотрудников компаний чаще всего сводится к формальному ознакомлению с инструкциями и приказами, а все просвещение на тему ИБ — к постерам с напоминаниями сменить пароль и быть бдительным. В некоторых организациях сотрудники отдела ИБ проводят семинары, на которых пы-

таются обучить коллег из других департаментов базовым знаниям и навыкам в области ИБ. Однако чаще всего слушатели не запоминают эту информацию, поскольку она им не интересна: мало кто готов выйти за пределы основной специальности и погрузиться в изучение новой сферы деятельности.

Отсюда возникает вопрос проработки нового, эффективного метода обучения сотрудников компании.

**95% ВСЕХ ВНУТРЕННИХ ИНЦИДЕНТОВ
В СФЕРЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ КОМПАНИЙ ВЫЗВАНЫ
ОШИБКАМИ ПОЛЬЗОВАТЕЛЕЙ**



КЛИПОВОЕ МЫШЛЕНИЕ

Сегодня все привыкли иметь дело с гаджетами, все привыкли к мобильности, к тому, что из любой точки — дома, в транспорте, на прогулке — можно подключиться к глобальной сети и получить любые сведения. Современный мир перегружен информацией, и сегодня практически никто не будет без особенной необходимости часами изучать сложные документы. Как установили психологи, любому человеку сложно сосредотачиваться на каком-то вопросе более 45 минут. Современная молодежь воспринимает информацию блоками, через короткие яркие образы или статьи, заголовки новостей, небольшие видеоклипы, — это т.н. клиповое мышление. При этом для привлечения внимания информация должна подаваться броско, в хорошем качестве, иначе она не дойдет до пользователя в полном объеме.

Еще один психологический аспект, который стоит использовать в работе с современными сотрудниками, пользователями гаджетов, — это любовь к компьютерным играм. Почему люди играют? Потому что это просто, доставляет удовольствие и в итоге игры люди получают некий результат. Если же давать ту же информацию в виде

сухого текста, никакого удовольствия такая «игра» не принесет. Как не принесут удовольствия и нормы, правила и принципы работы в информационной среде на рабочем месте, сведения о которых пытаются донести до сотрудников IT- и ИБ-департаменты.

ПСИХОЛОГИЯ В ОСНОВЕ ОБУЧЕНИЯ. СМЕНИТЬ АЛГОРИТМ

Что следует из сказанного выше? Для успешного обучения пользователей можно подойти к повышению культуры ИБ с использованием психологии. В первую очередь нужно изменить алгоритм обучения: сначала выработать у сотрудников правильное поведение, а не пичкать их новыми знаниями. Пример правильного поведения — не кликать бездумно по всем ссылкам в письмах. А уже после выработки поведения дать и более глубокие знания в области ИБ — для тех сотрудников, для которых это имеет смысл.

Слабым звеном в ИБ любой компании принято считать бухгалтерию. Однако, как показывает практика, очень часто после проведения занятий по повышению осве-

домленности сотрудники бухгалтерии начинают внимательно работать с входящими письмами. И нередко пересылают сомнительную корреспонденцию в IT-отдел. Где даже рядовой сотрудник имеет привилегированные права для работы в сети, но, как показывает практика «Лаборатории Касперского», часто плохо ими распоряжается. Например, в отличие от сотрудника бухгалтерии, IT-сотрудник запросто открывает вызвавшее подозрение у бухгалтера фишинговое письмо с отчетом в формате pdf, содержащим дропер. Таким образом из-за халатности инженера службы поддержки злоумышленники взломали сеть компании. Поэтому часто обучение ИБ надо начинать не с бухгалтерии, а с IT-департамента, как с сотрудников, имеющих наибольшие права по управлению сетью организации.

ИГРА КАК ИСТОЧНИК ЗНАНИЙ

В какой форме лучше проводить тренинги? В игровой. Любой обучающий теоретический модуль должен быть написан в доступной форме, легким языком. И после теоретической части следует сразу проводить практическую, чтобы стало понятно, как применить полученные знания. Итогом обучения должна стать некая интерактивная проверка новых знаний и умение применить их на практике. Продолжительность всего модуля обучения не должна превышать 20 минут, в идеале она должна составлять 10–15 минут, чтобы пользователь не устал, чтобы ему было интересно и его хорошее настроение повлияло на мотивацию дальнейшего получения новых знаний и навыков.

Идеально, если новая платформа обучения ИБ станет предметом обсуждения в рабочем коллективе. Это не

только повысит интерес отдельных сотрудников к вопросам ИБ, но и скажется на общей культуре ИБ в компании. Также росту интереса к процессу обучения может способствовать рейтинг сотрудников по полученным достижениям. Соревновательная часть очень мотивирует людей, большинство не хочет быть последними. Поэтому необходимо, чтобы процесс обучения был прозрачным,

ЧАСТО ОБУЧЕНИЕ ИБ НАДО НАЧИНАТЬ НЕ С БУХГАЛТЕРИИ, А С IT-ДЕПАРТАМЕНТА, КАК С СОТРУДНИКОВ, ИМЕЮЩИХ НАИБОЛЬШИЕ ПРАВА ПО УПРАВЛЕНИЮ СЕТЬЮ ОРГАНИЗАЦИИ



чтобы любой работник мог понять, где он находится относительно других сотрудников.

Как показывает практика нашей компании, соблюдение баланса между выработкой поведения в ИТ среде, предоставлениями знаний и мотивацией помогает активно и продуктивно внедрять программу повышения осведомленности в той или иной организации.

РЕЗУЛЬТАТЫ ИГР

Как ведут себя сотрудники компании, где успешно работает программа повышения осведомленности? Руководители начинают взаимодействовать со службой ИБ и понимают её значимость для бизнеса, а не отмахиваются от вопросов ИБ как от вторичных проблем. Естественно, обучение руководителей несколько отличается от обучения иных сотрудников. Но сам факт понимания того, что повышение осведомленности в сфере ИБ необходимо на всех уровнях карьерной лестницы, важен при обучении информационной безопасности высшего руководства любых компаний. Для менеджеров среднего уровня — руководителей подразделений — обучение необходимо для понимания личной ответственности за безопасную работу своих отделов. Потому они должны активно внедрять нормы ИБ в своих подразделениях и добиваться более безопасного поведения сотрудников, а не перекладывать всю ответственность за инцидент на ИБ-департамент компании.

В глобальном плане, по итогам проведения программы повышения осведомленности в области ИБ, все сотрудники организации должны понимать и разделять ценности безопасного поведения, соблюдать меры безопасности, сообщать о потенциальных инцидентах и активно взаимодействовать со специалистами отдела ИБ.

ИЗМЕНЕНИЕ МОТИВАЦИИ

Какие еще преимущества дает учет психологии при обучении? У большинства сотрудников компаний есть заблуждения, с которыми в обычной жизни трудно расставаться. И именно эти за-

ИДЕАЛЬНО, ЕСЛИ НОВАЯ ПЛАТФОРМА ОБУЧЕНИЯ ИБ СТАНЕТ ПРЕДМЕТОМ ОБСУЖДЕНИЯ В РАБОЧЕМ КОЛЛЕКТИВЕ. ЭТО НЕ ТОЛЬКО ПОВЫСИТ ИНТЕРЕС ОТДЕЛЬНЫХ СОТРУДНИКОВ К ВОПРОСАМ ИБ, НО И СКАЖЕТСЯ НА ОБЩЕЙ КУЛЬТУРЕ ИБ В КОМПАНИИ

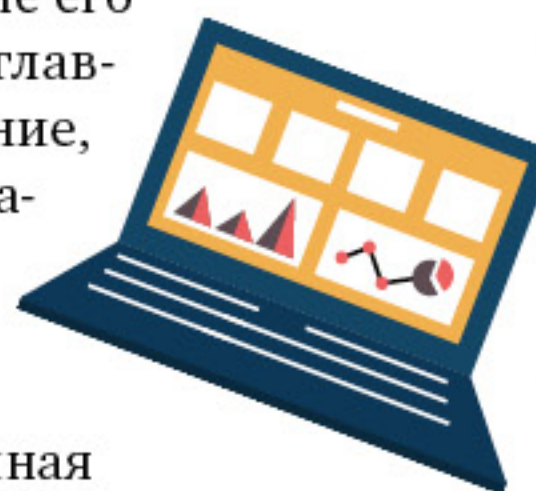
блуждения приводят к тому, что сотрудники не видят смысла в сознательном изучении основ кибербезопасности. Не видят смысла, а значит, не имеют никакой мотивации учиться. А раз не мотивированы, то и не учатся.

С помощью правильной мотивации можно сменить убеждения путем преобразования заблуждения по поводу кибербезопасности в адекватное восприятие реальности и позитивную модель поведения. Например, мнение, что хакеру неинтересны рядовые сотрудники, расслабляет при работе в сети. А понимание того, что страдают не только владеющие огромными деньгами и большими секретами, позволяет стать менее уязвимым. Страх, что хакеры сломают компьютер конкретного пользователя, можно преобразовать в понимание того, что хакеру намного интереснее данные, с которыми работает сотрудник или к которым он имеет доступ, а не его сломанная техника. И главное — сменить убеждение, что вопросы ИБ отнимают много времени в рабочем процессе, на то, что безопасность — это нормальная и естественная часть рабочего процесса. Вы же используете тормоза, когда едете куда-то? И тот факт, что это чуть-чуть удлиняет поездку, вас не смущает? Так же и с кибербезопасностью: несложные правила и принципы просто нужно встроить в свою работу, думать об этом, — а дополнительного времени это почти не займет. И — точно убеждает и вас самих, и всю компанию от больших и маленьких проблем, в том

числе чреватых потерей того самого, якобы сэкономленного времени.

Обучение по программе повышения осведомленности в сфере ИБ не должно быть разовой акцией. Это циклический процесс, в ходе которого проводится обучение с обязательным закреплением пройденного материала, при поддержке непосредственных руководителей и изучением дополнительных материалов по теме. После чего (или прямо в процессе!) можно провести оценку культуры кибербезопасности в организации и проверить уровень знаний на практике. Например, организовать симулированные фишинговые атаки на отдельно взятое подразделение или организацию в целом. По итогам тестовой проверки проводится оценка действий сотрудников и подразделений, делаются выводы, которые учитываются в следующем цикле обучения персонала и т.д. Возможные формы обучения я рассмотрел выше.

* * *



Что взять за основу обучающей платформы при внедрении программы осведомленности в сфере ИБ на предприятии — собственные наработанные практики или готовый коммерческий продукт, адаптированный под специфику организации при необходимости, — решать только менеджменту компании. АО «Лаборатория Касперского» создала свою обучающую платформу, распространяет ее на коммерческой основе, а также предоставляет консультативную поддержку по рекомендованным практикам и осуществляет техническую поддержку.

САМ СЕБЕ УЧИТЕЛЬ



Марина БРОДСКАЯ
обозреватель
BIS Journal

ЧТО ДЕЛАТЬ, ЕСЛИ ДУША
ТРЕБУЕТ ПЕРЕМЕН?
ЗАНЯТЬСЯ
САМООБРАЗОВАНИЕМ!

Самый простой способ получить знания и сертификат об окончании курса дополнительного образования по направлению информационной безопасности — пойти в учебный центр, коих можно много найти в любом городе, заплатить от 30 тыс. рублей за базовый курс и на неделю-две погрузиться в изучение новых дисциплин под руководством преподавателя. По окончании каждого курса можно сдать квалификационный экзамен и продолжить углубленное изучение разделов ИБ за дополнительную плату.

Другой способ получения новых знаний требует меньше финансовых и временных затрат, но больше силы воли и желания приобрести новые знания. В любом книжном магазине представлен большой выбор литературы по любым направлениям и вопрос только в том, чтобы купить действительно полезную книгу, а не перепечатку инструкции по установке и эксплуатации к какому-нибудь программному продукту, изданную под видом пособия по ИБ.

Любители электронных книг могут вообще сэкономить на покупке литературы и найти множество вариантов пособий «для чайников», которые часто выпускаются и распространяются

бесплатно при поддержке профильных компаний. Многие блогеры — специалисты в области ИБ — отслеживают выход подобных изданий и регулярно обновляют списки литературы, нередко сопровождая издания своими комментариями. Однако стоит учесть, что для чтения такой литературы стоит обладать минимальными знаниями английского языка и информационных технологий.

Также знания английского и информационных технологий потребуются тем, кто решит прослушать или прочитать в сети курсы лекций по дисциплинам, которые читаются в университетах мира, в том числе в Гарварде, Массачусетском технологическом институте или Университете Беркли. Хотя

можно начать и с отечественных вузов, многие из которых выкладывают курсы лекций по тем или иным дисциплинам, связанным с информационной безопасностью, на своих сайтах. Свои лекции и тестовые задания выкладывают в сеть и некоторые преподаватели региональных вузов. Но такие методические пособия хороши для изучения основ ИБ, поскольку лекции датированы 2003–2014 гг. и не актуализированы с учетом последних достижений хакеров и разработчиков средств защиты информации.

Если качество лекций по ИБ и криптографии, читаемых российскими преподавателями на основе отечественных методик, не устраивает, можно воспользоваться сайтами зарубежных университетов.



**ЭЛЕКТРОННАЯ БИБЛИОТЕКА СИСТЕМЫ
ФЕДЕРАЛЬНЫХ ОБРАЗОВАТЕЛЬНЫХ ПОРТАЛОВ**

В электронной библиотеке Системы Федеральных образовательных порталов в разделе «Информационно-коммуникационные технологии в образовании» в разделе «Информационная безопасность и защита компьютерной информации» собраны лекции, рабочие программы и учебные пособия, материалы конференций, которые представлены различными вузами, в том числе МГУ, СПбГУ, рядом региональных университетов и антивирусными компаниями.

www.ict.edu.ru/lib/

ПОРТАЛ «ИНТУИТ»

На портале «Интуит» Национального открытого университета размещен популярный у слушателей курс по основам ИБ Владимира Галатенко, а также порядка 40 курсов по основам информационной безопасности и криптографии, представленных различными университетами, компаниями и частными лицами. Самый свежий курс по «Криптографическим методам защиты информации» продолжительностью почти 22 ч. выложен в марте 2017 г.

www.intuit.ru

**КУРС 100W OPERATIONAL SECURITY (OPSEC)
FOR CONTROL SYSTEMS OF ICS-CERT**

Свои бесплатные курсы ИБ предлагает учебный центр ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) Департамента национальной безопасности США. Краткосрочный курс 100W Operational Security (OPSEC) for Control Systems посвящен общим вопросам ИБ: кто такие хакеры, какие техники получения критической информации они используют, какие основные способы защиты от хакерских атак существуют. Также предлагается пройти несколько тестов.

ics-cert.us-cert.gov

**КУРС 210W CYBERSECURITY FOR INDUSTRIAL
CONTROL SYSTEMS OF ICS-CERT**

Второй курс — 210W Cybersecurity for Industrial Control Systems состоит из 10 занятий по 1,5 ч каждое. Он затрагивает многие аспекты кибербезопасности для промышленных систем управления, включая основы безопасности, сравнительный анализ IT и архитектуры систем управления, уязвимости в системе безопасности, а также стратегий по предотвращению инцидентов. Слушатели изучают, какие кибератаки могут быть запущены на промышленном предприятии, почему они работают и какие стратегии для смягчения последствий и повышения кибербезопасности системы управления можно применить. По итогам курсов можно распечатать именной сертификат.

ics-cert.us-cert.gov

ЛЕКТОРИЙ МФТИ

На сайте «Лекторий МФТИ» представлен курс «Защита Информации», который состоит из 14 лекций. Его читает преподаватель кафедры радиотехники и телекоммуникаций С. М. Владимиров, а также два приглашенных лектора — И. Ю. Сысоев и А. И. Колыбельников. Курс предназначен для студентов 4-го курса ФРТК и 5-го курса ФАКИ МФТИ. В курсе рассматриваются математические основы криптографии, криптографические примитивы и их современные реализации, математические и прикладные криптографические протоколы, а также защита данных в современных информационных системах. Для успешного освоения курса желательно понимание основ теории групп и информатики.

lectoriy.mipt.ru

**ЛЕКЦИИ АМЕРИКАНСКИХ
УНИВЕРСИТЕТОВ**

На сайте Массачусетского технологического института (MIT) выложено несколько базовых курсов лекций по ИБ и криптографии для бакалавров и магистров. Лекции по интересующей нас тематике выложили Калифорнийский университет в Беркли, Университеты Вашингтона и Флориды, Университет Карнеги-Меллон и Университет Дрекселя.

MIT web.mit.edu

Калифорнийский университет в Беркли www.berkeley.edu

Университет Вашингтона
www.washington.edu

Университет Флориды
www.fsu.edu

Университет Карнеги-Меллон
www.cmu.edu

Университет Дрекселя
www.drexel.edu

Другой способ самообразования предлагают немногочисленные, но популярные у пользователей всего мира платформы онлайн-обучения. Самая известная подобная платформа — Coursera. Здесь по ключевым словам можно получить список всех курсов и лекций по интересующей теме. Платформа распознает IP-адрес и при запросе «информационная безопасность» выдает 26 ссылок на курсы как отечественных университетов (МФТИ, ВШЭ, МИФИ, Томский и Новосибирский госуниверситеты), так и на университеты Мичигана и Джорджии. При запросе «cybersecurity» список англоязычных курсов увеличивается на два десятка. А при запросе «information security» и уточнении запроса «компьютерные науки» появляется список из 136 англоязычных ресурсов — университеты США, Великобритании, разработки IBM и Google.

Большинство лекций и видеокурсов бесплатные, в подробном описании указаны требуемый уровень подготовки слушателя, сколько часов в неделю следует заниматься и что входит в промежуточную оценку знаний (проверочная работа, тест, диктант). А при выборе конкретного предмета указаны дата начала курса, продолжительность сес-

ПРИ ЗАПРОСЕ «INFORMATION SECURITY» И УТОЧНЕНИИ ЗАПРОСА «КОМПЬЮТЕРНЫЕ НАУКИ» ПОЯВЛЯЕТСЯ СПИСОК ИЗ 136 АНГЛОЯЗЫЧНЫХ РЕСУРСОВ — УНИВЕРСИТЕТЫ США, ВЕЛИКОБРИТАНИИ, РАЗРАБОТКИ IBM И GOOGLE

сии и расписание занятий. Привязка к датам занятий, с одной стороны, является минусом, а с другой, дисциплинирует. Тем более, что желание учиться может стать положительным фактором при запросе на финансовую помощь при оплате обучения, если такая есть.

Схожая с Coursera платформа Udey предлагает более 200 курсов по ИБ при запросе «cyber security». Курсы созданы как учебными центрами, так и простыми пользователями — специалистами в сфере защиты информации и расследовании киберпреступлений. На момент ознакомления с ресурсом цена за большинство курсов по акции составляла \$19.

А на платформе Udacity мне удалось найти всего один курс по основам ИБ, который читается студентам

всех курсов в Технологическом институте Джорджии, и введение в основы криптографии в рамках курсов Full Stack Web Developer Nanodegree Program.

В отличие от Udacity, на платформе edX выложено много курсов по разным направлениям информационной безопасности, от азов для начинающих до экономического обоснования сложных решений по ИБ. Многие курсы предназначены для самостоятельного изучения, другие проходят онлайн под руководством преподавателей. Занятия начнутся в апреле-августе 2017 г. Курсы представлены как американскими, так и европейскими университетами и техническими институтами. При желании по окончании действующих курсов можно получить сертификат, цена колеблется в зависимости от курса и его авторов и может составлять \$50–250 и выше.

Если по окончании самостоятельного изучения хотя бы одного из предложенных курсов вы поняли, что можете предотвратить любую хакерскую атаку или хотя бы защитить периметр домашней компьютерной сети, можете смело брать в руки детективы Джеймса Хедли Чейза и со знанием дела изучать методы действия хакеров середины прошлого века — как это сделано в одном из популярных у отечественных слушателей курсов по основам ИБ В.А. Галатенко. Найдете ли вы работу после самостоятельного изучения курсов по ИБ, зависит только от вас и потенциального работодателя. Но грамотность в этой области вы точно повысите.



КИБЕРБЕЗОПАСНОСТЬ В ШКОЛАХ: У НАС И У НИХ

ПОВЫШЕНИЕ КУЛЬТУРЫ ИБ И ПРОФОРИЕНТАЦИЯ — ГОСУДАРСТВЕННАЯ ЗАБОТА, А НЕ ДЕЛО ТОЛЬКО ОТДЕЛЬНЫХ ОРГАНИЗАЦИЙ

Начало 2017 года ознаменовалось развитием киберпротivостояния между США, странами Европы и Россией: стороны активно обвиняют друг друга в хакерских атаках. На этом фоне особый интерес вызывает сообщение о выделении средств на обучение британских школьников основам ИБ. Новостные агентства мира бурно обсуждали планы правительства Великобритании готовить квалифицированные кадры для работы в сфере кибербезопасности со школьной скамьи.

У НИХ

14 февраля 2017 г. королева Елизавета II официально открыла новый Центр национальной кибербезопасности Великобритании (NCSC) в Лондоне, он стал подразделением Центра прави-

тельственной связи страны. Фактически центр заработал еще 3 октября 2016 г., он был образован путем слияния трех ведомств — Группы безопасности в электронике и связи (CESG), CERT-UK и Центра кибероценки (Centre for Cyber Assessment). NCSC возглавил Кириан Мартин, под его руководством работают порядка 700 человек.

Накануне официального открытия Центра Кириан Мартин заявил, что обеспокоен увеличением кибератак против британских компаний и правительственных учреждений с целью кражи секретных материалов, научных разработок и персональных данных жителей страны. Чтобы решить проблему нехватки квалифицированных кадров в сфере информационной безопасности, по инициативе NCSC в британских школах появятся уроки кибербезопасности, на которых будут

искать будущих экспертов для защиты государства от хакерских атак.

Можно только гадать, что стало триггером для запуска программы по вовлечению талантливых школьников в сферу информационной безопасности: действительная нехватка квалифицированных кадров или итоги расследования мощной DDoS-атаки на телекоммуникационную компанию TalkTalk, которая произошла в конце 2015 г. Злоумышленники успели похитить персональные данные 4 млн клиентов компании, акции TalkTalk упали на 10%. Общие потери оператора составили около 35 млн фунтов.

Как бы то ни было, на пятилетнюю программу правительство Великобритании готово выделить до 20 млн фунтов. По данным сайта NCSC, в рамках Национальной школьной программы будут отобраны шесть тысяч учеников в возрасте от 14 до 18 лет, которые хотят связать свою жизнь с информационной безопасностью. По итогам обучения они получают право работать в сфере ИБ.

Для не определившихся с выбором профессии Центр национальной кибербезопасности предлагает 11–14-летним школьникам записаться на однодневные курсы, 14–15-летним подросткам — на четырехдневный вводный курс по ИБ, где они получают базовые знания и понятия по защите компьютеров и небольших сетей. А для ребят 15–16 лет, желающих в перспективе углубленно изучать информатику, разработаны пятидневные курсы, на которых студенты узнают об основных угрозах кибербезопасности для устройств, приложений и программного обеспечения, а также о способах их защиты. Подробная информация о курсах и сро-



Королева Елизавета II открывает новый Центр национальной кибербезопасности Великобритании (фотография с сайта ncsc.gov.uk)

Отдельный пункт программы — привлечение женщин в сферу ИБ. Онлайн этап первого конкурса для девушек 13–15 лет CyberFirst Girls Competition 2017 прошел в начале марта 2017 г. В нем могли принять участие девочки, объединившиеся в команды по четыре человека. Им предложены тесты на логику, кодирование, создание сетей и криптографию. Десять самых сильных команд встретятся в очном поединке в Лондоне. Победители получат компьютерное оборудование для своей школы стоимостью 1000 фунтов, а каждая из девушек будет награждена ценным призом. Таким образом, NCSC хочет привлечь девушек на работу в сферу ИБ. По оценкам экспертов, среди специалистов ИБ в США работают до 10% женщин.

ках их проведения доступна на сайте ведомства. Отдельно отмечается, что курсы будут бесплатными и пройдут в учебных заведениях по всей стране.

Помимо поддержки и профориентации школьников, NCSC проводит активную работу с университетами, преподавателями, научными кругами и промышленными предприятиями, где требуются квалифицированные специалисты по ИБ. Каждый бакалавр или магистр может подтвердить свою квалификацию специалиста по ИБ в центрах сертификации GCHQ. Для этого университет должен подать заявку в определенной форме до указанного срока. Оказывается поддержка и аспирантам и докторам наук, которые ведут научные исследования в области кибербезопасности, а также тем, кто занимается стартапами в сфере ИБ.

Впрочем, NCSC, предлагая ввести кибербезопасность в Национальную школьную программу, не стал первооткрывателем ИБ-направления в средних учебных заведениях. Подобные программы давно работают в Израиле, однако пока редки в Европе.

Еще в 2015 г. учителя и полицейские в Шотландии организовали курсы ИБ для школьников (первые подобные занятия для учеников в Европе) в надежде, что они расскажут дома об опасностях, с которыми можно столкнуться в глобальной сети. Инициативу шотландцев поддержал даже премьер-министр Великобритании Дэвид Кэмерон.

Академия Кайл (Kyle Academy) в Эйр организовала курсы для учеников средней школы, детей научили распознавать проблемы информационной безопасности, которые могут привести

к серьезным преступлениям. Таким образом — через просвещение — учителя и поддержавшая их инициативу Полиция Шотландии начали борьбу с киберпреступностью.

Первый курс обучения длился 10 недель, в его рамках школьники должны были рассказать дома о кибербезопасности родителям и проэкзаменовать их.

Полиция предоставила школьникам реальные практические исследования киберпреступлений, в частности, серии примеров вымогательства в Интернете, а также научила детей, как с этим бороться. Курсы оказали большое влияние на учеников и их родителей: они узнали, как хакеры организуют целевые атаки на компании Шотландии, что пароли к сетевым ресурсам интересны не только родственникам и друзьям. За счет того, что школьники рассказали родным и знакомым об основных правилах кибербезопасности, эффект от курса многократно увеличивался. А учитывая тот факт, что это малонаселенный район, где нет отделений банков и жители пользуются исключительно онлайн-банкингом, польза от таких занятий была значительной.

Опыт жителей графства планировали перенять школы других регионов.

У НАС

Как проходит просвещение в сфере кибербезопасности и профориентация школьников в России? Если исключить специализированные классы с уклоном в информатику и ИКТ, то согласно Федеральным государственным образовательным стандартам, информационной безопасности уделяется по 1–2 часа в 7 и 9 классах, часть информации по ИБ дается в виде дополнительных сведений при изучении других тем или в формате общения посредством интернета с учителями по другим предметам, которым методисты предлагают наладить контакты со школьниками через соцсети и электронную почту. Основная же часть просветительской работы проходит в виде акций.

Всякий, кто знаком с российской действительностью, помнит об особой озабоченности некоторых членов Федерального собрания РФ вопросами защиты детей и подростков от негативной информации в глобальной сети. Созданные при покровительстве этих государственных деятелей и финансовой поддержке профильных министерств и ведомств некоммерческие компании активно сражаются с детской порнографией, ежегодно проводят разовые акции в формате Единого урока кибербезопасности в сети или сетевых викторин и олимпиад для дошкольников и учащихся 1–11 классов.

Вот только беда в том, что акции эти разовые и зайти на сайт одной международной олимпиады, проводящейся при солидной поддержке правительства, нескольких министерств и Совета Федерации РФ, чтобы посмотреть вопросы прошлых лет, спустя несколько месяцев по окончании мероприятия, мне не удалось. А жаль, хотелось бы узнать, как обстоят дела на самом деле. Стоит отметить, что еще один участник

**ПО ИНИЦИАТИВЕ NCSC
В БРИТАНСКИХ ШКОЛАХ ПОЯВЯТСЯ
УРОКИ КИБЕРБЕЗОПАСНОСТИ,
НА КОТОРЫХ БУДУТ ИСКАТЬ
БУДУЩИХ ЭКСПЕРТОВ ДЛЯ ЗАЩИТЫ
ГОСУДАРСТВА ОТ ХАКЕРСКИХ АТАК**

такой акции по просвещению школьников — крупная IT-компания, которая не живет на гранты, — не закрывает свои сайты и любой желающий после регистрации может попробовать свои силы или пройти онлайн-обучение.

На практике школьные сайты пестрят формальными отчетами о проведенных уроках безопасности в сети Интернет, направленных на повышение уровня кибербезопасности и развитие цифровой грамотности. Ученикам рассказывают о пользе и вреде современных технологий, правилах поведения в соцсетях и видах онлайн-мошенничества. Дополнительно проводят уроки, опросы и тесты для старшеклассников, конкурсы рисунков и эссе для учеников помладше. Насколько актуальна эта информация для учеников отдаленных школ, где интернет бывает по праздникам, или для продвинутых в техническом отношении школьников, которые на досуге занимаются созданием сайтов и программированием?

Хорошо, что многое зависит не только от указаний сверху, но и от самих учителей. В поисках материала для статьи, я нашла симпатичный пример урока по информационной безопасности для 2 класса в рамках предмета «Окружающий мир». Составивший его учитель хорошо понимает, что школьники

В РОССИИ, СОГЛАСНО ФЕДЕРАЛЬНЫМ ГОСУДАРСТВЕННЫМ ОБРАЗОВАТЕЛЬНЫМ СТАНДАРТАМ, ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УДЕЛЯЕТСЯ ПО 1–2 ЧАСА В 7 И 9 КЛАССАХ. ОСНОВНАЯ ЖЕ ЧАСТЬ ПРОСВЕТИТЕЛЬСКОЙ РАБОТЫ ПРОХОДИТ В ВИДЕ АКЦИЙ

только начинают осваивать Интернет, и в доступной для детей форме рассказывает не только о пользе и преимуществах глобальной сети, поиске информации, правилах безопасного поведения в соцсетях, но и об опасностях при общении с незнакомцами, о вирусах и антивирусных программах и т.д. По итогам урока дети должны запомнить, что не стоит работать без установленного на компьютер антивируса, не стоит всем раздавать свои персональные данные и фотографии, скачивать неизвестные файлы и открывать письма от неизвестных отправителей. А в непонятных случаях стоит обратиться к родителям.

Старшеклассникам в рамках курса «Информатика» предлагают обсу-

дить такие вопросы как кража личных данных и утечка информации; вирусы, черви, трояны; спам; хакерские атаки; мошенничество; дезинформация; авторское право и нелегальное программное обеспечение. Цель этих уроков — расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков.

Самые продвинутые преподаватели предлагают учащимся 10 класса презентацию по ИБ, которая включает основные понятия кибербезопасности и угроз, классификацию противников и программно-технические средства ИБ, такие понятия как шифрование и аутентификация. Но такие уроки — исключение из ставших привычными стандартных наборов определений и правил, которыми ограничиваются обычные учителя информатики.

Если же в целом оценивать отечественную программу просвещения школьников (и их родителей) в области ИБ, то можно сказать одно — она не носит системного характера, а проходит в виде всевозможных, чаще формальных, акций, бонусы от которых получают заинтересованные в своем дальнейшем существовании структуры. А хорошо бы, изучив опыт Великобритании, создать свою национальную программу по просвещению подрастающего поколения (а также родителей и бабушек-дедушек) основам информационной безопасности. И еще со школьной скамьи проводить профессиональную ориентацию и выбирать лучших.



Урок кибербезопасности в московской школе

ШИФРЫ ТРЕХ ВОЙН

О МАСТЕРЕ ВЗЛОМА КОДОВ
Б. А. АРОНСКОМ



Дмитрий ЛАРИН
кандидат
технических наук



Геннадий ЕМЕЛЬЯНОВ
член-корреспондент
Академии криптографии РФ

В предыдущих номерах нашего журнала мы рассказали о криптографической деятельности С.С.Толстого. Еще одним замечательным специалистом, внесшим значительный вклад в победу под Москвой и дальнейшие успехи нашей дешифровальной службы во время Великой Отечественной войны, был Б.А.Аронский, под руководством которого были вскрыты немецкие дипломатические коды.

ИЗ ЮНКЕРОВ...

Борис Алексеевич Аронский (1898–1976) родился 25 (12) апреля 1898 года в Москве в семье служащего. С 1907 года он учился и в 1916-м окончил одним из лучших учеников Московскую Практическую Академию Коммерческих наук (так в те годы именовалось одно из средних учебных заведений).

В мае 1917 года Б.А.Аронский был призван на военную службу и направлен в Петергофскую (юнкерскую) Школу прапорщиков. После Октябрьской революции учебное заведение расформировали, и он вернулся в Москву.

В 1918 году Борис Алексеевич был призван в Красную Армию и направлен на военно-хозяйственные курсы. После их окончания с 1918 по 1922 гг. проходил службу в системе военных комиссариатов Поволжья и Урала, где познакомился с криптографической деятельностью. Также в 1918 году во время широкого набора Б.А.Аронский вступил в ряды РКП(б), но в 1921 году во время «большой чистки» был ис-



Б.А.Аронский,
6 октября 1917 года

ключен из рядов коммунистической партии как бывший юнкер. Однако данный эпизод не помешал развитию карьеры.

...В ПОЛИГЛОТЫ И ВЗЛОМЩИКИ

В 1922 году он был откомандирован на службу в Спецотдел ВЧК. Подробнее о рождении и развитии советской криптографической службы можно прочитать в статье [Емельянов, 2016].

Постоянно заботясь о своём самообразовании, Аронский стал знатоком русской и западной литературы. Успешной работе в Спецотделе способствовали выдающиеся лингвистические

способности — в процессе работы он овладел французским, английским, немецким, итальянским, финским, японским и другими языками. При этом следует отметить, что эти знания были специфическими — Борис Алексеевич в совершенстве знал язык и стиль дипломатической переписки, что в сочетании с природным аналитическим даром сделало его блестящим специалистом по взлому кодов. Под кодом криптографы понимали весьма распространенный шифр, представляющий собой обширный словарь, в котором каждому слову, знаку препинания или даже устойчивой группе слов приданы кодовые обозначения.

В 1930-е годы Аронский вскрыл ряд кодов иностранных государств. Вот что об этом писал ветеран советской криптографической службы Л.А.Кузьмин: «Дешифрование кода — работа чрезвычайно сложная и трудоёмкая. Она предполагает тщательный отбор по внешним признакам



Семья Аронских, 1915 год. Во втором ряду слева юный Борис



Группа сотрудников одного из советских военных комиссариатов, 1920 год. Крайний справа Б.А.Аронский



Б.А.Аронский, 1920-е гг.

из массы шифрперехвата комплекта криптограмм, относящихся к данному коду, затем проведение очень скрупулезного статистического анализа, который должен отразить частоту появления, места и «соседей» каждого кодобозначения во всём комплекте. В связи с отсутствием в те годы специальной техники всё это делалось вручную несколькими помощниками основного криптографа-аналитика. Тем не менее, многомесячная работа такого коллектива зачастую приводила к аналитическому вскрытию значительной доли содержания кодовой книги и возможности оперативного чтения очередных перехваченных кодированных телеграмм. Это и определило успех группы Аронского, сыгравшей огромное значение в исходе битвы за Москву» [Кузьмин, 1998, с. 84].

БОЕВОЕ КРЕЩЕНИЕ

Во время гражданской войны в Испании (1936–1939 гг.) дешифрование сообщений франкистов велось в Москве под руководством Б.А.Аронского. Вот лишь один из примеров их успешной работы. Из дешифрованной телеграммы советским специалистам стало известно о том, что франкисты намерены потопить советский корабль, который должен был выйти из Марселя в один из испанских портов. На борту этого судна находились советские лётчики, танкисты и другие военные специалисты, а также бойцы интербригад, следовавшие на помощь республиканцам. Франкисты собирались выделить для перехвата этого корабля значительные силы флота и авиации. Сведения об этом были переданы капитану советского корабля, его выход из Марселя был задержан, а маршрут изменён. Так благодаря работе советских дешифровальщиков судну удалось благополучно добраться до порта назначения [Гольев, 2008], [Ларин, 2008], [Соболева, 2002].

Война в Испании стала боевым крещением советских криптографов. Помимо группы Б.А.Аронского, работавшей в Москве, ряд специалистов был командирован непосредственно в район боевых действий. Среди направленных в Испанию советских специалистов была группа криптоана-

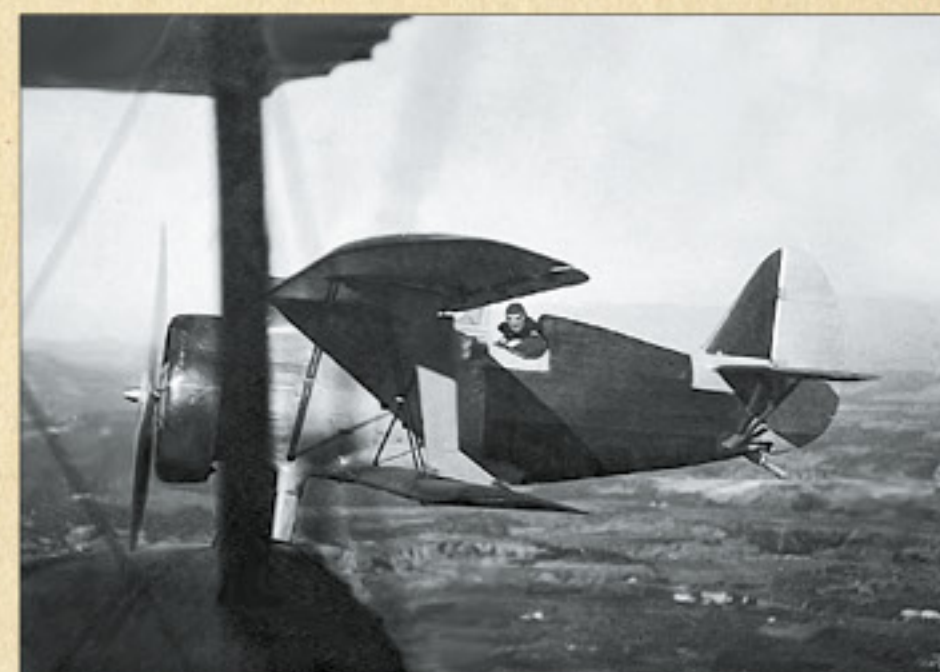
литиков (З.В.Березин, Г.К.Муха, Ф.М.Огарышев) [Соболева, 2002] и радиоразведчиков (А.Берсенов, В.Мухин, В.Плошай, Н.Прахин, В.Салин, Н.Шмырев, А.Юрьян). На замену им в последующие годы прибывали А.Анисимов, В.Ефремов, Е.Коссовский, В.Маркович, В.Модебадзе, Л.Сазыкин, И.Уханов. Вместе с радиоразведчиками и криптографами работали переводчицы З.Антонюк, Н.Павлова, Ц.Покровская [Болтунов, 2011]. Был организован перехват шифрпереписки испанских мятежников и итальянского корпуса, прибывшего на помощь генералу Франко. Весьма ценной была информация, добытая нашими специалистами об аэродромах, на которых базировалась вражеская авиация, в том числе немецкий легион «Кондор», включавший в себя несколько истребительных, бомбардировочных эскадрилий и эскадрилий самолетов-разведчиков, гидросамолетов и т.п.

Эти данные оперативно докладывались в штабы республиканского командования и советским военным советникам. Надо сказать, что информация, добытая радиоразвед-

ВОЙНА В ИСПАНИИ СТАЛА БОЕВЫМ КРЕЩЕНИЕМ СОВЕТСКИХ КРИПТОГРАФОВ. ПОМИМО ГРУППЫ Б.А.АРОНСКОГО, РАБОТАВШЕЙ В МОСКВЕ, РЯД СПЕЦИАЛИСТОВ БЫЛ КОМАНДИРОВАН НЕПОСРЕДСТВЕННО В РАЙОН БОЕВЫХ ДЕЙСТВИЙ



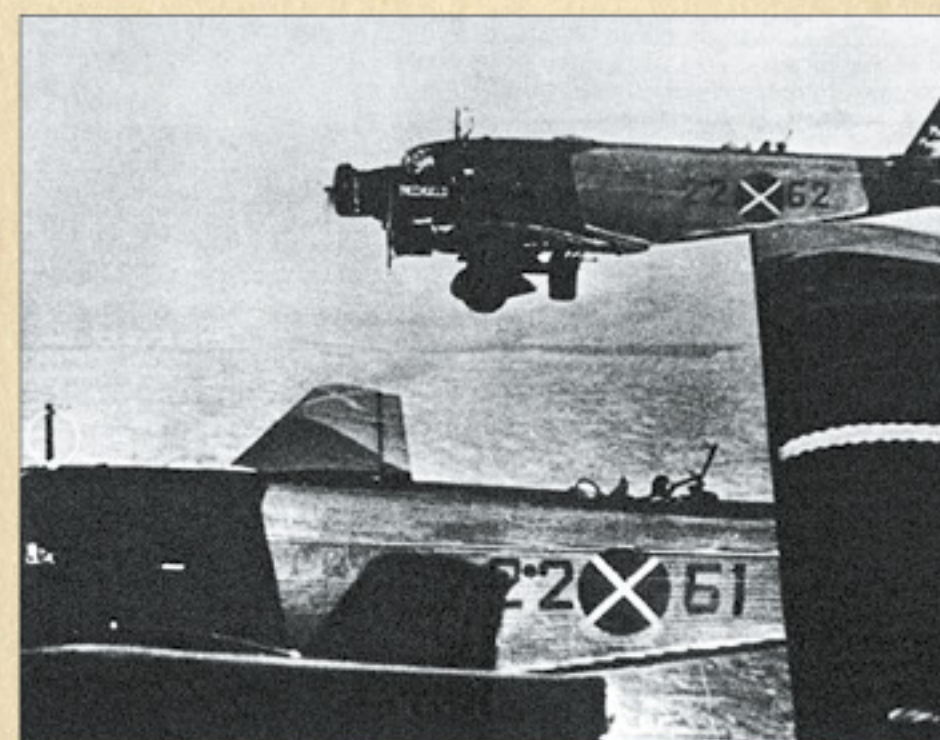
Антифранкистский лозунг на улице Мадрида, 1937



Истребитель И-15 ВВС Испанской республики



Итальянский бомбардировщик SM.81



Немецкий бомбардировщик Юнкерс Ю 52

кой, использовалась весьма эффективно. Помимо войсковой информации, серьезное внимание уделялось работе с агентурными шифрами мятежников. Советские дешифровальщики вскрыли код агентурной сети франкистов, и в результате этой работы была осуществлена ликвидация ряда вражеских агентурных сетей [Соболева, 2002].

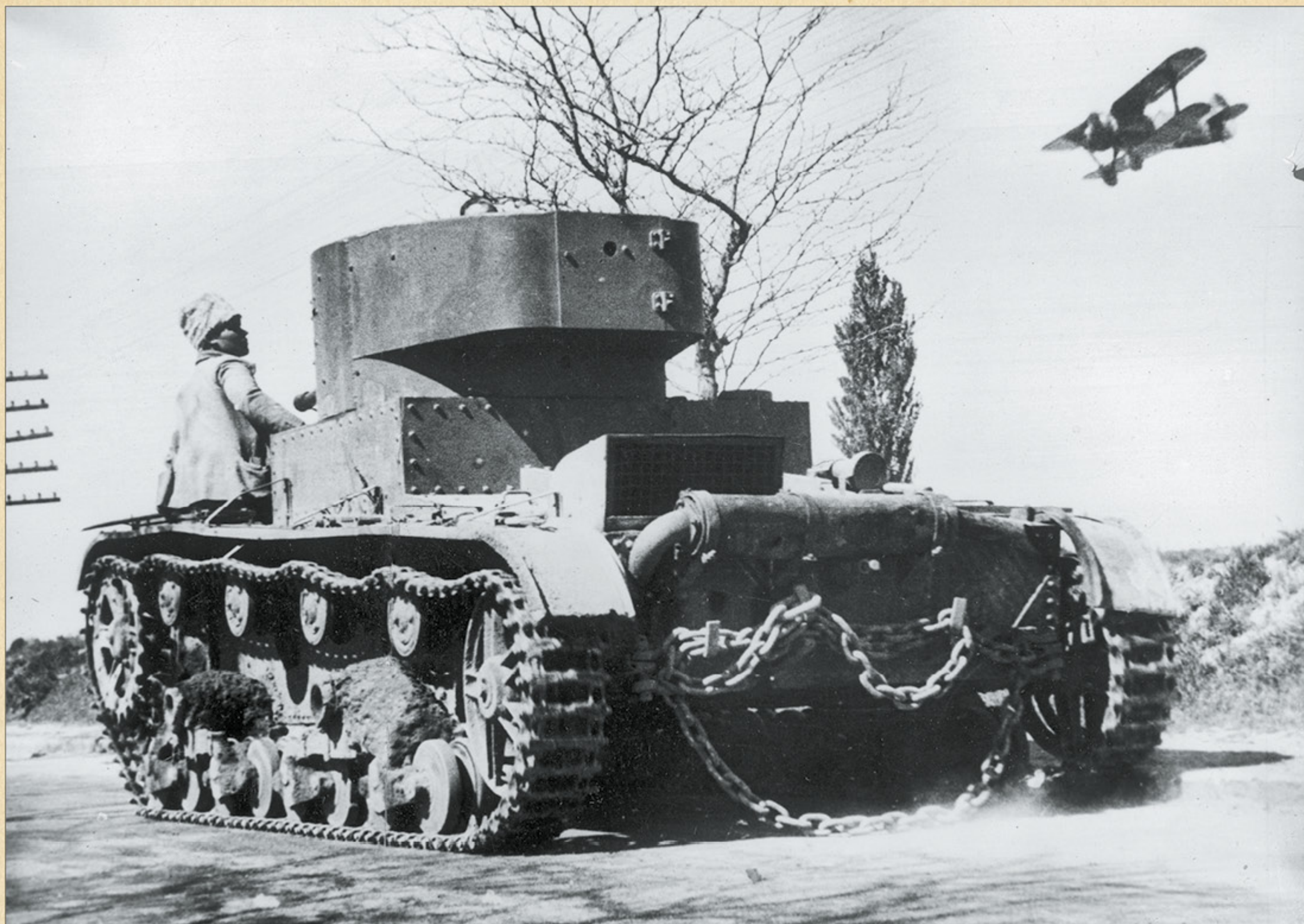
В НЕБЕ ИСПАНИИ

Приведем примеры успешных операций республиканцев, важную роль в которых сыграли советские радиоразведчики и дешифровальщики. Успешно действовали наши радиоразведчики и криптографы и против вражеской авиации не только на аэродромах, но и в воздухе. О предстоящих налетах вражеских бомбардировщиков радиоразведка сообщала за 20–30 минут до подхода самолетов к объектам, расположенным на морском побережье [Болтунов, 2011]. Перехватывая и дешифруя радиопереговоры штабов соединений вражеских ВВС, советские специалисты почти сразу полу-

чали точную информацию о времени вылета и маршрутах следования франкистских, итальянских и немецких самолетов. Это сразу сказалось на результатах воздушных боев, несмотря на численное превосходство вражеской авиации. Уже 4 ноября 1936 года советские истребители И-15 сбили без потерь 7 самолетов противника. 6 ноября, в день начала генерального наступления войск Франко на Мадрид, советские истребители сбили 9 самолетов врага и снова не потеряли ни одного. Советские и испанские пилоты точно знали время и маршруты следования самолетов противника. Они могли разрабатывать стратегию нападения, наносить удары по врагу и поэтому быть совершенно неуязвимыми для него.

Позднее в бой вступили новейшие советские истребители И-16, которые навели еще больший ужас на противника.

Таким образом, в конце 1936 года с господством авиации мятежников было покончено. Более того, пилоты советских истребителей, заранее получив информацию от советских радиоразведчиков и криптоаналитиков, атаковали идущие



Танк Т-26 Испанской республики. В небе виден самолёт И-15

на бомбардировку «Юнкерсы» и «Савойи» франкистов и их немецких и итальянских союзников, которые даже не решились продолжать выполнение задания, столкнувшись с нашими и испанскими пилотами. Они бросились удирать от наших истребителей, не понимая, как самолеты, воюющие на стороне республики, могли так точно определить господствующее для атаки положение [Клепов, 2009]. Подробно о воздушных боях в небе Испании можно прочитать в книге [Абросов, 2003].

В МАДРИДЕ И ГВАДАЛАХАРЕ

Весьма серьезным достижением наших криптоаналитиков было установление точного места, где войска франкистов планировали нанести удар по Мадриду. Время и место было точно указано в перехваченном и дешифрованном сообщении, информация была своевременно доложена руководству Испанской республики. Республиканская армия заранее перебросила туда свои резервы, включая новые на тот момент советские танки Т-26.

Располагая точными сведениями, полученными от наших радиоразведчиков и криптографов, республиканская армия почти окружила войска франкистов. Битва за Мадрид оказалась в целом неудачной для Франко. Оборона испанской столицы наглядно показала, что знание планов противника,

добываемых дешифровальщиками и агентурной разведкой, позволяет и с малыми силами вести успешные военные действия. [Клепов, 2009].

Еще одним успехом республиканских войск стала Гвадалахарская операция. В начале марта 1937 года мятежниками был разработан план захвата Мадрида. Теперь они решили вести штурм города с северо-востока. Но для этого следовало первоначально захватить Гвадалахару — столицу одноименной провинции в пятидесяти километрах от Мадрида. Основную роль в этой операции должны были играть итальянские дивизии. Советские специалисты выявили планы противника по проведению операции и лишили его возможности использовать фактор внезапности. Итальянцы и франкисты понесли большие потери [Клепов, 2009].

В целом отметим, что в результате работы наших связистов, криптографов и радиоразведчиков республиканское командование получило важные сведения о планах военных действий франкистов, их итальянских и немецких союзников, численности и составе их войсковых группировок, базах и путях снабжения и т.д. В свою очередь советские и республиканские линии связи были надежно защищены от врага. Наши специалисты закончили свою работу в Испании в начале 1939 года и по возвращении в СССР были награждены ценными подарками.

«РЯДОВОЙ СПЕЦ»

Вернемся к биографии Б.А.Аронского. Как известно, в 1937–38 годах волна репрессий prošлась и по сотрудникам НКВД. Борис Алексеевич по воспоминаниям Л.А.Кузьмина рассказывал, что «эта участь миновала его по-видимому потому, что в то время он не являлся членом ВКП(б), а был всего лишь «рядовым спецом». В партию же он вступил только в тяжёлое время войны» [Кузьмин, 1998, с. 84].

В 39–40 годах Аронский участвовал в советско-финской войне. За боевые заслуги он был награжден орденами Красного Знамени и Знаком Почета, а во время Великой Отечественной — дважды орденом Ленина и орденом Трудового Красного Знамени.

Трудно переоценить заслуги Б.А.Аронского и в Великой Отечественной войне. В первые же дни, при помощи своих помощников и переводчиков, он дешифровал кодированные донесения Германии и послов ряда ее союзников. По поручению императора Японии послы докладывали своим правительствам о том, что Япония уверена в скорой победе над Россией, но пока сосредотачивает свои силы на юге Тихого океана против США. Чуть позже эта информация была подтверждена в донесениях советского разведчика Рихарда Зорге. Основываясь на этих данных, Сталин принял решение о переброске дальневосточных и сибирских дивизий под Москву. Эти войска определили успех в исходе битвы за Москву [Анин, 1996], [Кузьмин, 1998].



Б.А.Аронский,
старший лейтенант
госбезопасности,
1939 год

ТРУДНОЕ СЧАСТЬЕ

Напряженный труд работников дешифровальной службы в годы войны был высоко отмечен партией и правительством. В газете «Правда» № 94 (8865) от 4 апреля 1942 года был опубликован Указ Президиума Верховного Совета СССР «О награждении работников НКВД Союза ССР за образцовое выполнение заданий Правительства» от 3 апреля 1942 года. 54 специалиста были награждены орденами и медалями. В том числе орденом Ленина награждены два капитана государственной безопасности Аронский и Толстой, орденом Трудового Красного Знамени 6 человек, орденами Красной Звезды и «Знак почета» — 13

человек и медалями «За трудовую доблесть» и «За трудовое отличие» — еще 33 человека. Так советское правительство оценило вклад дешифровальщиков в победу под Москвой [Кузьмин, 1998–1, с. 83].

Позже Борис Алексеевич рассказывал, что работал в те годы неделями без сна и отдыха и был счастлив, поскольку своим трудом добывал материалы, нужные Верховному командованию для организации победы над фашизмом. В 1943 году Б.А.Аронский принимал участие в подготовке молодых специалистов для криптографической службы СССР. Окончил войну начальником отдела 5 Управления НКГБ СССР.

(Окончание в следующем номере)

ЛИТЕРАТУРА

1. [Абросов, 2003] Абросов С.В. В небе Испании 1936–1939. М., 2003.
2. [Анин, 1996] Анин Б.А., Петрович А.И. Радиошпионаж. М., «Международные отношения», 1996.
3. [Болтунов, 2011] Болтунов М.Е. «Золотое ухо» военной разведки. М.: Вече 2011. // <http://read24.ru/fb2/mihail-boltunov-zolotoe-uh-voennoy-razvedki/>
4. [Бутырский, 2012] Бутырский Л.С., Ларин Д.А., Шанкин Г.П. Криптографический фронт Великой Отечественной. Монография. М.: Гелиос АРВ, 2012. 2 изд. исправл. и дополн. М. 2013.
5. [Гольев, 2008] Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008.
6. [Емельянов, 2016] Емельянов Г.В., Ларин Д.А. Рождение советской криптографии // Информационная безопасность банков, № 2 (21) 2016, с. 61–65, № 3 (22), 2016 с. 74–79.
7. [Зубов, 2013] Зубов А.Ю., Зязин А.В., Никонов Н.В., Рамоданов С.М., Фролов А.А. Олимпиады по криптографии и математике. М.: МЦНМО, 2013.
8. [Клепов, 2009] Клепов А. Информационное оружие Сталина // www.proza.ru/2009/06/17/949
9. [Кузьмин, 1998–1] Кузьмин Л.А. Не забывать своих героев // Защита информации. Конфидент № 1, 1998, с. 83–85.
10. [Кузьмин, 1998–2] Кузьмин Л.А. ГУСС — этап в развитии советской криптографии // Защита информации. Конфидент. № 4, 1998, с. 89–94.
11. [Ларин, 2008] Ларин Д.А., Шанкин Г.П. Криптографическая деятельность во время гражданской войны в Испании. // Защита информации. INSIDE. № 1, 2008, с. 62–64.
12. [Органы, 1995] Органы государственной безопасности СССР в Великой Отечественной войне 1941–1945. Сборник документов. М.: «Русь» 1995. Издание подготовлено в Академии ФСБ России. <http://mosohin.ru>
13. [Соболева, 2002] Соболева Т.А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.
14. [Энциклопедия, 2004] Энциклопедия секретных служб России. М.: Астрель, 2004.
15. [agentura] <http://www.agentura.ru>
16. [kosino] kosino-uh-tomski.vaonews.ru/2p=6155
17. [v-olymp] v-olymp.ru
18. [vif2ne] <http://vif2ne.ru>

ЗАЩИТА СЕГОДНЯ — ШАГ В БЕЗОПАСНОЕ ЗАВТРА

Стратегические решения в сфере IT-безопасности

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 «АРинтер») - Platinum Partner «Лаборатории Касперского». Компания ARinteg предоставляет полный комплекс услуг в области защиты информационных ресурсов.
www.ARinteg.ru



kaspersky.ru/corporate

СТО ЛЕТ НАЗАД



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

ТРИУМФ И ТРАГЕДИЯ РАДИОРАЗВЕДКИ БАЛТИЙСКОГО ФЛОТА

В наступившем 2017 году есть немало поводов задуматься о прошедших событиях вековой давности. Вероятно, прежде всего, вспоминаются Первая мировая война 1914–1918 годов и Революция. Но ведь это было время решительных перемен и в организации криптографической деятельности: очень скоро началась эпоха криптографии шифровальных машин. И старт новой эпохи в криптографии, безусловно, был ускорен мировой войной.

ВОЙНА В ЭФИРЕ

По существу, тогда заявил о себе новый, тайный фронт между противоборствующими державами. Пожалуй, особенно

ярко новый фронт проявился в войне на море, где не было колющей проволоки, разделяющей противников. Как же происходили сражения на тайном фронте? Полемикой, источником побед и поражений стал радиоэфир.

ДО ШИФРОВАЛЬНЫХ МАШИН

Надо сказать, что ВМФ противоборствующих государств использовали при организации связи в основном кодирование посредством кодовых книг с последующим шифрованием сообщения, в случае необходимости его засекречивания [1, 2]. Кодовая книга не являлась собственно шифром, а использовалась для формализации содержания передаваемых сообщений. Отдельные слова, фразы, числа из пер-

воначального текста (так называемые словарные величины) заменялись на условные обозначения (кодовые величины). Это позволяло уменьшить общий объем передаваемого сообщения и сделать его удобным для передачи любыми корабельными средствами — семафором, телеграфом или по радио. Полученный таким образом текст из буквенных групп (для буквенных кодов) или из цифровых групп (для цифровых кодов), при необходимости его засекречивания подвергали шифрованию. Следует отметить, что слабость самих словарных кодов с точки зрения засекречивания сообщений прекрасно понимали ещё в XIX веке. Поэтому при передаче секретных сведений радиодиаграмма, составленная по кодовой

книге, дополнительно «закрывалась» каким-либо шифром. Для этого обычно использовали шифр простой (взаимнооднозначной) замены и уже в таком виде сообщение передавали в эфир.

Слабость подобного шифрования стала особенно заметной с началом Первой мировой войны с её массовым применением засекречивания связи и активным внедрением радиосвязи в морские сообщения. При этом следует признать, что использование в столь сложных условиях более надёжных, но и более трудоёмких в применении криптографических средств тогда не представлялось возможным, так как шифрование и расшифрование переписки осуществлялось вручную. Заканчивался период ручной криптографии, шифровальных машин в тот период ещё не было. Шифровальные машины, начавшие своё распространение уже в 20-е годы XX столетия, как раз продемонстрировали учёт опыта минувшей войны. Так созрел переход к периоду машинной криптографии.

ПЕРВОРОДНЫЙ ХАОС

Но в 1914–1918 годах дешифровальщики имели явное преимущество перед связистами, обеспечивающими засекреченную связь. Особенно это стало заметно в радиосвязи, где каждый владелец чувствительного приёмника мог вести перехват шифрованных радиопередач. Огромный объём шифр-перехвата, неотлаженный порядок работы связистов в сетях засекреченной связи, многочисленные ошибки и прямые нарушения режима шифрованной переписки не только открыли перед криптографами-дешифровальщиками новые возможности, но и привели к мысли об использовании для взлома шифра всего связанного с ним массива информации, а не одной лишь шифротелеграммы. Так начинался современный криптоанализ.

СЧАСТЛИВЫЙ СЛУЧАЙ

Среди ярких эпизодов криптографической деятельности 1914–1918 годов особенно заметна по своим впечатляющим последствиям «магдебургская» история, начавшаяся в туманную балтийскую ночь на 26 августа 1914 года. Эти последствия давно по достоинству

оценены исследователями, так, американский историк криптографии Д. Кан назвал их «самой счастливой удачей во всей истории криптоанализа» [3].

Вполне разделяя такой взгляд, добавим лишь, что удача досталась тем, кто был к ней готов, и приведём подробности происшедшего.

В ту ночь германские крейсера «Аугсбург» и «Магдебург» под прикрытием трёх эскадренных миноносцев предприняли попытку напасть на русский дозор в устье Финского залива. Однако в условиях сильного тумана крейсер «Магдебург» выскочил на камни у острова Оденсхольм. Попытки сняться с мели успехом не увенчались и был отдан приказ об эвакуации экипажа [4].

Инцидент произошёл недалеко от русского наблюдательного поста, который своевременно сообщил по телефону начальнику Службы связи Балтийского флота, что явственно слышна немецкая речь и шум машины. По приказанию командующего Балтийским флотом адмирала Н. О. Эссена к месту аварии были направлены эсминцы «Лейтенант Бураков» и «Рьяный» с начальником Службы связи капитаном 1-го ранга А. И. Непениным, а также дежурные крейсера «Богатырь» и «Паллада».

Их быстрое появление у Оденсхольма помешало выполнить эвакуацию «Магдебурга». Уже под огнём русских крейсеров миноносцу V-26 удалось снять часть экипажа «Магдебурга» и уйти, получив на отходе прямое попадание в кормовую часть. Некоторое время «Магдебург» отвечал огнём из своих орудий, но после отхода миноносца прекратил сопротивление [1]. Большая часть оставшихся на германском крейсере моряков в панике бросилась вплавь на берег. О секретных документах в суматохе, видимо, забыли. Посланный на «Магдебург» лейтенант М. В. Гамильтон вместе с немецкими матросами спустил флаг крейсера, поднял Андреевский флаг и послал одного из немецких матросов доложить командиру о прибытии русских. Вот как он описывал дальнейшее в своих мемуарах: «Я швырял ногами различные вещи, в изобилии валявшиеся на палубе. И вдруг под пакетом с рубашками заметил сигнальный код. Не желая

привлекать внимание немцев, я стал толкать его ногами к борту и, когда наш вельбот оказался под нами, сбросил его в вельбот» [4].

Поиск криптографических документов вели целенаправленно. Вскоре была сформирована и приступила к работам особая экспедиция из водолазов и минёров. «По воспоминаниям старшего лейтенанта И. И. Ренгартена, 29 августа водолазом был обнаружен утопленник. Он сжимал в руках сигнальную книгу (2-й экземпляр)» [4].

Всех захваченных у острова Оденсхольм немецких моряков в Петрограде допрашивали офицеры разведки Морского Генерального штаба (МГШ), затем их отправили в отдалённые от фронтов районы России. Командира «Магдебурга» вместе с пленными офицерами содержали в лагере для военнопленных под Хабаровском (5).

Наибольшую ценность для русских радиоразведчиков и криптографов среди обнаруженных документов представляли два экземпляра «Сигнальной книги германского флота» (SKM), секретные карты квадратов Балтийского моря, шифры и радиотелеграфные журналы крейсера. Вероятно, противник осознавал цену своей потери. Но замена кодовой книги дело весьма непростое, в результате немцы свой код не сменили.

ПОДГОТОВЛЕННАЯ ПОЧВА

Следует отметить, что это были не первые документы по радиосвязи германского флота, с которыми познакомились балтийские радиоразведчики. Ещё до начала войны в штаб Балтийского флота был передан германский сигнальный код для кораблей разведочной службы, добытый агентурной разведкой МГШ. И. И. Ренгартен оперативно выполнил перевод этого документа, что позволило ему уже в предвоенное время составить представление об особенностях организации радиосвязи на германском флоте. Да и в целом Балтийский флот был подготовлен к эффективному использованию трофеев с «Магдебурга».

Архивные документы свидетельствуют о планомерной подготовке флота к войне в эфире. «Идея ведения радиоразведки (РР) на Балтийском фло-

те сформировалась к концу 1911 года в среде радиотелеграфных специалистов... Личным составом корабельных соединений действующего флота был в течение 1912–1913 годов получен ценный опыт ведения РР как при нахождении кораблей в море, так и во время стоянки в пунктах базирования» [6].

И ДЕЛО ПОШЛО

Теперь о том, как балтийские моряки распорядились своей удачей. Работа с трофейными документами шла в Службе связи и в штабе Балтийского флота. И. И. Ренгартен достаточно быстро разобрался в тонкостях действовавшей организации радиосвязи германских кораблей: в правилах радиообмена, системе радиопозывных, методике составления радиогрмм. «Сигнальная книга германского флота» представляла собой трехбуквенный алфавитный словарный код. Для передачи особо важной информации, радиогрммы, составленные по «Сигнальной книге», дополнительно «закрывались» шифром простой замены. «В первые месяцы войны открытые (то есть без зашифрования) радиогрммы составляли значительную часть германского радиообмена. Наличие в штабе флота «Сигнальной книги» позволило русскому командованию легко получить доступ к их содержанию. Разбор и обработку РРМ, как правило, производил сам И. И. Ренгартен. Имеются сведения, что разбором перехваченных радиогрмм, с учетом новизны и важности этого дела, интересовался и лично командующий флотом. В дневнике адмирала Н. О. Эссена имеется, например, такая запись за 6 ноября 1914 года: «Разбирал германские телеграммы от 4 ноября и нашел одну незашифрованную...» [6].

Уже к середине октября 1914 г. И. И. Ренгартену и его помощникам удалось наладить дешифрование немецкого радиообмена и читать составленные по сигнальной книге радиогрммы. Во второй половине ноября был вскрыт общий шифр, введенный в действие 16 октября 1914 г., что позволило начать читать значительную часть шифрованного радиообмена германского флота.



Иллюстрация 1. Боевое братство — экипаж британской подводной лодки Е-19

БЛАГОРОДНЫЕ СОЮЗНИКИ

Спасённый из воды экземпляр сигнальной книги передали союзникам. Капитан I ранга М. А. Кедров вручил его Первому лорду Адмиралтейства У. Черчиллю в присутствии начальника Морского Генерального штаба принца Людвига Баттенбергского [4].

Вот как оценивает захват немецких кодовых книг на «Магдебурге» в своих мемуарах У. Черчилль: «6 сентября ко мне с визитом прибыл русский военноморской атташе. Из Петрограда он получил сообщение с изложением случившегося. Оно уведомляло, что с помощью кодовых книг русское Адмиралтейство в состоянии дешифровать по меньшей мере отдельные участки немецких военноморских шифртелеграмм. Русские считали, что Адмиралтейству Англии, ведущей морской державы, следовало бы иметь эти книги и карты. И если бы мы прислали корабль, то русские офицеры, в ведении которых находились книги, доставили бы их в Англию. Мы незамедлительно отправили такой корабль, и октябрьским вечером принц Луи и я получили из рук наших верных союзников слегка попорченные морем бесценные документы» [3].

У. Черчилль здесь не только отдаёт дань благодарности своим русским союзникам, но и фактически признаёт первенство моряков России в начале применения криптоанализа к радиоперехвату.

ОТВЕТНЫЙ ЖЕСТ

В качестве ответного шага уже в октябре 1914 г. в Балтийское море были направлены три британские подводные лодки. Две из них сумели прорваться через преграды и минные поля в датских проливах. В сентябре 1915 года группа британских подводных лодок совершила новый прорыв в Балтийское море, среди них была лодка Е-19. По общему мнению, Ф. Кроми, командир Е-19, был самым успешным британским подводником на Балтийском театре военных действий. Главным успехом Е-19 стало торпедирование 7 ноября 1915 года в западной Балтике немецкого крейсера «Унди́не» с расстояния в километр. Подводники получили заслуженные награды, Ф. Кроми стал кавалером ордена св. Георгия 4 степени. Экипаж подводной лодки Е-19 представлен на илл. 1. По левую и правую руку от командира расположились двое русских радиотелеграфистов.

КОМНАТА № 40

Вернёмся вновь к переданным британской стороне документам, по общему признанию действительно бесценным для Англии. Они дали «такой мощный толчок её усилиям организовать криптоанализ перехваченных криптограмм противника, что в течение всего оставшегося периода войны она намного опережала своих противников в дешифровании» [3].

Но в начале спешно сформированной группе британских криптографов оказалось вовсе не просто воспользоваться даром русских союзников. «Английские криптоаналитики были ещё настолько неопытны, что им потребовалось почти 3 недели, чтобы начать читать отдельные участки некоторых немецких военно-морских донесений» [3].

По утверждению У. Черчилля, «скрупулёзное накопление этих отрывочных сведений составляло основу информации, по которой с достаточной степенью точности можно было определить характер военных приготовлений противника в Гельголандской бухте, прилегающей к северо-западному побережью Германии» [3].

К этому времени «вся группа переместилась в большую комнату № 40, расположенную близко к оперативному отделу, куда передавали дешифровки». Постепенно в «Комнате 40» пополнялся арсенал сведений о криптографическом оснащении германского ВМФ и британские разведчики делились находками со своими российскими союзниками.

СЧАСТЛИВЫЙ СЛУЧАЙ-2... И 3!

Второй важный код, используемый немецким флотом, был захвачен в самом начале войны в Австралии. В кодовой книге (HVB) содержался четырёхбуквенный код, используемый немецким флотом для сообщения с его торговы-

ми судами. Код использовался в основном патрульными кораблями, но также и подводными лодками. Третью шифровальную книгу в «Комнате 40» получили от моряков британского траулера, ловившего рыбу близ острова Тексель в Северном море. 30 ноября рыбаки выловили сундучок, выброшенный за борт с немецкого эсминца, погибшего в бою. В сундучке среди секретных документов лежал и экземпляр немецкой военно-морской кодовой книги, «книги судоходства» (VB).

Это был код, которого не доставало в «магдебургской» находке. Код состоял из цифровых групп по 5 цифр в каждой. Он был предназначен для связи с военными кораблями, а также военно-морскими атташе, посольствами и консульствами.

РАДИОСТАНЦИЯ ОСОБОГО НАЗНАЧЕНИЯ

Расширение возможностей радиоразведки Балтийского флота по добытию ценной разведывательной информации привело И. И. Ренгартена (илл. 2) к решению «инициировать вопрос о создании особой береговой радиостанции, которая бы специализировалась исключительно на задачах радиоразведки и в первую очередь на задачах шифрперехвата... В феврале 1915 г. морским министром было принято решение об организации радио-



Иллюстрация 2. И.И. Ренгартен, инициатор создания РОН

станции особого назначения (РОН), на которую возлагалась задача ведения шифрперехвата, и где решено было сосредоточить всю дешифровальную работу по германскому флоту» [6].

«Радиостанцию разместили в безлюдном месте на южном побережье Финского залива в районе мыса Шпитгамн. РОН фактически включала в себя три составных элемента: 2-киловаттную радиостанцию, предназначенную для экстренной передачи особо важной информации, приемные посты для добытия шифрматериалов и дешифровальное бюро, на которое возлагалась задача их обработки. РОН начала реально функционировать с 20 февраля 1915 года» [7].

(Окончание в следующем номере)

ЛИТЕРАТУРА

1. Партала М.А. Рифы и мифы острова Оденсхольм // Защита информации. Инсайд. 2007. № 1.
2. Соболева Т.А. История шифровального дела в России. М., 2002. С. 281–282.
3. Кан Д. Война кодов и шифров. М., 2004.
4. Ежов М. Ю. Один из мифов о крейсере «Магдебург» // Вопросы истории. 2007. № 2.
5. Партала М.А. «Магдебургская» история — «работа над ошибками» // Защита информации. Инсайд. 2014. № 2.
6. Партала М.А., Симонов Д.Н. Радиоразведка русского императорского флота на Балтийском море: история создания // Защита информации. Инсайд. 2005. № 1
7. Партала М.А. Радиостанция особого назначения на мысе Шпитгамн (1915–1917) и её место в истории радиоразведки Балтийского флота // Санкт-Петербург и страны Северной Европы: Материалы седьмой международной научной конференции — СПб.: РХГА, 2006.
8. Партала М.А. Радиоразведка Балтийского флота в Первую мировую войну (к истории создания) // Санкт-Петербург и страны Северной Европы: Материалы шестой международной научной конференции — СПб.: РХГА, 2005.
9. Кикнадзе В.Г. Развитие сил и средств радиоразведки отечественного военно-морского флота в первой половине XX века: исторический опыт и уроки. Диссертация докт. ист. наук. Военная академия ГШ ВС РФ, 2014.
10. Партала М.А. «Сигнальная книга» с турецкого крейсера «Меджидие» // Защита информации. Инсайд. 2007. № 5.

ЗАМЕТКИ БЕЗОПАСНИКА

Среди российских безопасников есть немало достойных специалистов, опыт и мысли о профессии которых интересны и полезны коллегам. Рубрика «Мысли вслух» нашла отклик у наших читателей прежде всего тем, что в ней представлены небольшие по объему и написанные в свободной форме заметки, эссе, необычные случаи из практики, вопросы, предложения, личные наблюдения, философские обобщения и прочая, прочая... — в общем, все то, что называется живым общением профессионалов.



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

12 ЗАКОНОВ ВСАМДЕЛИШНОЙ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

Недавно, прочитав онтологическое исследование общества «Россия — поместная федерация» от Симона Кордонского, я поразился, насколько точно там сформулированы мои ощущения от противоречивости корпоративной жизни в целом и корпоративных служб ИБ в частности. Симон противопоставляет «реальность» (политики и процедуры) и «на самом деле» (практику). В его трактовке политики и процедуры в России всегда противостоят практике, чтобы в образовавшейся «лакуне» (на языке переговорщиков «поляне для торга») было пространство для маневра, а значит и возможность торговаться, договариваться и извлекать финансовую или нефинансовую прибыль.

Источник нашей «лакуны» — практика корпоративной жизни, ведь даже в лучших компаниях противоречий полно. Почему так — сотрудники не знают, исполнители валят на менеджеров, те на топ-менеджеров, а те в свою очередь — на акционеров, т.е. как будто толком не выстроены процессы управления компанией (в клинических случаях я использую термин «корпоративная шизофрения»).

Однако «плохо» управляемые компании как-то растут, зарабатывают прибыль, выходят на новые рынки, и в общем чувствуют себя неплохо, а значит мы чего-то не знаем и есть пространство для исследования и эмпирических опытов.

С помощью концепций Симона Кордонского я обобщил личный и клиентский опыт корпоративных ситу-

аций — сформулировал 12 законов «всамделишной» корпоративной безопасности. О них не написано в ФГОСах, лучших практиках или security guides, но их понимание изрядно упрощает корпоративную жизнь безопаснику, позволяя достигать большего и легче переносить стресс.

1. Безопасность по умолчанию непонятна бизнесу. Умелые безопасники держат непонятность на удобном для них уровне.

2. Чем мутнее и толще пачка утвержденных документов по безопасности, тем меньше спорят с безопасником в целом и в частности по бюджетам и выполнению политик ИБ — много читать бояться практически все.

3. Чем понятнее деятельность, тем меньше смысла ею заниматься безопасности. Ведь тогда есть риск, что безопасность станет сервисной прозрачной организацией и будет работать в «мысле» — в бэк-офисе.

4. Если что-то работает как-либо (особенно если безопасность уже что-то делает), лучше этого не менять. Перемены — враг безопасности.

5. Настоящая безопасность живет только под чьей-то «крышей». «Крышей» в зависимости от типа корпоративной культуры могут выступать СЕО, регулятор, вышестоящая организация или лучшие практики. А лучше все вместе — «крыши» много не бывает.

6. Никто не знает, чем должна заниматься безопасность. А значит, чтобы заниматься хоть чем-то, должна быть веская причина. Желательно в рамках выполнения обещаний «крыше».

7. Никто не знает, сколько людей и денег нужно для обеспечения безопасности. А значит их количество ограничено только мощностью «крыши» и толщиной пачки обосновывающих документов.

8. Никто не знает, как нужно измерять безопасность. А значит лучшее практически полезное измерение — удовлетворенность «крыши».

9. Лучший способ повысить безопасность — ничего не делать. Рано или поздно произойдет аудит или инцидент, и сразу всем захочется повышать безопасность. А без аудита или инцидента никто не будет хотеть, и никакого толку от активности безопасности не будет.

10. Дешевая безопасность — плохая безопасность. Так недалеко и до понимания сервисной роли безопасности и даже богомерзского SLA.

11. Гибкая безопасность — не лучше дешевой. Для безопасности нет ничего хуже перемен.

12. Нет ничего хуже структурированного подхода к безопасности, ведь тогда руководителя службы ИБ можно заменить — процессы-то налажены.

КАК Я ПРОИГРАЛ СДЕЛКУ НА 10 МЛН РУБ., ИЛИ О СКОРОСТНОМ РЕЖИМЕ В КИБЕРБЕЗОПАСНОСТИ

Пару лет назад я вел пилот одного из ведущих мировых SIEM в B2C-банке ТОП-50 (SIEM A). В Банке уже был другой ведущий SIEM (SIEM B), но мой партнер был дешевле и лучше сочетался с архитектурой ИБ банка (у него было много технологий от того же вендора). За меня было много чего — банк купил у нас антифрод-проект, нас знали на уровнях CSO и CISO, и CSO и CISO были профи и не имели заоблачных требований к SIEM. Банк не хотел платить за поддержку дорогого SIEM B (как раз скакал доллар), у меня была поддержка директора бизнес-юнита ИБ и вендора SIEM A.

Против меня был только один фактор — скорость. Я и моя платформа (работодатель) просто не успевали за процессами Банка. Мы были медленнее во всем — выделении ресурсов, поставке пилотного оборудования, настройке коннекторов и правил, да даже в изъятии оборудования после пилота. В конце-концов, мой личный пайплайн тогда составлял 20 сделок и миллиард рублей — и отчитывался я за каждую.

Хотя определенные «косяки» были и у Банка (в силу скорости Банк уде-

лял каждому проекту всего по чуть-чуть внимания — сильно разбрасывался), причина провала сделки все же оказалась в разной скорости бизнеса Интегратора и Банка. Банк непрерывно выводил новые сервисы и услуги, боролся за прибыльность, оптимизировал штат, ключевые заказчики генерировали больше половины бизнеса, госконтракты и госкомпании давали еще больше, сокращения были чисто ритуальные (отдали 1–2 человек в паническом декабре 2014).

А через год я закрыл несколько на порядок более крупных сделок — работал с клиентами, что жили на схожей с нами скорости. С B2B госкомпаниями всегда работать принципиально легче — Интегратор принципиально быстрее их, уже они не поспевают за нами, а затормозить всегда легче, чем набрать скорость.

Подобная история в последние пару лет наблюдается чуть ли не у всех бизнесов. Потребители живут на скорости X, бизнес (так же как и киберпреступность) пытается выжать хотя бы X-1, служба ИТ/ИБ и игроки рынка ИБ — хотя бы X-2. Может быть поэтому в по-

следнее время крупные игроки рынка ИБ стали источником целого ряда spin-off'ов (например, Solar Security, Reaxoft, Ангара, Иридис) — новые игроки за счет компактности, большей управляемости и маневренности могут набрать большую скорость и отгрызают контракты у крупняка. А крупняк не больно и сопротивляется, ведь у него все хорошо и проблема скорее в управляемости — миллиардные обороты не всегда сопровождаются устойчивой диверсифицированной структурой бизнеса, непрерывным денежным потоком и «вкусной» маржинальностью (хотя бы на среднем уровне в индустрии).

* * *

Из этой истории я вынес простой урок — успех все-таки от слова успевать (например, в сумасшедшем режиме нарушая половину корпоративных регламентов удалось закрыть сделку по IDM за 3 месяца). А при выборе сотрудников/места работы/подрядчиков/клиентов обеим сторонам стоит подумать, совпадают ли ритмы работодателя и сотрудника.

ЭТА ТОНКАЯ ГРАНЬ МЕЖДУ УЧИТЕЛЕМ ИНФОРМАТИКИ, ТОП-МЕНЕДЖЕРОМ И ХАКЕРОМ



Поделится Валерий Естехин

РОССИЯ — ВЕЛИКОБРИТАНИЯ: ЛЮДИ И БАНКИ

Завершая наш «Лондонский цикл», мы попросили автора представить на этот раз не забавную историю из его жизни, а обобщенный взгляд на отношение англичан и россиян к национальным банковским системам. И вот, пожалуйста! Категоричность суждений оставляем на совести автора.

Руководствуясь чисто исследовательским интересом, я задавал друзьям-англичанам вопрос: «Не боитесь, что Ваш банк лопнет, и вы потеряете свои деньги?» Ответом был изумленный взгляд, в котором читалось: «С виду вы вроде неглупый человек, а задаете такой нелепый вопрос!» Англичанину и в голову не придет, что он может потерять свой кровный банковский вклад. Банковская система Соединенного Королевства надежна и устойчива, словно респектабельная набережная Темзы.

В Матушке же России в национальную банковскую систему люди не верят по причине недавнего горького опыта и кислой текущей действительности. Достаточно вспомнить такие крупные, даже по британским меркам, банки, как «Менатеп», «Российский кредит», «Мосбизнесбанк», «Инкомбанк» и другие, растворившиеся в небытии буквально вчера по историческим меркам. Для властей и СМИ все уже былём поросло, концы в воду, но не для людской памяти и кошельков!

Ныне российские СМИ ежедневно оповещают о лопающихся, словно мыльные пузыри, банках по всей необъятной державе. Ничего подобного в истории Соединенного Королевства даже отдаленно не случалось.

В ПРЕДЫДУЩИХ НОМЕРАХ:

BIS Journal №3 / 2016:

«Полтора часа длилась беседа банковских «особистов» с Леонидом. По форме — агличкой, притворно вежливой, по существу — в стиле железных чекистов бериевских времен. Выясняли о Леониде буквально все, начиная с реквизитов паспорта, кончая датой свадьбы с любимой женой».



BIS Journal №4 / 2016:

«В первоклассных лондонских банках обычных россиян, жаждущих открыть счет, откровенно пугаются. Стена недоверия к нашей стране, выстроенная британскими СМИ, сыграла свою роль. Тень гениального и ужасного российского хакера висит над британскими банками!»

**БАНКОВСКАЯ СИСТЕМА СОЕДИНЕННОГО
КОРОЛЕВСТВА НАДЕЖНА И УСТОЙЧИВА,
СЛОВНО РЕСПЕКТАБЕЛЬНАЯ
НАБЕРЕЖНАЯ ТЕМЗЫ**

Но задавать вопрос героя песни В. С. Высоцкого: «Где деньги, Зин?», — считается в России верхом бестактности. Украденное у доверчивых вкладчиков и государства плавно перетекает в бездонные карманы кучки хозяев национальной экономики. Они без зазрения совести мирно заседают в Думе, правительстве, крупнейших корпорациях, СМИ, творческих союзах и т. д. Их лица не сходят с телеэкранов.

Правосудие лишь застенчиво отворачивается, храня гробовое молчание. Почему? Тайна сия велика есть. В нашем общественном сознании все это воспринимается, как нечто совершенно естественное, что для англичан выше разума.

В Соединенном Королевстве подобное фарисейство немыслимо. В банковском сообществе там железно действует принцип героя известного телесериала: «Вор должен сидеть в тюрьме!». Утаить информацию о махинациях банки не в силах. И маются по острогам немногочисленные аглицкие жулики от банков (найдите страну без них — удивлюсь), как миленькие. А политическому или культурному деятелю, замешанному в грязных банковских махинациях, никто руки не подаст. Народ в стране живет чрезвычайно щепетильный.

Теперь о сравнении собственно банковской деятельности. Остановимся лишь на ключевом аспекте.

При разработке и внедрении новых банковских продуктов «консер-

В МАТУШКЕ ЖЕ РОССИИ В НАЦИОНАЛЬНУЮ БАНКОВСКУЮ СИСТЕМУ ЛЮДИ НЕ ВЕРЯТ ПО ПРИЧИНЕ НЕДАВНЕГО ГОРЬКОГО ОПЫТА И КИСЛОЙ ТЕКУЩЕЙ ДЕЙСТВИТЕЛЬНОСТИ

вативные» англичане, в отличие от «дерзновенных» россиян, на удивление остро чувствуют веяния времени. Ярким примером служит «молодежная политика» банков. Беру на себя смелость провести вольную историческую параллель. «Молодежь — барометр партии», — говаривал незабвенный Л. Д. Троцкий. Именно молодежь стала «барометром» для английских банкиров. Они наперебой предлагают ей всё новые интересные продукты, включая специальные счета и банковские карты, выгодное кредитование, различные льготы, разыгрывают призы, проводят конкурсы и викторины.

Мы же, увы, отстаем на несколько лет. Такие новые для России банковские продукты, как Cash Back, Apple Pay и другие, в Великобритании давно стали обыденными. У нас они предстают в виде «осетрины второй свежести». Среди банковских приоритетов молодежь где-то на последних местах. Главное — толстосумы, толстосумы...

Про информационную безопасность: система Internet Banking для физических лиц организована в Великобритании на порядок удобней, проще и надежней, чем в России. С чистой совестью подтверждаю это из личного опыта.

Но есть, безусловно, и позитивные моменты. Наши банкиры, подобно британским коллегам, сообразили, наконец, что самые-таки надежные клиенты — обычные пенсионеры. Деньги у них, естественно, крошечные, зато их самих великое множество. Как говорится, курочка по зёрнышку...

В целом призываю наших банкиров следовать примеру англичан и действовать согласно девизу В. В. Маяковского: «Твори, выдумывай, пробуй!» Если постараться — получится. Пример тому — удачная программа «Спасибо» родного для миллионов россиян Сбербанка. Не хуже британских банковских программ.

BIS Journal №1 / 2017:

«Если вы, друзья читатели, ждете личный банковский перевод из Соединенного Королевства, или сами собираетесь перевести туда кому-нибудь деньги, — хладнокровно готовьтесь к любым неожиданностям и неприятностям. И не пытайтесь потом «найти правду» в «черном ящике» системы информационной безопасности российских и британских банков — бесполезно».



КРОССВОРД



Автор кроссворда:
Мария Кузнецова

ПО ГОРИЗОНТАЛИ:

1. Член группы людей, имеющей доступ к закрытой информации, принадлежащей этой группе.
5. Постоянное наблюдение за объектами и субъектами.
6. Экспериментальное определение количественных и/или качественных характеристик свойств объекта.
8. Неправомерное получение информации с использованием технического средства.

ПО ВЕРТИКАЛИ:

2. Тип вторжения, при котором логический объект системы изменяется таким образом, что он разрешает нарушителю произвести полномочное воздействие на что-либо.
3. Успешное преодоление механизмов защиты системы.
4. Предоставление прав, гарантирующих доступ к ресурсам в соответствии с правами на доступ.
7. Одна из специализаций внутри организованных преступных группировок, занимающихся технологиями интернет-мошенничества.

НАПОЛОВИНУ ВСЕРЬЕЗ

А ты сменил пароль?

Специалисты фирмы Микрософт опубликовали список наиболее надежных онлайн-паролей. На первом месте в категории среднеразмерных паролей с большим отрывом стоит пароль Y67hd@19nQQ, который и рекомендован всем пользователям Windows для использования.

Наблюдения

Действия профессиональных хакеров можно предсказать, но Интернет полон любителей...

Ни одно средство защиты, введенное в эксплуатацию, не прошло тестирования. Ни одно средство защиты, прошедшее тестирование, не готово к вводу в эксплуатацию (закон противоположности).

Если после отпуска вы забыли свой пароль, отдых удался.

Диалоги

- Как трем программистам организовать бизнес?
- Один пишет вирусы, другой антивирусы.
- А третий?
- Операционные системы...

Хакер читает внуку: «И стал он кликать золотую рыбку...»

- Деда, а почему рыбку?
- А потому, дружок, что мышек тогда еще не было.

Два хакера:

- А у тебя кто провайдер?
- ФСБ.
- Как ФСБ?!
- Да типа они у нас в конторе жучков поставили, так я через них...

Словарик ИБ

Флешка — часто ходящая по чужим компьютерам флэшка.

Поделились Алексей Лукацкий и Евгений Родыгин



ПРОГНОЗ НА ГОД ПЕТУХА

Через 100 лет после Февральской и Октябрьской революций

Весна: с повышенной интенсивностью продолжится законотворчество в сфере кибербезопасности, новые нормативные требования регуляторов — новый план работ для служб ИБ.

Лето: Сбербанк начинает «пылесосить» кадры и скупать компании в США и по всему миру.

Осень: традиционная зачистка банков (банкопад на фоне листопада).

Зима: разгул киберпреступности и DDoS-атак. Все атакуют всех.

Весь год в тренде: искусственный интеллект, биометрические технологии, кибербезопасность, большие данные, криптовалюты... Распространение цифровых технологий на все сферы жизни, вплоть до очков и слуховых аппаратов.

Поделился Валерий Естехин



РКІ-Форум Россия

15 лет

г. Санкт-Петербург
12–14 сентября 2017 года

www.pki-forum.ru



Встречаемся в Питере!



Медиа Группа **АВАНГАРД**



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Книжное
издательство

Нам 10 лет!