



10> Анатолий АКСАКОВ
Государственная Дума РФ
**Перемены будут! Они
продиктованы вызовами**

14> Вадим КАЛУХОВ
Банк России
**Сходить в банк раз
в жизни — это нормально**

26> Игорь НОВИКОВ
Сбербанк
**ИБ и бизнес
нашли общий язык**



34> Александр БАРАНОВ
АО ГНИВЦ
**Кто разработает
универсальный метод
идентификации?**

70> Reinhold WOCHNER
Raiffeisen Bank International
**Искусственный
интеллект — это
не мечта, а предмет ИБ**

ЭХ, ТРОЙКА! КУДА Ж НЕСЕШЬСЯ ТЫ?





Ежегодные мероприятия в области информационной безопасности:

- **IX Уральский форум** (13–17 февраля 2017 года, Республика Башкортостан)
Ключевое мероприятие Банка России по информационной безопасности финансовой сферы.
ural.ib-bank.ru
- **VI Форум Ассоциации защиты информации** (12 апреля 2017 года, г. Москва)
Конференция «Актуальные вопросы информационной безопасности». Проводится при поддержке всех регуляторов отрасли.
www.forum-azi.ru
- **XXII Конференция «Комплексная защита информации»** (май 2017 года, республика Беларусь)
Конференция Союзного государства России и Беларуси, проводится при поддержке Совета безопасности Российской Федерации.
www.kzi.su
- **Информационная безопасность платежных систем. PCI DSS Russia 2017** (31 мая 2017 года, г. Москва)
Однодневная конференция по информационной безопасности платежных систем, проводится при поддержке Ассоциации российских банков и Банка России.
payment.ib-bank.ru
- **VI Симпозиум CTCrypt 2017** (5–7 июня 2017 года, г. Санкт-Петербург)
Симпозиум «Современные тенденции в криптографии». Организаторы: ТК 26, Академия криптографии РФ и МИАН им. В.А.Стеклова.
www.ctcrypt.ru
- **XV PKI-Форум Россия** (13–15 сентября 2017 года, г. Санкт-Петербург)
Международная научно-практическая конференция, посвященная проблематике инфраструктуры открытых ключей, электронной подписи и электронного документооборота. Проводится по инициативе Минкомсвязи России.
www.pki-forum.ru
- **III Международная конференция «Актуальные вопросы развития наличного денежного обращения»** (октябрь 2017 года)
Международная конференция по безопасности оборота наличных денег и ценностей. Проводится при поддержке Объединения «РОСИНКАС» и Банка России.
inkas.ib-bank.ru
- **SOC-Forum** (15 ноября 2017 года, г. Москва)
Ежегодная конференция по практике противодействия кибератакам и построения центров мониторинга ИБ. Проводится при поддержке всех регуляторов отрасли.
soc-forum.ib-bank.ru



Артем ЗУБКОВ
генеральный директор
Медиа Группы
«Авангард»



Игорь НЕКРАСОВ
главный редактор
BIS Journal



Андрей МИНАКОВ
директор по развитию
BIS Journal

Вышел в свет BIS Journal № 24 — первый номер 2017 года. Надо признать, он получился одновременно и деловым, и как-то непреднамеренно революционным, футуристическим. Под одной обложкой сошлись статьи — а что такое статьи, как не знаки времени, оставленные на бумаге? — и сугубо практические, и рисующие на редкость твердыми штрихами будущее отрасли информационной безопасности. Заметим, будущее не отдаленное, а близкое, имеющее вполне просматриваемые, объемные очертания — почти полный каркас строящегося здания на фоне солнечного неба и других таких же стремительных новостроек соседних отраслей. Будущее это тревожит и будоражит воображение. Как-то оно там все повернется?

Пружиной такого устремления в будущее стал отчет с Форума FINOPOLIS-2016, зафиксировавший мощнейший рывок российских банков в сторону новых финансовых технологий. По сути, тот форум будто провел демаркационную линию: цифровой банк и облачные технологии — это настоящее и будущее банков, а привычная модель банка-офиса не сбрасывается со счетов только для того, чтобы дать окрепнуть молодой поросли, ну, и обслуживать поколение пожилых людей. В развитие этой темы в наших традиционных разделах «Регуляторы» и «Банки» обсуждается ключевая проблема безопасности «безофисных» банков и «облаков» — дистанционная идентификация личности.

Другая, не менее важная, тема — кадры в области информационной безопасности — оказалась настолько объемной и многогранной, что BIS Journal создал для нее новый специальный раздел «Образование и карьера». Представленные в нем фрагменты социологического исследования «Кадровая ситуация в ИБ 2016: Россия», не сомневаемся, не оставит равнодушным ни одного из членов ИБ-сообщества. Полный отчет об исследовании будет представлен на IX Уральском форуме.

Также в качестве авторов были привлечены и депутаты Государственной Думы, курирующие информационную безопасность. Законодательные зерна в сфере ИБ были брошены в думскую почву давно. В этом году ожидаем нового урожая.

Безусловно, и эти, и множество других серьезных тем будут обсуждаться и подробно разбираться на IX Уральском форуме. И мы рады осознавать, что это большое важное дело традиционно начинается задолго до того, как съедутся гости — с нового номера BIS Journal.

До встречи на Форуме, друзья!

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»
Держинский 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
Левиев 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 платежных 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, waralbum.ru**
Менеджер по распространению: **Кузнецова М.Д.**
Цветокорректор: **Наumenko М.Б.**
Корректор: **Бальтерманц Л.Ф.**
Выпускающий редактор: **Богданов А.Д.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»
Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д.21 (м. «Достоевская»)
Координаты: 55.779380, 37.61150
Тел./факс: +7 499 271-70-85
Интернет-версия: journal.lib-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 17.01.2017. Тираж 7000 экз.
Заказ № 155/7. Цена договорная.
Отпечатан в «Типографии на Угрешской»
115088 РФ, Москва, ул. Угрешская, д.2, стр.2.
Тел.+7 495 720-62-28

© BIS Journal, 2017

НОВОСТИ

5 В России, в мире, криминал, угрозы

РЕГУЛЯТОРЫ

12 **Законодательство /**
Анатолий АКСАКОВ (Государственная Дума)
Перемены, продиктованные вызовами

16 **Дистанционные сервисы /**
Вадим КАЛУХОВ (Банк России)
Сходить в банк раз в жизни

20 **Аутсорсинг /**
Артем СЫЧЕВ (Банк России),
Сергей ВИХОРЕВ
(«ПЕТЕР-СЕРВИС Спецтехнологии»)
Поговорим об аутсорсинге безопасности информации

БАНКИ

28 **Управление /**
Игорь НОВИКОВ (Сбербанк)
Язык, понятный бизнесу

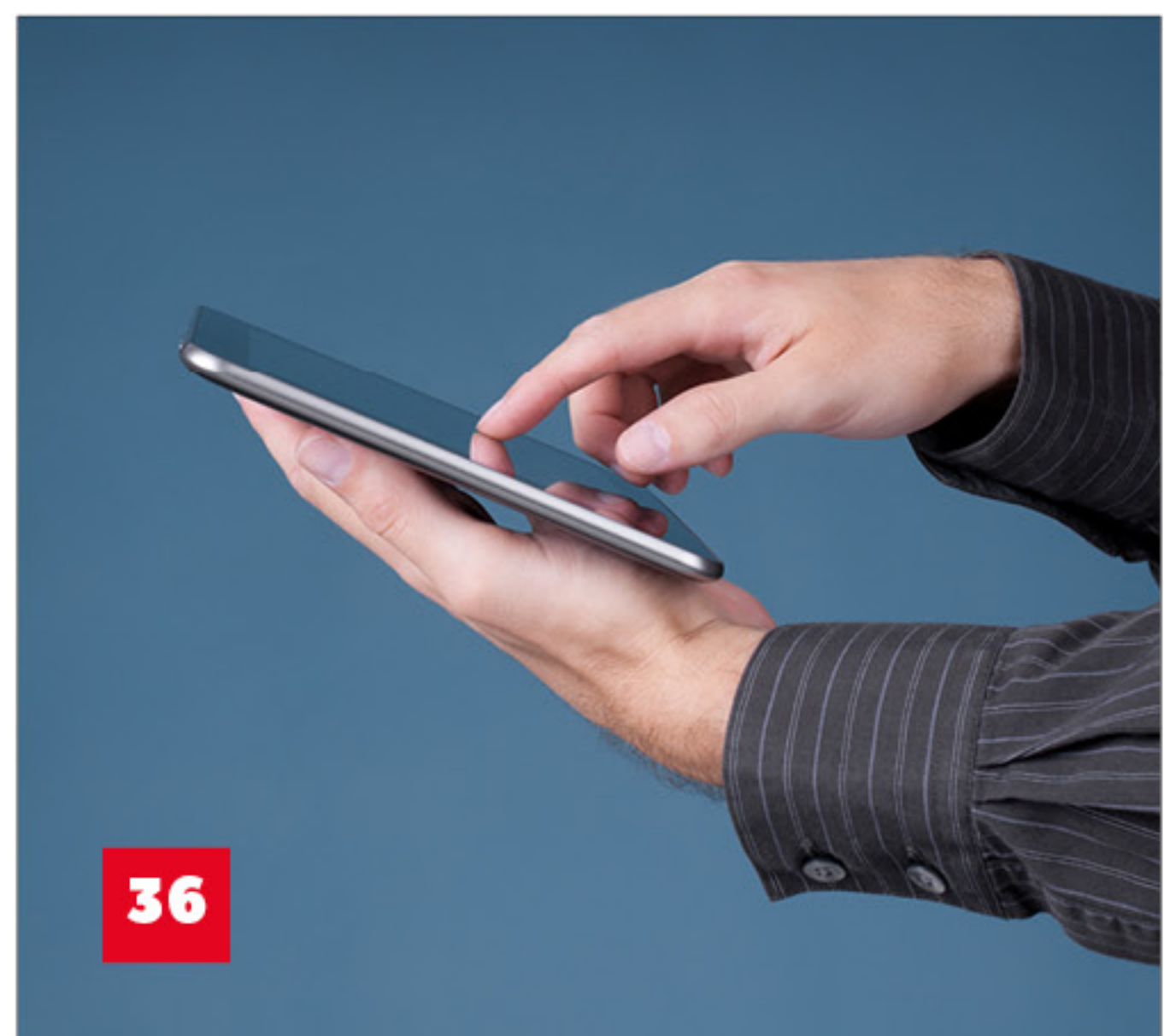
32 **Управление /**
Виктор СЕРДЮК (АО «ДиалогНаука»),
Михаил РОМАНОВ
(ООО «Новые технологии безопасности»)
Обратная сторона привилегий

34 **Управление /**
Дмитрий МИХЕЕВ (ООО «АйТи Бастион»)
Как мы контролировали работу
привилегированных пользователей

36 **Электронный документооборот /**
Александр БАРАНОВ (АО ГНИВЦ)
Облачная электронная подпись

42 **Электронный документооборот /**
Владимир ИВАНОВ («Актив»)
Как перейти на новые стандарты электронной
подписи

44 **За рубежом /**
Елена ХАРЛАМОВА (BIS Journal)
Банковская безопасность в Беларуси





УГРОЗЫ И РЕШЕНИЯ

- 46 VPN-продукты /**
Андрей ФРОЛОВ (ПАО «Почта Банк»),
Александр ВЕСЕЛОВ (ООО «С-Терра СиЭсПи»)
Практический опыт построения VPN сетей в банках
- 48 Тренды /**
Александр ХЕГАЙ (АО Cross Technologies)
ТОП-10 средств ИБ, на которые стоит обратить внимание в 2017 году
- 50 DLP-системы /**
Сергей ОВЧИННИКОВ (ГК «Конфидент»)
Можно ли банку обойтись без DLP-системы?
- 52 ИБ и бизнес /**
Мария ВОРОНОВА (ГК InfoWatch)
Как безопасность содействует бизнесу?
- 54 Технологии /**
Сергей ШЕРСТОБИТОВ (ГК Angara)
Будущее — за перспективными технологиями и сервисами
- 55 Технологии /**
Дмитрий ГУСЕВ (ОАО «ИнфоТеКС»)
ViPNet HSM PS: новый уровень обеспечения безопасности платежных систем
- 56 Сервисы /**
Александр ЧЕЧУЛИН (ICL-КПО ВС)
«Киберугрозы множатся, средства защиты тоже...»
- 58 Визуализация /**
Михаил ЛАРИН («АМТ-ГРУП»)
Как «готовить» ИБ-визуализацию
- 60 Аудит /**
Никита КЕЛЕСИС (Digital Security)
Чужой в банке: гость, которого не ждали
- 62 Антифрод /**
Алексей СИЗОВ («Инфосистемы Джет»)
Антифрод на пороге машинного обучения
- 64 Firewall /**
Максим ФИЛИППОВ (Positive Technologies)
Как защитить банк от киберугроз?
- 66 Дистанционный банкинг /**
Денис КАЛЕМБЕРГ (SafeTech)
Безопасность как двигатель дистанционных сервисов
- 68 Импортозамещение /**
Алексей САБАНОВ,
Александр ДОДОХОВ («Аладдин Р.Д.»)
Смена СУБД. Как не наломать дров при импортозамещении
- 70 PCI DSS /**
Анна АНТОНОВА («Информзащита»)
Трудный стандарт

ИНФРАСТРУКТУРА

- 72** **Деловые мероприятия**
FINOPOLIS 2016
- 78** **Деловые мероприятия /**
Алексей ЛУКАЦКИЙ (эксперт ИБ)
SOC-Форум: послевкусие
- 84** **Ценности /**
Андрей АКИНИН («Вэб Контрол»)
Новый мир — новые подходы?
- 88** **Презентация**
Книга «Чтоб было в тех землях не знатно...»



ОБРАЗОВАНИЕ И КАРЬЕРА

- 90** **Социология /**
Александр БОДРИК (эксперт информационной безопасности)
Кадровая ситуация в ИБ 2016: Россия
- 96** **Обзор /**
Марина БРОДСКАЯ (BIS Journal)
Куда пойти учиться за границей?
- 99** **Что ждёт молодого специалиста?**
- 101** **Юбилей**
ФУМО — 20 лет!



СУБЪЕКТЫ

- 104** **Корифеи /**
Геннадий ЕМЕЛЬЯНОВ (Академия криптографии РФ), **Дмитрий ЛАРИН** (кандидат технических наук)
Они ковали Победу
- 110** **Мысли вслух /**
Александр БОДРИК (эксперт ИБ)
Паутина рисков третьих сторон
- 114** **Последний день Помпеи**
- 116** **Обратная связь /**
Павел РОГОВ (читатель BIS Journal)
Лондон — Москва: где деньги?
- 118** **Гороскоп-2017**



ОФФТОПИК

- 120** **Блогеры улыбаются**
Кроссворд, юмор

БЛОКИРОВАТЬ ВРЕДОНОСНЫЕ САЙТЫ СТАЛО ПРОЩЕ

Интернет-ресурсы с вредоносным содержанием, относящимся к сфере финансовых рынков и национальной платежной системы, будут блокироваться на основании информации, полученной напрямую от Банка России. Соответствующее соглашение заключено между регулятором и Координационным центром национального домена сети Интернет — администратором национальных доменов верхнего уровня.рф и.ru.

Таким образом, Банк России получил статус компетентной организации, имеющей право выявлять сайты-нарушители, распространяющие вредоносные программы, ресурсы с противоправным контентом, а также фишинговые сайты, и предоставлять эти данные Координационному центру и аккредитованным регистраторам доменных имен для блокировки таких сайтов.



Новые полномочия помогут Банку России защитить персональные данные и деньги граждан от посягательств со стороны кибермошенников.

Сведения о случаях неподобающего использования доменного имени в национальной платежной системе и сфере финансовых рынков можно направлять в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) Банка России по адресу fincert@cbr.ru или телефону +7 (495) 772-70-90.

КЛИЕНТ СМЕНИЛ SIM-КАРТУ

Российские банки смогут узнавать у мобильных операторов информацию о смене клиентами SIM-карт. Такую возможность одобрили представители Центробанка РФ, Минкомсвязи и кредитных организаций. По мнению сторон, нововведение поможет противостоять кибермошенникам, которые по поддельным доверенностям в салоне связи могут получить копии SIM-карт кли-

ента для доступа к его online-счету. Для доступа к счетам мошенники используют вредоносное ПО, однако для проведения операций в интернет-банке нужны одноразовые коды, которые отправляются на мобильный номер владельца счета. Такому мошенничеству можно воспрепятствовать за счет обмена между банком и оператором связи сведениями, не содержащими персональных данных. Участники встречи в Центробанке рассмотрели возможность, при которой финучреждение запрашивает у оператора связи данные о том, менял ли клиент SIM-карту. Также стороны пришли к соглашению относительно правовых вопросов для реализации предложения.

Однако, по мнению представителя МТС Д. Солодовникова, появление промежуточного звена (базы данных) создает риск утечки информации. К тому же, пока не понятно, кто будет держателем базы и за чей счет она будет финансироваться.



ФСБ ПОДГОТОВИЛА ЗАКОНОПРОЕКТ

Федеральная служба безопасности представила на обсуждение Общественному совету при ФСБ проект закона «О безопасности критической инфраструктуры Российской Федерации».

Законопроект стал ответом на участвовавшие попытки организации масштабных кибератак на объекты критически важной инфраструктуры. «Нет сомнений, что сегодня необходимо уделять больше внимания вопросам безопасности в Интернете, чтобы обеспечить системное и эффективное противодействие любым киберугрозам, — отметил зампред Общественного совета при ФСБ В. Титов. — Принятие закона позволит создать правовую и организационную основу для надежного функционирования системы безопасности критической ИТ-инфраструктуры страны».

В КРЫМУ ВПЕРВЫЕ ОСУДИЛИ ХАКЕРА

Суд Центрального района города Симферополя приговорил хакера к двум годам колонии-поселения и штрафу — 600 тыс. рублей. Для России этот случай пока уникален. Впервые на скамью подсудимых попал гражданин, который незаконно переводил мобильный трафик за рубеж.

В мае 2016 года 23-летний москвич А. Журинов, используя сим-карты ГУП РК «Крымтелеком» и ООО «СевТелекомСвязь», с помощью специального оборудования, компьютерных и информационных технологий, позволяющих обходить защиту операторов связи, осуществил незаконную маршрутизацию мобильного трафика в Республику Куба. В результате осуществления звонков по международному направлению предприятиям связи нанесен ущерб на сумму более 35 млн рублей.

«БЕЛЫЕ» ХАКЕРЫ АТАКУЮТ КИБЕР-ПРЕСТУПНИКОВ

Специалисты «Лаборатории Касперского» обнаружили неизвестную ранее кибергруппировку, которая атакует командные серверы хакеров.

Неизвестные получают доступ к таким серверам и анализируют содержащиеся на них похищенные персональные данные. После чего рассылают жертвам сообщения с информацией об утечке и призывом позаботиться о безопасности. Сообщения рассылаются на английском и испанском языках. Таинственные «белые» хакеры называют себя Group Demosfenes. Название предположительно отсылает к имени древнегреческого философа и оратора Демосфена, знаменитого своими афоризмами, среди которых есть и такой: «Всякое слово без дела ничтожно и пусто».

ПЕРЕВЕЛ УКРАДЕННЫЕ ДЕНЬГИ НА СВОЙ СЧЕТ

Кибервзломщик Томаш Сковрон из Великобритании перевел украденные 840 тыс. фунтов стерлингов на свой именной счет, за что был арестован и получил срок пять лет тюремного заключения.

29-летний Томаш Сковрон был членом преступной хакерской группировки. Свои аферы преступники проводили при помощи вредоносных программ. Большая часть украденных денег обналичивалась. Полиция определила IP-адрес, с которого осуществлялись банковские махинации, и вышла на Сковрона. Детективы изъяли у него телефоны и компьютеры, судебная экспертиза установила причастность подозреваемого к киберпреступлениям. Также Сковрон имел неосторожность переводить часть украденных денег на свой именной счет в банке.

СОСТАВЛЕН РЕЙТИНГ КИБЕРВОЙСК МИРА

Россия вошла в топ-5 государств с наиболее развитыми кибервойсками. Численность российских спецподразделений составляет примерно 1 тыс. человек, расходы на них — около \$ 300 млн в год. К такому выводу пришли аналитики компании Zecurion.

На первом месте в рейтинге оказались США (госфинансирование на уровне \$ 7 млрд в год, армия хакеров — порядка 9 тыс. человек). На второй строчке — Китай. Госфинансирование — примерно \$ 1,5 млрд в год, а армия оценивается, как самая многочисленная, — 20 тыс. хакеров. Третье место занимает Великобритания, она выделяет на отрасль, включающую 2 тыс. сотрудников, \$ 450 млн. Четвертое — Южная Корея. Ее бюджет на армию из 700 хакеров — \$ 400 млн.

По оценкам аналитиков, специализированные подразделения по кибербезопасности официально используют



несколько десятков стран, неофициально — более сотни. «Оценка потенциала в этой сфере основана на военных бюджетах государств, стратегиях кибербезопасности, уставных документах, справочной информации международных организаций, официальных комментариях и инсайдерской информации», — говорится в сообщении Zecurion.

РОССИЯ, ТУРЦИЯ И БРАЗИЛИЯ РИСКУЮТ БОЛЬШЕ ДРУГИХ

По итогам 2016 года, подведенным аналитиками «Лаборатории Касперского», Россия, Турция и Бразилия возглавили список стран, где пользователи наиболее подвержены риску заражения финансовым вредоносным ПО, — за год в этих странах с банковскими угрозами столкнулись около 5 % пользователей, то есть каждый двадцатый.

Эксперты связывают увеличение числа атак банковских зловредов с ро-

стом числа пользователей мобильного банкинга. Так, из 10 наиболее популярных сегодня банковских троянцев пять предназначены для кражи финансовых данных с устройств на базе Android. По сравнению с 2015 годом доля подобных атак на смартфоны и планшеты Android увеличилась в 4,5 раза.

Кроме того, в 2016 году появилось восемь новых семейств зловредов для платежных терминалов (POS) и банкоматов. Таким образом, общее число вредоносного ПО для этих устройств выросло на 20% по сравнению с 2015 годом.

Всего же к концу 2016 года в коллекции вредоносного ПО, распознаваемого защитными решениями «Лаборатории Касперского», насчитывается один миллиард объектов. Среди них вирусы, троянские программы, бэкдоры, шифровальщики, рекламное ПО и др.



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



ДЕРЖИСЬ, БАНКОМАТ!

По прогнозам специалистов, в 2017 году хакеры сосредоточатся на краже денег из банкоматов (АТМ). Размер хищений может составить более 2,5 млрд рублей, что больше показателей 2016 года на 25-30%.

У злоумышленников есть два способа получить чужие деньги. Первый – подключение хакерских устройств к диспенсеру банкомата. В этом случае АТМ выдает злоумышленникам все имеющиеся в нем деньги (до 20 млн рублей), что наносит ущерб кредитным организациям. Второй способ: кибермошенник получает доступ к серверу управления АТМ, запускает вредоносное ПО, после чего снимает средства в офлайне с поддельных карт. При этом потери несут уже граждане. Доказать факт кражи во втором случае сложно, в связи с чем средства пострадавшим часто не компенсируются.

КУПИТЬ ОБОРУДОВАНИЕ ДЛЯ ВЗЛОМА СМАРТФОНОВ? ЛЕГКО!

Журналисты Motherboard Vice провели эксперимент: попытались приобрести специальное оборудование, которое правоохранные органы используют для взлома мобильных гаджетов.

Оказалось, такие устройства можно купить без всяких разрешений. На eBay запросто продают оборудование Universal Extraction Forensics Devices (UFED), которое позволяет извлечь с устройства список контактов, почту, текстовые сообщения и т. д. Необходимое ПО для него доступно в онлайн, его может скачать кто угодно. На том же eBay предлагают аддон Cellebrite UFED CHINEX для извлечения паролей и информации со смартфонов. Польский сайт для частных детективов открыто предлагает UFED Touch Ul-



time для извлечения и удаления данных, а также обхода парольной защиты Android-устройств.

X Юбилейный межотраслевой

CISO FORUM 2017: Суровые будни CISO

17–18 Апреля 2017 • Отель DoubleTree by Hilton Moscow



ТОЛЬКО ФАКТЫ:

- 400+ участников
- 70+ спикеров; 80% — CISO
- 3 параллельных потока для разного профессионального уровня

- 2+ интервью на сцене с трендсеттерами
- 3+ круглых стола
- 4+ уникальных мастер-классов
- 12+ практических кейсов

Регистрация уже открыта! www.infosecurity-forum.ru

УБИЙЦА СТАЛ... ВЫМОГАТЕЛЕМ

Обнаружена новая версия вредоносной программы KillDisk, предназначенная для атак на Windows и Linux-системы.

За распространением новой «инкарнации» KillDisk стоит группировка TeleBots, выделившаяся из состава хакерской группы Sandworm, которая в 2015 году проводила с помощью KillDisk атаки на украинские энергетические компании. Но если тогда нападения носили политический характер, то теперь KillDisk стал инструментом обогащения. Зловред шифрует файлы инфицированных устройств, а за восстановление данных киберпреступники требуют беспрецедентный по меркам этого криминального бизнеса выкуп в 222 биткоина (порядка \$200 тыс.).

Windows-версия вредоноса использует алгоритм шифрования AES с 256-битным ключом. Ключ для рас-

шифровки хранится на сервере злоумышленников. Linux-версия использует алгоритм Triple-DES. В этом случае программа не хранит ключ шифрования на зараженном компьютере и не отправляет его на удаленный сервер, поэтому даже уплата выкупа не гарантирует восстановления данных. С другой стороны, по оценке экспертов в работе Linux-версии присутствует уязвимость, благодаря которой восстановление все же возможно.



ХАКЕРЫ ВЗЯЛИСЬ ЗА РОУТЕРЫ

Новая тенденция появилась в области распространения вредоносной рекламы: теперь атакам подвергаются не браузеры пользователей, а их роутеры. При таком методе хакерам удастся внедрить рекламу в каждую страницу.

С помощью зараженных рекламных объявлений на роутер посылается изображение, содержащее AES-ключ, который используется для дешифровки трафика, поступающего пользователю с эксплоит кита DNSChanger. Таким способом незаконные операции удастся скрыть от специалистов по информационной безопасности. После получения AES-ключа злоумышленники контролируют роутер и встраивают собственные рекламные объявления, подменяя на сайтах легитимную рекламу.

iFin
media

АРБ
Ассоциация
Российских
Банков

НАУФОР

iFin-2017

XVII МЕЖДУНАРОДНЫЙ ФОРУМ

7-8 февраля 2017, г. Москва,
«Рэдиссон Славянская»

**Электронные финансовые
услуги и технологии**

Спонсоры

BSS

iGAM

BIFIT

→ Технологии

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

→ Бизнес

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

ТОСТЕРЫ ПРОТИВ БАНКОВ

Зафиксированы DDoS-атаки на крупные российские банки, которые проводятся через компьютерную сеть, состоящую из множества зараженных персональных устройств.

Речь идет о домашних роутерах, веб-камерах, тостерах, кофемашинах. Они были объединены в огромную сеть (порядка 500 000 устройств), которая в один момент начала посылать тысячи запросов на сайты крупнейших банков России. По информации расследования, кибератаки координировались западными хакерами. Их цель заключалась в том, чтобы не допустить вмешательства из РФ в процесс выборов президента США. В дальнейшем, убедившись в действенности таких атак, западные злоумышленники объединились с восточноевропейскими и стали преследовать общие корыстные цели.

ПОКЕМОН GO, ПОХОЖЕ, УГРОЖАЕТ

Главный регулятор СМИ Китая заявил о невозможности выдачи лицензии Pokemon Go на территории страны из-за вероятности угрозы географической информационной безопасности.

Отмечается, что игра может оказать положительное влияние на развитие игровой индустрии, однако несколько инцидентов показали, что она ставит под угрозу «географическую информационную безопасность, транспортную безопасность и личную безопасность». В частности, в официальном магазине приложений Google Play обнаружен вирус, замаскированный под инструкцию для игры Pokemon Go. В настоящее время власти оценивают Pokemon Go и подобные приложения и игры. До принятия окончательного решения разрешения на разработку таких игр в Китае выдаваться не будут.

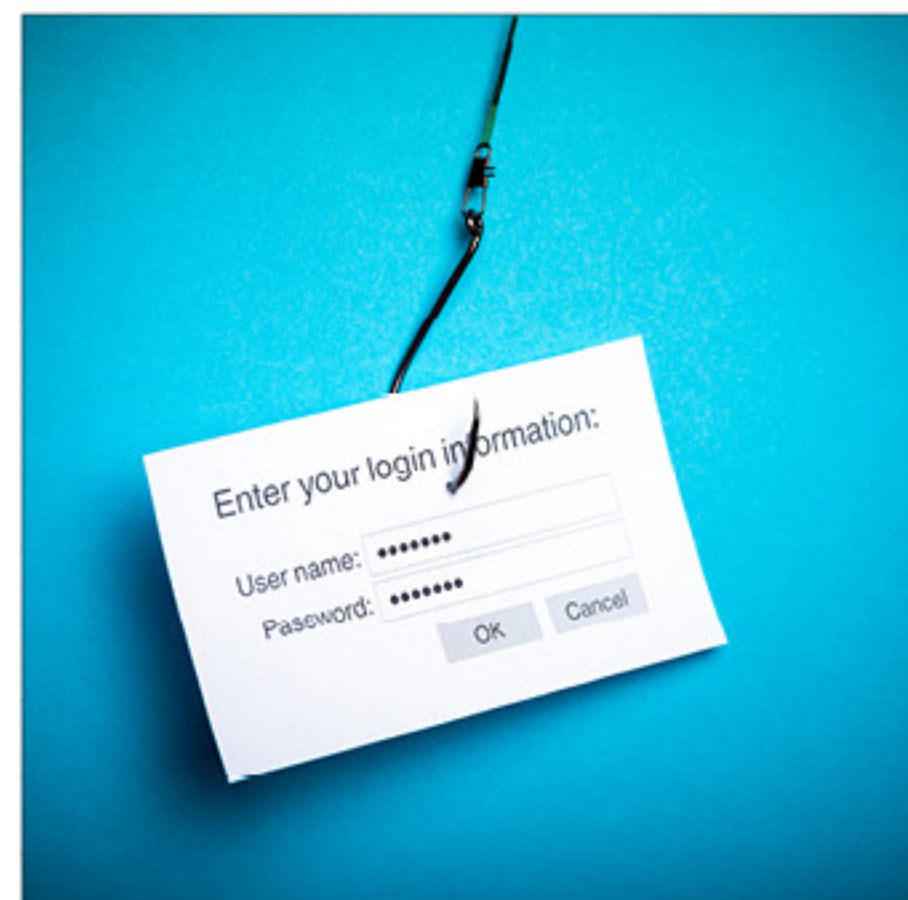
ЛЮДИ, БУДЬТЕ БДИТЕЛЬНЫ!

В киберпространстве началась массовая хакерская атака на владельцев iPhone. Пользователям гаджетов приходят странные SMS-сообщения со ссылкой на фишинговые сайты, угрожающие безопасности личных данных граждан.

О масштабной киберугрозе сообщило издание Life.ru, предупредив о новой тактике злоумышленников, заключающейся в вирусной рассылке SMS-сообщений якобы от представителей администрации iCloud. В сообщениях содержатся ссылки на сайты, после перехода на которые пользователь получит возможность усовершенствовать интерфейс своего устройства. Это официальная версия, которой пользуются мошенники.

На деле же владелец iPhone попадает на фишинговый сайт, где злоумышленники получают свободный доступ ко всем его персональным данным. Life.ru обращает внимание на бездей-

ствие правоохранительных органов перед лицом этой напасти и призывает граждан к бдительности. Защититься от угроз с помощью антивируса нельзя. Нужно просто внимательно вчитываться в любое подозрительное SMS, предварительно проверяя URL-адрес отправителя сообщения. Такие несложные меры помогут противостоять мошенникам.



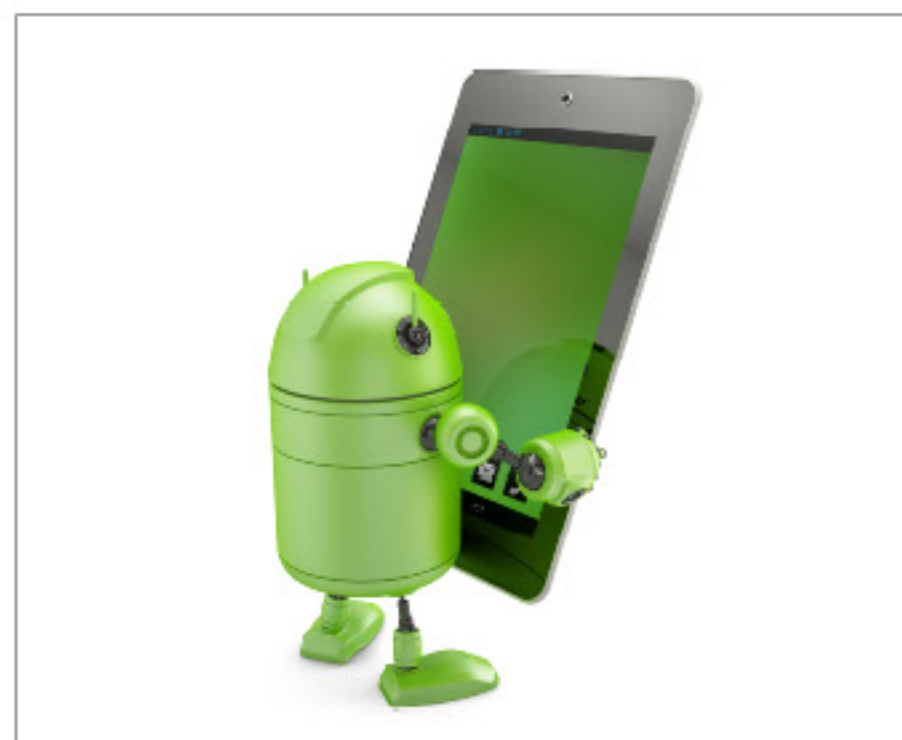
В РОССИИ ЗАРАБОТАЕТ СИСТЕМА ANDROID PAY

В настоящее время оплату покупок в РФ можно производить только с отдельных моделей смартфонов Apple и Samsung. В течение 2017 года в стране начнет функционировать система Android Pay, и платежи станут возможным осуществлять со всех устройств, поддерживающих NFC-технологии.

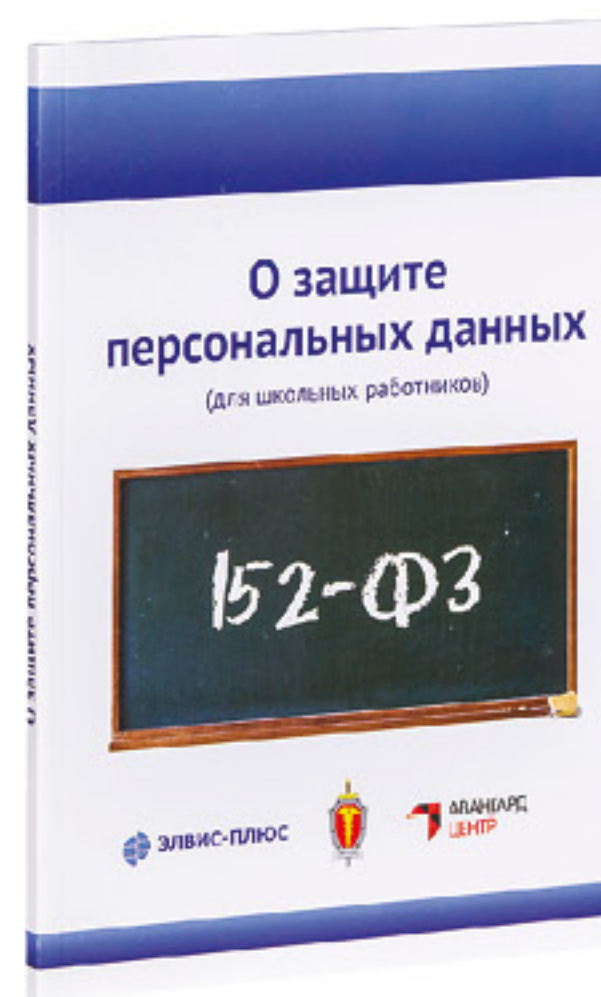
Проект по внедрению в России системы бесконтактной оплаты Android

Pay поддерживается сразу несколькими крупными банками. В частности, руководители Райффайзенбанка заявили о своей готовности к рассмотрению возможностей сотрудничества в этой сфере. В Альфа-банке также говорили о том, что проведение расчетов за покупки с помощью смартфона будет иметь большую популярность у клиентов банка, поскольку такой метод не только удобен, но и более безопасен. В качестве вероятных партнеров по внедрению новой платежной системы упоминаются Тинькофф Банк и Бинбанк.

При осуществлении оплаты через Android Pay к продавцу попадут не все параметры банковской карточки, а только цифровой токен, являющийся одноразовым. В то же время, если смартфон будет взломан, хакер получит доступ ко всем карточкам, хранящимся в его памяти.



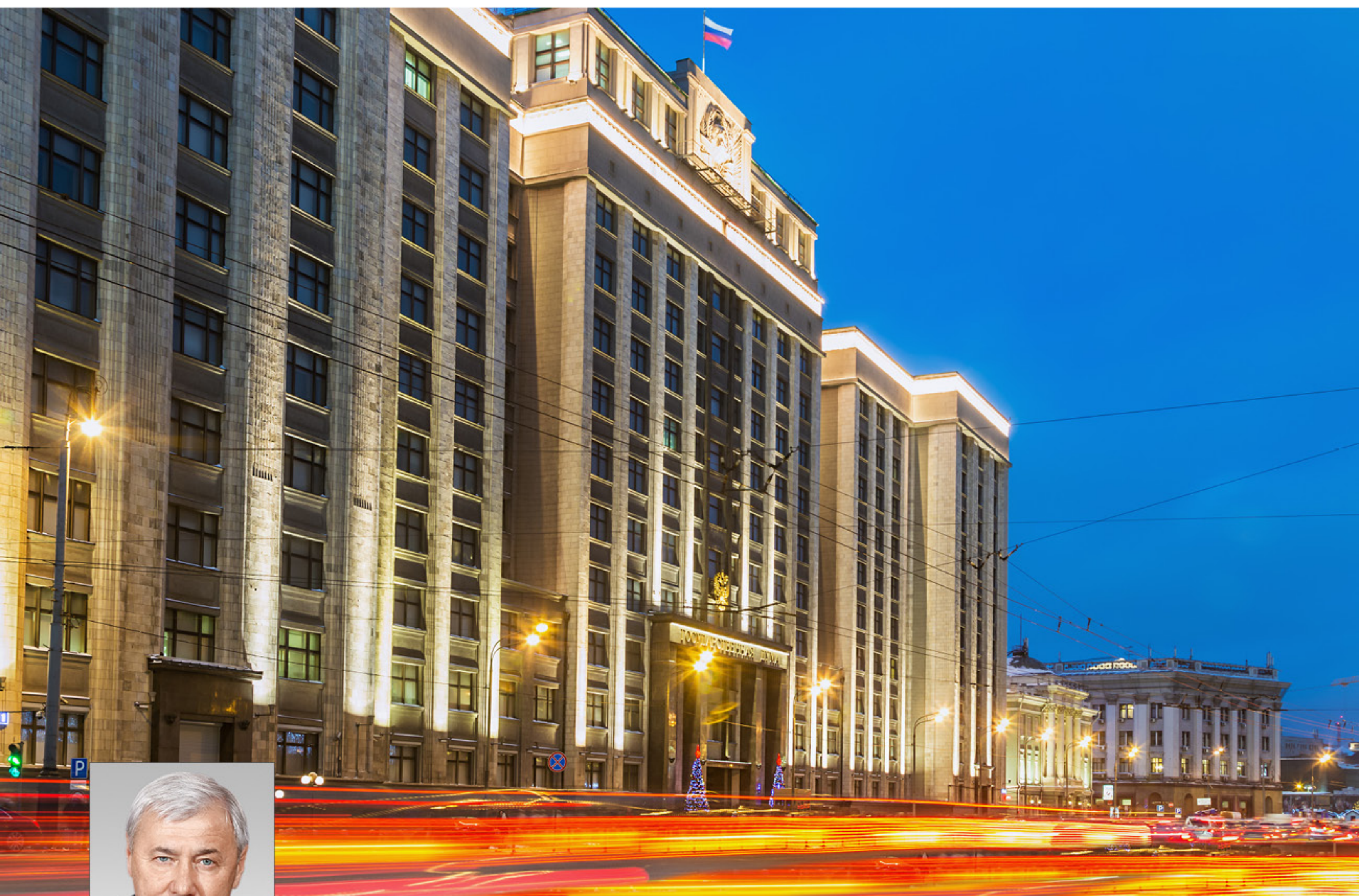
Издательство Медиа Группы «Авангард»



Лучшие книги по ИБ
теперь можно купить онлайн:

books.ib-bank.ru

ПЕРЕМЕНЫ, ПРОДИКТОВАННЫЕ ВЫЗОВАМИ



Анатолий АКСАКОВ
председатель комитета
Государственной Думы РФ
по финансовому рынку

КАК ПРЕДСТОИТ РАЗВИВАТЬ
ЗАКОНОДАТЕЛЬСТВО ДЛЯ УСИЛЕНИЯ
ПРОТИВОДЕЙСТВИЯ КИБЕРКРИМИНАЛУ
В ФИНАНСОВОЙ СФЕРЕ

Работа Государственной Думы РФ по развитию законодательства будет включать изменения, о которых говорилось 3 июня 2016 года на совещании Правительства России, посвященном вопросам информационной безопасности в кредитно-финансовой сфере. Совершенно правильно отмечалось, что противодействие киберпреступности является многосторонней системной задачей. Такая работа в настоящее время ведётся по нескольким направлениям.

КОМПЛЕКСНАЯ АКТУАЛИЗАЦИЯ

Кроме формирования необходимой инфраструктуры, использования технических и организационных мер, необходимо, конечно, совершенствование законодательной базы. Ощутимого результата добиться не получится, внося изменения в какой-то отдельный закон. Предстоит актуализировать, усовершенствовать целый комплекс нормативных актов, принадлежащих к разным отраслям права: уголовному, процессуальному, административному и финансовому.

Проходят согласования поправки в Уголовный кодекс РФ об изменении статей, касающихся компьютерных преступлений, разработанные с участием ведущих банков. Эти поправки разрабатывались, исходя из насущных требований современной практики. Жёсткость ответственности за преступления должна быть приведена в соответствие с их общественной опасностью.

В частности, в статье 159.6 Уголовного кодекса РФ предполагается изменить квалификацию ряда киберпреступлений в финансовой сфере с мошенничества на кражу. Стоит вспомнить, что указанная статья, введённая Федеральным законом от 29 ноября 2012 года № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», в своё время вызвала большие споры среди специалистов.

Отличительной чертой мошенничества является способ завладения чужим имуществом — обман или злоупотребление доверием. В киберпреступлениях хищение или приобретение права на чужое имущество сопряжено с преодолением компьютерной защиты и осуществляется путем манипуляции с компьютерной информацией. Обмана или злоупотребления доверием, в том смысле, в каком он был определен Пленумом Верховного Суда еще в 2007 году, по сути, нет. Предстоит устранить это несоответствие, которое оставляет злоумышленникам надежду на более мягкое наказание.

УЖЕСТОЧЕНИЕ СООБРАЗНО ОПАСНОСТИ

Учитывая общественную опасность компьютерных преступлений в кредитно-финансовой сфере, можно ожидать дальнейшего ужесточения ответственности за их подготовку и совершение. Ранее в русле этой тенденции в 2011 году были внесены изменения в ст. 272, 273 и 274 главы 28 Уголовного кодекса РФ. Нами был подготовлен законопроект дальнейших изменений в Уголовный кодекс РФ, каса-

ющихся усиления уголовной ответственности за хищение денежных средств с банковского счета, включая электронные платежи.

До сих пор такие деяния квалифицировались согласно части 1 статьи 158, по общему состав преступления, — как обычная кража. Виновные проговаривались к наказанию в виде лишения свободы на срок всего до 2 лет. После принятия предлагаемых изменений такие кражи смогут квалифицироваться как специальный состав преступления. Подобные преступления начнут подпадать под действие части 3 статьи 158-й Уголовного кодекса РФ, перейдут из категории небольшой степени тяжести в тяжкие. Наказание за их совершение лишением свободы увеличится на срок до 6 лет.

Одновременно законопроект расширяет объективную сторону состава преступления, связанного с мошенничеством с использованием электронных средств платежа — не только платёжных карт, но и интернет-банкинга и других подобных современных способов. Ранее состав подобных преступлений предусматривал действия только с платёжными картами и вообще не наказывался лишением свободы, только штрафом. Теперь такие преступления предлагается наказывать лишением свободы на срок до 3 лет.

ПРОХОДЯТ СОГЛАСОВАНИЯ ПОПРАВКИ В УГОЛОВНЫЙ КОДЕКС РФ ОБ ИЗМЕНЕНИИ СТАТЕЙ, КАСАЮЩИХСЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ, РАЗРАБОТАННЫЕ С УЧАСТИЕМ ВЕДУЩИХ БАНКОВ

Кроме того, в законопроекте ужесточается наказание за мошенничество в сфере компьютерной информации согласно уже упомянутой статье 159.6 Уголовного кодекса РФ. Срок лишения свободы за подобные преступления увеличивается до 5 лет. Этот законопроект находится на согласовании в Правительстве России и Верховном Суде РФ. Конечно, этот процесс не будет быстрым и простым, но предлагаемые нововведения должны пройти всестороннюю проверку на соответствие системному характеру законодательства, принципам соразмерности и справедливости. В этом видится залог эффективности работы по совершенствованию законодательства.

В ходе проводящихся согласований, а также работы по принятию предлагаемого законопроекта Государственной Думой, возможна корректировка некоторых содержащихся в нём положений. Непреодолимых противоречий нет, речь идёт о чисто рабочих вопросах.

Например, у Верховного Суда РФ свой подход к тому, к какой краже можно приравнять хищение средств с банковского счета. То ли к краже в крупном размере, от 250 000 до 1 млн рублей, то ли к краже с причинением значительного ущерба гражданину, который определяется с учетом его

имущественного положения, но не менее 5 000 рублей. От ответа на данный вопрос зависит определение категории тяжести преступления — средней тяжести или тяжкое. Что соответственно, определяет строгость наказания, лишение свободы сроком на 5 или на 6 лет.

АДРЕСНАЯ ДЕТАЛИЗАЦИЯ

Ещё одна тенденция, как показывает зарубежный опыт, в частности, США и Великобритании, — усиление детализации в уголовном законодательстве различных видов компьютерных преступлений. Таких, как кража паролей, DDoS-атаки и многие другие незаконные действия злоумышленников. Превалирующая пока в российском уголовном законодательстве квалификация подобных деяний как неправомерного доступа к информации перестала соответствовать их серьезности и опасности.

Однако следует помнить, что в США и Великобритании действует прецедентная система права, при которой велика роль судебного усмотрения, способного компенсировать коллизии между специальными нормами уголовного закона. Этот правовой механизм имел свои предпосылки, формировался веками, и нельзя просто так скопировать его на наши реалии. В Российской Федерации — свой путь правотворчества, адаптации норм к судебной практике.

Детализация различных видов компьютерных преступлений в российском законодательстве, конечно, будет вестись. Вопрос и в том, насколько быстро, качественно и посредством каких механизмов. Важно, чтобы этот процесс шёл с учетом специфики нашей правовой системы. Вспомним, что до 2012 года в Уголовном кодексе РФ был закреплён только один общий состав мошенничества. Потом Государственная Дума РФ приняла уже упомянутый Федеральный закон № 207-ФЗ. Появились специальные статьи, позволяющие квалифицировать мошенничество в отдельных сферах: в кредитовании, в страховании, при использовании банковских карт, в сфере информационных технологий.

Скажем откровенно: все трудности с квалификацией ряда преступлений после этого разом не исчезли. Например, мошенничество в сфере информационных технологий может быть совершено в различных сферах — кредитования, страхования, социальных выплат, интернет-банкинга — и содержать признаки нескольких специальных составов преступлений. Учитывая подобный опыт, нужно стремиться, чтобы детализация в законодательстве различных видов компьютерных преступлений не привела к лишнему усложнению правоприменительной практики.

НУЖНО СТРЕМИТЬСЯ, ЧТОБЫ ДЕТАЛИЗАЦИЯ В ЗАКОНОДАТЕЛЬСТВЕ РАЗЛИЧНЫХ ВИДОВ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ НЕ ПРИВЕЛА К ЛИШНЕМУ УСЛОЖНЕНИЮ ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ

ПРИОСТАНОВКА ПОДОЗРИТЕЛЬНЫХ ТРАНЗАКЦИЙ

Ещё одним узким местом остаются пробелы в законодательстве, не позволяющие сформулировать официальные критерии неправомерных электронных платежей. Такие критерии необходимы, чтобы приостанавливать сомнительные транзакции до результатов разбирательства. По мнению экспертов, это мешает выстраивать безопасное информационное пространство в кредитно-финансовой сфере.

Можно дать оптимистический прогноз ликвидации указанного пробела: нами подготовлен законопроект, который находится на стыке ряда отраслей права и вносит изменения в несколько нормативных актов. В частности, — в Федеральные законы ФЗ-161 от 27 июня 2011 года «О национальной платежной системе», закон ФЗ-395-1 от 2 декабря 1990 года «О банках и банковской деятельности», ФЗ-86 от 10 июля 2002 года «О Центральном банке Российской Федерации», а также в Арбитражный процессуальный кодекс РФ.

Законопроект получил положительную оценку Банка России. Сейчас идет процесс согласования с Правительством Российской Федерации. Он направлен на решение проблемы несанкционированных снятий денежных средств со счетов физических лиц, которые осуществляются в первую очередь с использованием платёжных карт, посредством сети Интернет и устройств мобильной связи. Доля таких операций, составившая в IV квартале 2014 года 66 %, выросла до 74 % к концу 2015 года. По прогнозам экспертов, в 2017 году ожидается дальнейший рост числа атак на счета клиентов, в том числе через платежные системы, платформы для оплаты государственных услуг, посредством средств мобильной связи и систем дистанционного банковского обслуживания.

Законопроект закрепляет право, а в ряде случаев и обязанность банка приостанавливать транзакцию, если выявлены признаки совершения перевода денежных средств без согласия плательщика. Обязательные признаки несанкционированных снятий будут вырабатываться Банком России. Так же банки могут самостоятельно вырабатывать факультативные признаки неправомерных транзакций, которые они смогут использовать в работе с клиентами.

ВОЗВРАЩЕНИЕ ПОХИЩЕННЫХ СРЕДСТВ

Кроме того, для случаев, когда выявлены признаки совершения перевода денежных средств без согласия плательщика, устанавливается порядок действий банков для возврата денег законному владельцу. Законопроект определяет порядок возврата денежных средств при доказанности факта, что перевод был осуществлен без согласия клиента. Нужно подчеркнуть: при этом законопроект не удлиняет срок проведения платежей клиентов кредитных организаций.

С практической точки зрения данный правовой механизм выглядит так. Дело не безнадежно, даже если деньги по поддельному электронному платёжному по-



ручению списаны со счёта владельца без его согласия. Банк-плательщик на основании имеющихся признаков несанкционированного списания может направить банку-получателю уведомление о приостановлении зачисления денежных средств.

Далее в течение 14 рабочих дней банк-плательщик должен представить решение арбитражного суда, принятое по особой ускоренной процедуре, в котором устанавливается факт несанкционированного снятия денежных средств. Тогда несанкционированно переведённые денежные средства могут быть возвращены их владельцу.

Если же такого судебного решения своевременно не поступит, то деньги зачисляются на счет банка-получателя. В этом случае ответственность за ущерб, причинённый владельцу денежных средств, возлагается на него самого. Банк может сам выявить подозрительный платёж и дополнительно проверить его правомерность.

Но и клиент банка, владелец денежных средств на счету, должен заботиться о том, чтобы добросовестно незамедлительно уведомлять банка об инцидентах — списании денежных средств без его согласия. Чтобы, в отведённое на это время, несанкционированный платёж был приостановлен, и проведены процедуры возврата денег.

Для противодействия киберпреступности в финансовой сфере нуждаются в развитии нормы Федеральных законов ФЗ–152 от 27 июля 2006 года «О персональных данных» и 395–1-ФЗ «О банках и банковской деятельности» — в части, касающейся банковской тайны. Ряд норм нуждаются в дополнении и конкретизации, поскольку препятствуют информацией банку друг с другом и с правоохранительными органами о дропперах. То есть о лицах, напрямую занимающихся выводом и снятием наличными денежных средств, похищенных в результате киберпреступлений.

Подготовленный нами законопроект создаст правовую возможность формирования базы данных покушений на совершение переводов денежных средств без согласия клиента, включая удачные случаи. Главным оператором этой базы, согласно федеральному законодательству, будет ведущий государственный регулятор финансового сектора — Банк России. Кредитные организации обязаны будут направлять регулятору информацию обо всех подобных инцидентах. Объем и порядок предоставления такой информации будет устанавливаться ведомственными нормативными документами Банка России.

**Вадим КАЛУХОВ**

директор Департамента финансовых технологий, проектов и организации процессов Банка России

СХОДИТЬ В БАНК РАЗ В ЖИЗНИ

ДИСТАНЦИОННАЯ ИДЕНТИФИКАЦИЯ
БАНКАМИ НОВЫХ КЛИЕНТОВ
ПОВЫСИТ КОНКУРЕНТОСПОСОБНОСТЬ
ФИНАНСОВЫХ РЫНКОВ

В развитии дистанционного банковского обслуживания узким местом пока остаётся «первичный контакт» с клиентом. Чтобы заключить договор обслуживания и открыть первый счёт, гражданину необходимо пройти «физическую» идентификацию, непосредственный личный контакт с сотрудником банка. Крупные банки, способные содержать разветвлённую сеть офисов, оказываются в привилегированном положении на рынке. Создание возможности дистанционной идентификации банками новых клиентов поможет развитию конкуренции на финансовых рынках.

ВЕКТОР ДИСТАНЦИОННОСТИ

В настоящее время большинство банковских и платёжных сервисов выполняются дистанционно. Еще 10–15 лет назад дистанционное обслуживание предлагали далеко не все банки, и охватывало оно лишь отдельные операции. Например, клиенту предоставлялась возможность получить электронную выписку операций и движения средств на счёте. Это было модное нововведение, достаточно локальное, своего рода «фишечка».

Футурологи-оптимисты сулили новшеству блестящее будущее, но раньше всерьёз к ним прислушивались мало — подобные прогнозы не столь часто сбываются. Вспомним такую услугу, как телебанк, то есть совершение банковских операций посредством голосовой связи или тонального набора по телефону. Сейчас она мало где сохранилась и фактически отмирает, подобно тому как с развитием мобильной телефонии сошла на нет пейджинговая связь и некоторые другие виды телекоммуникаций.

Стоит отметить ещё одну тенденцию — к банкоматам возвращается их первоначальная функция выдачи и приёма наличных денежных средств. А ведь несколько лет назад была мода на их превращение в многофункциональные мини-офисы для самообслуживания клиентов. Банкоматы были оборудованы сканерами для считывания штрих-кодов бланков платёжных поручений и много ещё чем. Эта ветвь развития была достаточно востребована в определённый период времени, однако сегодня дополнительные услуги банкоматов не пользуются большим спросом.

В настоящее время оборот наличных денежных средств сокращается. Доля операций по оплате картами товаров и услуг за последние три года выросла более чем в два раза — с 13 до 29% — и продолжает увеличиваться. Рудиментом становится покупка недвижимости за наличные. Кроме того, заработная плата и социальные выплаты стали начисляться гражданам на счета банковских карт, всё больше используются электронные платежи, и такие возможности расширяются.

За прошедшее время положение дел в сфере дистанционного банковского обслуживания кардинально изменилось в лучшую сторону. Действий, требующих физического присутствия клиента в офисе банка, остаётся всё меньше. Хотя, конечно, какие-то услуги сохраняются, например, хранение в банковских сейфовых ячейках ценностей и важных документов. Средняя наполняемость ячеек по-прежнему достаточно высока — 70–80%.

УДОБНО И НЕДОРОГО

Сегодня подавляющее большинство финансовых операций совершается дистанционно. Бурно развивается, обрастая широким функционалом, интернет-банкинг — веб-сервисы и мобильные приложения. «Рабочим местом» клиента выступает персональный компьютер или мобильное устройство.

Появилась возможность дистанционного открытия и закрытия депозитов, создания регулярного платёжного поручения (автоплатежа, который выполняется банком с заданной периодичностью) и многого другого. Теперь клиенты банков при первой необходимости могут моментально переводить друг другу денежные средства. Не нужно забывать и о новых технологиях, которые могут внести свой вклад в развитие финансового рынка.

Банковские операции теперь можно выполнять в любое время и практически в любом месте — дома, на работе, в транспорте, на улице, за границей. Для клиентов это очень удобно: всё реже нужно лично посещать офис банка, не приходится тратить время на ожидание в очереди. Потребительские привычки меняются по мере распространения новых, более удобных и дешёвых сервисов.

Дистанционное обслуживание значительно сокращает банковские расходы на ведение бизнеса, в частности, на содержание офисов. Отделения банков перестают быть форпостами обслуживания клиентов, ассортимент и количество операций в них сокращаются. Уменьшается и количество рабочих мест сотрудников банка. Растет число «банков без офисов».

УЗКОЕ МЕСТО

«Узким местом» в расширении дистанционного банковского обслуживания остаётся необходимость для пользователя обязательно быть клиентом банка. Это возможно лишь после физической явки в офис и непосредственного контакта с сотрудником банка. В настоящее время такая операция должна совершаться лично гражданином для каждого банка, клиентом которого он хочет стать. Только после этого для него становятся доступными дистанционные банковские сервисы.

Идентификация, требующая «первичного» физического присутствия клиента в офисе банка или контакта с полномочным банковским представителем, накладывает ограничения на развитие конкуренции в отрасли. Вследствие этого у большинства банков офисов немного. Банки не могут позволить себе затраты на содержание своих отделений «в шаговой доступности» для большинства потенциальных клиентов. В привилегированном положении оказываются крупнейшие кредитные организации. Некоторые банки находят выход из положения, развиваясь как смежное направление других видов бизнеса, оказывающего услуги, которые требуют физического присутствия, например, торговых сетей или логистики — транспортировки посылок гражданам.

Ряд операций, которые уже можно осуществлять дистанционно (например, кредитование), банки пока предпочитают совершать по старинке, в офисах. Дело в том, что пока не существует полноценного электронного документооборота, который позволил бы клиенту дистанционно предоставлять банку весь пакет документов, необходимых для рассмотрения кредитной заявки.

Банк России в настоящее время совместно с заинтересованными ведомствами и организациями (Минкомсвязи России, ПФР и другими) работает над решением этой проблемы для того, чтобы необходимые документы могли быть запрошены банком с согласия клиента из баз данных государственных органов посредством Единого портала государственных и муниципальных услуг (функций). Среди них паспортные данные, прописка, семейное положение, налоговые выплаты и ряд других сведений, «первоисточником» которых является государство.

ЭЛЕКТРОННОЕ РЕШЕНИЕ

Таким образом, одной из операций, которую на данный момент нельзя совершить удаленно, остаётся пока первичная идентификация. Гражданин, желающий стать клиентом



банка, должен лично предъявить сотруднику этой кредитной организации удостоверяющий личность документ — паспорт гражданина Российской Федерации. После этого производится проверка подлинности паспорта, в том числе по государственным базам данных, а также другие процедуры идентификации личности гражданина; задаются вопросы по принципу «знай своего клиента».

Если у банка есть сомнения в источниках доходов потенциального клиента, он может отказать в обслуживании. Только после успешного прохождения перечисленных процедур возможно заключение договора банковского обслуживания клиента и открытие первого, «первичного» счёта. Последующие банковские операции — открытие новых счетов и так далее — клиент может совершать уже дистанционно, проходя электронные процедуры идентификации.

Необходимость физического присутствия, даже только для первичной идентификации клиента, всё равно создаёт определённую нагрузку на банки. Они вынуждены содержать сеть офисов в различных регионах страны и населённых пунктах, нести значительные финансовые затраты. Содержание сети офисов оказывается нерентабельным и по силам только крупным кредитным организациям. Во многих местах есть офисы только одного—двух-трёх банков, услуги остальных для клиентов недоступны. Это негативно отражается на конкуренции, препятствует равному доступу клиентов к банковским услугам и их удешевлению.

Процедура электронной, дистанционной первичной идентификации граждан, которые хотят стать клиентами банков, важна для развития кредитно-финансовой системы в целом, для усиления конкуренции. Нельзя забывать и о людях с ограниченными возможностями передвижения, для которых каждый выход из дома для визита в банковский офис — непосильная нагрузка. Это серьёзная социальная проблема, которая должна быть решена.

ТОЛЬКО ОДИН РАЗ

Банк России совместно с Минкомсвязи России, Росфинмониторингом и другими заинтересованными организациями, включая кредитно-финансовые, прорабатывает возможность дистанционной первичной идентификации клиента банка.

Суть предлагаемого решения в том, что человеку достаточно всего один раз физически пройти банковскую идентификацию, чтобы в дальнейшем дистанционно становиться клиентом других банков.

Полная идентификация гражданина, когда он становится клиентом банка, проводится всего один раз только одной кредитно-финансовой организацией. При этом проверяется действительность гражданского паспорта Российской Федерации, устанавливается личность, фиксируются паспортные и биометрические данные — делается фотопортрет, контрольная запись речи и так далее. Берётся письменное согласие гражданина на размещение этих данных в ЕСИА — Единой системе идентификации и аутентификации, используемой в качестве единого канала идентификации граждан, получающих услуги посредством ЕПГУ.

Кроме того, оформляется разрешение гражданина использовать эти данные для дистанционного заключения договора оказания услуг иными финансовыми организациями. Стандартный функционал профиля пользователя ЕСИА будет расширен, дополнен перечисленными проверенными данными (фотопортретом, записью речи и другими), а также согласием гражданина на их использование для указанных целей. Единоразово лично пройдя банковскую идентификацию, гражданин сможет дистанционно становиться клиентом других кредитно-финансовых организаций через интернет-ресурсы.

Для «первичной» дистанционной идентификации он сможет воспользоваться своим профилем в ЕСИА при помощи логина, пароля и номера мобильного телефона, зарегистрированных в ЕСИА. Дистанционно проводить идентификацию нового клиента банки смогут также при помощи сеанса видеосвязи — зафиксировать его фотопортрет, особенно произношения контрольной фразы и сравнить с имеющимися биометрическими образцами, получив через ЕСИА сведения о степени их совпадения. Дополнительно, при возникновении сомнений в достоверности идентификации или полученных сведений, банк может попросить клиента ответить на вопросы в рамках процедуры «знай своего клиента», согласно действующим нормам Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Такова суть решения, которое предлагается Банком России совместно с заинтересованными ведомствами и участниками финансовых рынков. Решение проходит «обкатку», подробно обсуждается на ключевых отраслевых деловых мероприятиях. Прошлой осенью дискуссия состоялась на Форуме инновационных финансовых технологий FINOPLIS 2016, а в 2017 году, как предполагается, она пройдет на IX Уральском форуме «Информационная безопасность финансовой сферы».

И, КОНЕЧНО, БЕЗОПАСНОСТЬ

Проводимая коллективная работа, безусловно, результативна: решение проходит предварительную апробацию и прорабатывается детально. Для осуществления задуманного понадобится развитие нормативно-правовой базы, на уровнях

как федерального законодательства, так и ведомственных регулирующих документов. Банк России является регулятором кредитно-финансовой сферы и своими нормативными документами, конкретизирующими положения федерального законодательства, устанавливает определенные правила для участников отрасли, в том числе по согласованию с профильными государственными органами может устанавливать требования и для дистанционной идентификации новых клиентов.

Есть все основания полагать, что уже в 2017 году станет ясно, в какие сроки это решение из идеи перейдет в стадию «дорожной карты» (со сроками реализации, ресурсами и ответственными за реализацию). В настоящее время ведется проработка вопросов безопасности предлагаемого решения как для государства, так и для кредитно-финансовых организаций и их клиентов.

Должна быть большая степень уверенности, что кредитно-финансовая организация в состоянии выполнить действующие нормы. Будет установлено, в какой форме (обязательной или рекомендательной) и для каких групп банков будут действовать новые положения. Всем банкам будет предоставлено право дистанционно идентифицировать новых клиентов. Но тем, кто будет этим правом пользоваться, придется выполнять установленные требования.

Может возникнуть вопрос, заинтересованы ли в дистанционной идентификации новых клиентов крупные банки с разветвленной сетью офисов. Не «перетекут» ли в результате их клиенты к конкурентам? Такие опасения безосновательны. Крупные банки в последнее время активно развивают дистанционные высокотехнологичные сервисы, сознательно идут на обострение конкуренции, в том числе друг с другом. У них есть возможность вкладывать значительные средства в развитие бизнеса, в передовые банковские технологии. Если взять мобильные приложения, то разработки крупных банков — среди лучших.

Кроме того, все банки заинтересованы в снижении издержек, в уменьшении количества офисов. К этому подталкивает значительное сокращение необходимости физических контактов банковских сотрудников и клиентов. Практическое использование дистанционной идентификации новых клиентов поможет банкам определить оптимальную модель офисной сети, найти новые формы сочетания в ней собственно банковского и других видов бизнеса.

* * *

Банк России как регулятор финансового рынка также заинтересован как в большей прозрачности отрасли и сокращении бумажного документооборота, так и в развитии конкуренции. Возможности дистанционной идентификации банками новых клиентов существуют далеко не во всех странах. Например, они уже есть в Швейцарии, Германии и Испании. Развитие безопасных дистанционных сервисов поможет сделать наш финансовый рынок высокотехнологичным и конкурентоспособным на глобальном уровне.



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

В статье очень хорошо изложена актуальность введения удалённой идентификации клиентов банков. Однако для решения проблемы выдвигаются предложения, игнорирующие накопленный международный опыт и рекомендации международных стандартов.

Первичная идентификация является одним из базовых элементов доверия к операциям, которые основываются на последующей идентификации и аутентификации субъектов. Личное присутствие и верификация идентификационной информации при первичной идентификации является необходимым условием для операций с высоким уровнем рисков в ряде международных стандартов, например, в ISO 29115. Только личное общение и ответы на определённые вопросы могут (при подготовке специалиста и технических возможностях проверки) дать определённую долю уверенности в подлинности предъявленных идентификационных данных. Идентификация по биометрическим данным имеет вероятностную природу. Увеличение хранилища биометрических образцов влечёт за собой существенный рост погрешности идентификации и времени отклика, что ставит под сомнение её применимость для массовой однозначной идентификации граждан. Примером отказа от биометрической идентификации клиентов после 5 лет работы и неоправданных вложений является банк Халык в Казахстане. Биометрия может использоваться как дополнительное средство идентификации с невысоким уровнем доверия к результатам.

Приведённые примеры Испании, Швейцарии и Германии, на которые ссылается автор, требуют внимательно-го анализа. Введение дистанционной первичной идентификации было бы возможно, но (как это реально сделано там) с большими ограничениями и весьма аккуратно, с просчитанными рисками для определённых операций.

Попытка перепрыгнуть пропасть, разделяющую наши страны, в один прыжок, уже была показательно сделана в виде шумного, но недавно закрытого проекта УЭК. Этот пример показал, что для развития таких проектов должна быть выстроена мощная и взаимосвязанная инфраструктура доверия, на базе которой должны функционировать отлаженные сервисы не для «отчета наверх», а реально работающие, и, главное, необходимые гражданам.

BIS-КОММЕНТАРИЙ

Так, надежда на ЕСИА, являющейся центральной частью предлагаемого плана, по моему мнению, сильно преувеличена. Хранилище идентификационных данных ЕСИА примерно на десятки миллионов самых активных трудоспособных граждан наполнено не слишком достоверной информацией, за которую не хотят и не могут отвечать чиновники Минкомсвязи. Причина проста: согласно ст. 8 152-ФЗ и п. 3.5 Руководства пользователя ЕСИА, версия 2.1 выпуска 2014 г., любой гражданин может в любой момент внести исправления в свои данные по упрощённой учётной записи (это большая часть записей физ.лиц). Наполняя эту базу дополнительной информацией, надо понимать, что уровень достоверности данных поднимется с сегодняшнего почти нуля незначительно и не сразу.

Специалисты по защите информации в банковском сообществе знают, что около 80% клиентов банка являются добропорядочными гражданами, а как минимум 5% клиентов банков являются по крайней мере потенциальными нарушителями, борьба с которыми ведётся десятилетиями. Предлагаемые механизмы удалённой идентификации без тщательной проработки и оценки рисков могут открыть «ящик Пандоры» для развития систематических финансовых нарушений, размер которых быстро может вырасти с 5% до 20 и даже 30%, поскольку мошенники получат возможность пользоваться полученной «дырой» в безопасности многократно.

Если уж браться за решение проблемы удалённой идентификации клиентов, то решать её надо на основе европейского опыта и с учётом международных стандартов, таких, как ISO/IEC 24760, ITU-T Y.2720, X1252, X.1255. Суть стандартов — в управлении идентификационной информацией граждан по уровням доверия. Трансляция доверия к идентификации от одной организации к другой — отдельная задача, решение которой имеет не только техническую, но и ряд других составляющих — правовую, нормативную, организационную, страховую и т.д. Крупнейшие банки могут объединиться и создать свою, «банковскую ЕСИА», персонально отвечая за первичную идентификацию клиентов, тщательно следя за достоверностью и защищённостью собираемой информации, как это сделано в Норвегии и ряде других стран. При этом имеется ряд условий. Например, применяемые системы защиты должны быть прозрачными и понятными для клиентов и банков, иначе не появится доверие клиента на бытовом уровне... Процесс создания межбанковского центра доверия к идентификации может возглавить Банк России. Коммерческие банки и граждане оценят этот шаг, и это может послужить во благо делу информатизации общества в России.



Артём СЫЧЕВ
заместитель начальника
ГУБЗИ Банка России



Сергей ВИХОРЕВ
директор по ИБ филиала
«ПЕТЕР-СЕРВИС
Спецтехнологии»

ПОГОВОРИМ ОБ АУТСОРСИНГЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ЭССЕ НА ТЕМУ, КАК ВОВКА
В ТРИДЕВЯТОМ ЦАРСТВЕ
АУТСОРСИНГ ПОЛЬЗОВАЛ

Окончание.
Начало в № 4(23)/2016 г.

Соглашение об уровне предоставления услуг (SLA)

Соглашение об уровне предоставления услуг (SLA) — это формальный договор между заказчиком и поставщиком услуги, гарантирующее предоставление услуги с уровнем качества не ниже согласованного и содержащее:

- ♦ описание состава предоставляемой услуги (сервиса);
- ♦ обязательства поставщика услуг и условия предоставления услуг;
- ♦ права и обязанности сторон, описание и распределение зон ответственности;
- ♦ согласованный уровень качества услуги (перечень ключевых параметров качества);
- ♦ описание расчета ключевых параметров качества и частоты отчетов;
- ♦ методы и средства контроля ключевых параметров качества;
- ♦ описание процедуры контроля за исполнением соглашения;

♦ описание процедуры отчетов о проблемах и условия эскалации проблем;

♦ описание процедуры восстановления работы в случае перебоев;

♦ описание процедуры решения рассогласований (спорных вопросов);

♦ описание процедуры запросов на изменение;

♦ описание порядка платежей, связанных с оказанием услуги (сервиса).

Описание состава услуги, предоставляемой поставщиком услуг, должно содержать:

♦ стороны, вовлеченные в соглашение, и сроки действия соглашения;

♦ общее описание услуги;

♦ функции безопасности информации, реализуемые поставщиком услуг;

♦ состав используемого программного и аппаратно-программного обеспечения;

- ♦ местоположение оборудования, используемого для оказания услуги;
- ♦ каналы связи, используемые поставщиком услуг для оказания услуги;
- ♦ состав входящей информации, обеспечивающей выполнение услуги;
- ♦ процедуры, используемые поставщиком услуг и порядок их применения;
- ♦ стандарты безопасности информации, используемые поставщиком услуг;
- ♦ наличие необходимых лицензий у поставщика услуг на выполнение работ;
- ♦ наличие лицензий на использование задействованного программного обеспечения;
- ♦ состав работников, занятых для оказания услуги, их функции, роли и обязанности;
- ♦ уровень квалификации работников, занятых для оказания услуги;
- ♦ состав ведущейся поставщиком услуг документации и отчетность по услуге.

Контрольные параметры качества услуги (сервиса), вносимые в соглашение, должны быть измеримыми и представляться в виде числовых метрик. Состав ключевых параметров качества зависит от состава заказываемых услуг. Для выбора ключевых параметров качества рекомендуется использовать стандарты ITIL и COBIT. Например, в качестве параметров качества услуги могут выступать:

- ♦ Время реакции на обращение пользователя — время, прошедшее с момента поступления и регистрации запроса на обслуживание (сообщение пользователя о проблеме) до момента фактического начала работ по факту обращения.
- ♦ Время решения проблемы — время, прошедшее с момента фактического начала работ над проблемой до закрытия заявки. Временем начала работы над проблемой считается момент отправки заказчику уведомления о начале работ. Временем решения проблемы считается момент отправки заказчиком сообщения, подтверждающего закрытие заявки.
- ♦ Время жизни инцидента — суммарное время, прошедшее с момента поступления и регистрации обращения, до момента закрытия заявки на обслуживание.
- ♦ Минимальное время реакции исполнителя — минимальное время, необходимое поставщику услуг при аварийных ситуациях для устранения их последствий.
- ♦ Уровень брака — это количественное или процентное выражение количества сбоев, включающее в себя число отказов за отчетный период, число случаев несоблюдения сроков и случаев предоставления услуги неприемлемого качества, приведших к необходимости ее повторного оказания.
- ♦ Техническое качество — в случае разработки приложений в режиме аутсорсинга этот критерий определяет уровень технического качества предоставленного программного кода. Контроль за этим параметром обычно



осуществляется при помощи коммерческих программных инструментов, проверяющих такие характеристики, как длина кода, уровень структурированности, уровень сложности, а также погрешности кода.

- ♦ Доступность услуги — количество времени или временной промежуток, в котором услуги, предоставляемые поставщиком услуг, остаются доступными. Параметр может принимать значения «да» или «нет». Оговаривается допустимый уровень (максимальное время недоступности).
- ♦ Средняя доступность услуги — среднее количество сбоев (фактов, когда предоставляемые поставщиком услуг, остаются доступными) за период предоставления услуги.
- ♦ Удовлетворенность сервисом — степень удовлетворенности заказчика услуг уровнем предоставленной поставщиком услуги (сервиса). Параметр определяется отдельно для каждой значимой функции при помощи внутренних и внешних опросов. Опросы могут проводиться нейтральной третьей стороной.

Количество параметров качества услуги (сервиса), вносимых в соглашение, должно быть минимальным, но достаточным для проведения объективной оценки качества предоставляемой услуги. При выборе значений показателей параметров качества услуги (сервиса) можно исходить из текущего состояния процесса, передаваемого на аутсорсинг. Установленные параметры должны быть достижимы в текущей обстановке и при существующих обстоятельствах. При определении метрик параметров качества услуги (сервиса) необходимо учитывать, что разные работники заказчика могут требовать разных условий оказания одних и тех же услуг.

В соглашении об уровне предоставления услуг должна быть также отражена ответственность заказчика при использовании услуги (сервиса), например:

- ♦ необходимость подготовки и поддержки соответствующих конфигураций оборудования и программного обеспечения;

- ♦ соблюдение правил настройки и проведения регламентных работ;

- ♦ процедура изменения согласованной конфигурации.

Соглашение об уровне предоставления услуг требует периодического пересмотра и внесения изменений в случаях изменения:

- ♦ внешних обстоятельств;

- ♦ ожиданий и/или потребностей заказчика;

- ♦ рабочей нагрузки;

- ♦ появление лучших средств, процедур и параметров измерения качества услуг.

Соглашение о конфиденциальности (NDA)

Соглашение о конфиденциальности (NDA) — это формальный договор между заказчиком и поставщиком услуги, направленный на урегулирование вопросов обмена информацией, подлежащей защите, и создания правового основания для возложения на виновную в нарушении конфиденциальности информации сторону обязанности по компенсации убытков невиновной стороне.

Соглашение о конфиденциальности является одной из мер по защите информации, но самостоятельно не является достаточным механизмом защиты информации. Для создания правовой основы действия Соглашения о конфиденциальности, как правового механизма, позволяющего защитить коммерческую тайну, у заказчика должен быть введен режим коммерческой тайны в соответствии с законодательством Российской Федерации, а само соглашение должно учитывать требования этого законодательства и включать следующие существенные условия:

- ♦ предмет соглашения, определение конфиденциальной информации;

- ♦ формы и способы предоставления конфиденциальной информации;

- ♦ условия обеспечения конфиденциальности информации;

- ♦ сроки действия режима конфиденциальности информации;

- ♦ права и обязанности сторон по сохранению конфиденциальности информации;

- ♦ допустимость раскрытия конфиденциальной информации в определенных случаях;

- ♦ ответственность за нарушение Соглашения о конфиденциальности;

- ♦ порядок разрешения споров.

При определении предмета соглашения необходимо закрепить в Соглашении о конфиденциальности полный перечень информации, которая не подлежит разглашению и требует защиты. Целесообразно использовать перечень (выписку из перечня) информации, составляющий коммерческую тайну у заказчика. Необходимо также в данный перечень включать информацию, подлежащую защите в силу закона (персональные данные, банковская тайна и др.) и которая может стать известной поставщику услуг при оказании услуги.

При определении форм и способов представления информации необходимо исходить из того, что информация может передаваться как в письменной или электронной форме, так и устно. При этом необходимо определить порядок маркирования (нанесения грифа, атрибутирования) на носители информации и порядок фиксирования конфиденциальности устной информации.

При определении условий обеспечения конфиденциальности необходимо:

- ♦ определить состав мер, которые надлежит исполнить для защиты информации;

- ♦ регламентировать порядок защиты, хранения, обмена (предоставления) информации;

- ♦ установить порядок допуска работников поставщика услуг к защищаемой информации;

- ♦ определить порядок возврата и/или уничтожения информации по окончании услуги.

Сроки действия режима конфиденциальности определяются по согласованию сторон, но не могут быть меньше сроков хранения документов и соблюдения конфиденциальности, установленных законодательством Российской Федерации для различных видов информации.

При определении прав и обязанностей сторон в Соглашении о конфиденциальности необходимо отразить право заказчика осуществлять контроль за соблюдением установленного режима защиты информации и обязанность поставщика услуг предоставлять возможность такого контроля. Необходимо также оговорить право сторон на обращение в суд за разрешением спорных вопросов и истребование понесенных убытков (ущерба).

В Соглашении о конфиденциальности должны быть оговорены случаи, при которых допускается раскрытие конфиденциальной информации, предусмотренные законодательством.

Меры ответственности сторон за нарушение Соглашения о конфиденциальности определяются в соответствии с общими нормами, установленными ст. ст. 15, 330, 394 ГК РФ и могут включать как возмещение убытков в полном объеме, так и реального ущерба.

При определении порядка разрешения споров, целесообразно использовать обязательный претензионный досудебный порядок разрешения споров.

Требования по безопасности информации

Составление Требований по безопасности информации характерно для технологических сервисов безопасности информации и, в частности, при оказании услуг:

- ♦ по реализации мер защиты;

- ♦ по предоставлению защищенной инфраструктуры ИС;

- ♦ по обработке защищаемой информации.

Не будем забывать, что ответственность за правильный выбор мер защиты и формирование требований к механизмам и функциям защиты лежит на заказчике. В случае, если поставщик услуг в рамках оказания услуги проводит оценку угроз безопасности информации и состояния защищенности информационной системы заказчика, он может подготовить

предложения по необходимым требованиям безопасности информации, однако, окончательное решение о достаточности данных требований принимает непосредственно заказчик.

Требования по безопасности информации, которые надлежит выполнить поставщику услуг, могут быть оформлены в виде ссылки на необходимость выполнения требований, изложенных в руководящих и методических документах ЦБ РФ, ФСТЭК России и ФСБ России для соответствующего класса защищенности используемых средств защиты, либо как самостоятельный документ, описывающий конкретные функции (механизмы) безопасности и их параметры, которые должны быть реализованы при оказании услуги.

В качестве методического материала при выборе требований к механизмам (функциям) безопасности информации можно использовать «Методический документ ФСТЭК России. Меры защиты информации в государственных информационных системах», утвержденный 11.02.2014 г.

Поручение на обработку защищаемой информации

Поручение на обработку информации характерно при передаче поставщику услуг обработки информации (технологический сервис), в том числе обязательно для сведений, содержащих персональные данные. При этом, поручение должно содержать:

- ♦ цель обработки и состав персональных данных, подлежащих обработке;
- ♦ перечень действий (операций) поставщика услуг с обрабатываемой информацией;
- ♦ уровень защищенности ИС, который должен быть обеспечен;
- ♦ требования к защите обрабатываемой информации;
- ♦ порядок уничтожения информации по завершении обработки;
- ♦ порядок оценки эффективности принятых мер защиты.

Регламент взаимодействия

Регламент взаимодействия — документ, определяющий порядок взаимодействия подразделений и работников поставщика услуг и заказчика в рамках процесса предоставления услуги (сервиса). Регламент представляет собой свод правил принятия решений исполнителями в разных ситуациях и позволяет организовать горизонтальные взаимодействия подразделений и/или работников поставщика услуг и заказчика услуг. Регламент должен содержать:

- ♦ терминологию, используемую при оказании услуги;
- ♦ состав процессов, регулируемых регламентом;
- ♦ порядок инициирования, выполнения, эскалации и закрытия регулируемых процессов;
- ♦ порядок контроля исполнения процессов.

В качестве формы регламента можно использовать ГОСТ Р 6.30–2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».

Регламент может содержать описание процессов взаимодействия подразделений и/или работников поставщика услуг и заказчика при:

- ♦ нештатных ситуациях;
- ♦ инцидентах безопасности информации;
- ♦ при эскалации возникающих проблем;
- ♦ осуществлении контроля и мониторинга качества предоставляемых услуг;
- ♦ размещении и эксплуатации оборудования и программного обеспечения;
- ♦ обеспечении физического допуска на объекты поставщика услуг.

Конкретный состав регламентируемых процессов определяется объемом и составом предоставляемых услуг. При описании регламентируемых процессов надо указывать:

- ♦ событие, запускающее процесс;
- ♦ событие, завершающее процесс;
- ♦ срок выполнения процесса;
- ♦ место выполнения процесса;
- ♦ функции (действия), выполняемые в рамках процесса;
- ♦ правила и методы выполнения процесса;
- ♦ исполнителей процесса;
- ♦ права и ответственность исполнителей;
- ♦ средства документирования процесса;
- ♦ средства контроля выполнения процесса.

К событиям, запускающим процесс (наступление определенных условий), как правило, относятся:

- ♦ получение внешнего сигнала или воздействия (должны быть указаны допустимый вид и источник такого сигнала);
- ♦ инициатива определенных работников (право инициативы должно быть установлено нормативным актом);
- ♦ достижение определенных (критических) значений контролируемыми параметрами (должны быть указаны величины значений);
- ♦ наступление определенных сроков (календарных или относительных).

Событие, завершающее процесс, состоит, как правило, в получении всех требуемых выходных объектов и достижении цели регулируемого процесса. Момент события, завершающего процесс, как правило, жестко связан с моментом учета выполнения данного процесса.

Срок выполнения процесса задается либо как общая продолжительность процесса с момента запуска процесса до момента его завершения, либо как требуемое время завершения процесса. Для учета выполнения процесса, рекомендуется в регламенте предусмотреть порядок фиксации моментов запуска и завершения процесса.

Функции (действия), выполняемые в рамках процесса, должны соответствовать функциям, установленным в должностных инструкциях, положениях о подразделениях.

В регламенте указываются конкретные исполнители процесса. В случае, если указать конкретного исполнителя невозможно, в рамках регламента надо определить роль (совокупность функций, прав и ответственности), необходимую для выполнения регулируемого процесса и установить порядок определения конкретного работника, исполняющего данный процесс. Указываемый исполнитель должен соответствовать масштабу процесса.

В регламенте четко фиксируются моменты передачи управления процессом (или передачи объектов процесса) от одного исполнителя к другому.

Как приложение к регламенту могут оформляться графические схемы процессов, описываемых регламентом, которые служат для иллюстративных, облегчающих понимание регламента целей и не заменяют собой текст регламента. Такие схемы, как правило, оформляются для часто повторяющихся процессов.

ЧАСТЬ 4. КТО ЛУЧШЕ?

Действительно, кто лучше? Кого выбрать поставщиком услуг безопасности информации? Вопрос далеко не праздный. Авторы уже не раз отмечали, что отношения между поставщиком услуг и заказчиком строятся на доверии. А доверие, в свою очередь, определяется той степенью осведомленности заказчика о деятельности поставщика, которую он может себе позволить. Поэтому, на предварительном этапе необходимо сосредоточиться на всесторонней оценке претендента и подходить к этому так, как подходит расчетливая будущая теща к выбору будущего зятя. К оценке поставщика услуг надо привлекать все силы службы собственной безопасности заказчика, риск-менеджеров и всех, кто отвечает за оценку контрагентов. Такая оценка должна проводиться на основе сбора и анализа информации, имеющейся в открытом доступе, а также сведений, предоставляемых самим поставщиком услуг или полученных в ходе предварительных переговоров. Каждый поставщик должен соответствовать тем требованиям, которые выдвигает заказчик. А требования эти могут быть как объективные, так и субъективные.

Объективные требования к поставщику услуг

При выборе поставщика услуг (сервисов) безопасности информации необходимо удостовериться в наличии у него:

- ♦ необходимых лицензий;
- ♦ необходимых ресурсов производственных мощностей;
- ♦ системы менеджмента сервисами и качеством;
- ♦ квалифицированных кадров;
- ♦ опыта оказания аналогичных услуг;
- ♦ аттестата соответствия требованиям безопасности или
- ♦ заключения независимых экспертов.

Большинство видов услуг (сервисов) безопасности информации, а также передачи информации, относятся к лицензируемым видам деятельности. В соответствии с законодательством Российской Федерации поставщик услуг должен иметь действующую на все время оказания услуги и на территории, на которой осуществляет деятельность заказчик услуги:

- ♦ Лицензию на оказание телематических услуг связи¹ — для поставщиков операционных и технологических сервисов,



связанных с предоставлением хостинга, доступа в Интернет, электронной почты, доступа к информации с использованием инфокоммуникационных технологий.

- ♦ Лицензию на оказание услуг по предоставлению каналов связи в соответствии² — для поставщиков технологических услуг (услуга по предоставлению защищенной инфраструктуры ИС), связанных с предоставлением (арендой) каналов связи.

- ♦ Лицензию на деятельность по технической защите конфиденциальной информации³, в том числе на проектирование в защищенном исполнении средств и систем информатизации, установку, монтаж, испытания, ремонт средств защиты информации, защищенных программных (программно-технических) средств обработки информации — для всех поставщиков сервисов (услуг) безопасности информации.

- ♦ Лицензию на деятельность по технической защите конфиденциальной информации⁴, в том числе контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации — для поставщиков управленческих сервисов безопасности информации.

- ♦ Лицензию на предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей⁵ — для поставщиков технологических сервисов (услуга по реализации мер защиты, услуга по предоставлению

¹ Постановление Правительства Российской Федерации от 18.02.2005 г. № 87

² Постановление Правительства Российской Федерации от 18.02.2005 г. № 87

³ Постановление Правительства Российской Федерации от 03.02.2012 г. № 79

⁴ Постановление Правительства Российской Федерации от 03.02.2012 г. № 79

⁵ Постановление Правительства Российской Федерации от 16.04.2012 г. № 313

защищенной инфраструктуры ИС), связанных с использованием средств криптографической защиты информации.

♦ Лицензию на предоставление услуг по имитозащите информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей⁶ — для поставщиков технологических сервисов (услуга по предоставлению защищенной инфраструктуры ИС, услуга по обработке защищаемой информации, услуга по реализации мер защиты), связанных с использованием имитозащиты обрабатываемой информации.

♦ Лицензию на предоставление юридическим и физическим лицам защищенных с использованием шифровальных (криптографических) средств каналов связи для передачи информации⁷ — для поставщиков технологических сервисов, связанных с предоставлением (арендой) каналов связи.

♦ Лицензию на изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств⁸ — для поставщиков технологических сервисов безопасности информации (услуга по реализации мер защиты, услуга по предоставлению защищенной инфраструктуры ИС), связанных с формированием и использованием сертификатов электронных подписей или формированием исходной ключевой информации.

Оценка необходимых ресурсов и производственных мощностей поставщика услуг связана с тем, что при оказании услуги заказчик услуги непосредственно присутствует в процессе, передаваемом на аутсорсинг, а также с необходимостью индивидуализации предоставляемого сервиса под нужды заказчика. При изучении наличия необходимых ресурсов и производственных мощностей поставщика услуг необходимо оценить:

- ♦ объемы выделяемых ресурсов для предоставления услуги;
- ♦ наличие у поставщика услуг собственных средств и специалистов;
- ♦ наличие и достаточность для оказания услуги производственных площадей;
- ♦ номенклатуру (спецификацию) имеющихся у поставщика услуг средств и ресурсов;
- ♦ наличие резервного оборудования и мощностей, используемых для оказания услуги;
- ♦ период времени, необходимый на получение ресурсов.

Оказание сервиса (услуги) безопасности информации предполагает необходимость управления персоналом поставщика услуг, регламентации процессов и системы обеспечения безопасности информации, задействованных при

оказании услуги. При изучении системы менеджмента сервисами и качеством поставщика услуг необходимо изучить:

- ♦ организацию управления процессами у поставщика услуг;
- ♦ организацию управления качеством предоставляемой услуги;
- ♦ организацию управления безопасностью информации.

Для оценки организации управления целесообразно опираться на требования национальных стандартов Российской Федерации⁹.

Соответствие требованиям данных стандартов свидетельствует о некотором уровне надежности поставщика и добротности его компании, поэтому целесообразно, чтобы поставщик услуг имел соответствующие сертификаты соответствия требованиям данных стандартов, являющихся внешним независимым подтверждением достижения требований стандарта.

При рассмотрении сертификатов необходимо обращать внимание на объект оценки, которая должна соответствовать содержанию предоставляемой услуги (сервиса). Необходимо также учитывать, что наличие сертификата соответствия требованиям ГОСТ Р ИСО/МЭК 27001–2006 свидетельствует о наличии у поставщика услуг системы управления информационной безопасностью, но не гарантирует соответствие самой системы обеспечения безопасности установленным требованиям.

Квалификация и компетентность работников поставщика услуг, участвующих в оказании услуги, оценивается по наличию у них сертификатов производителей оборудования и программного обеспечения, свидетельств обучения и повышения квалификации по направлению информационных технологий и обеспечения безопасности информации, стажа работы по требуемым направлениям деятельности.

При оценке квалификации и компетентности работников поставщика услуг, необходимо убедиться, что внутренними документами поставщика услуг определен порядок организации работ по повышению квалификации (профессиональному обучению и (или) дополнительному образованию) работников.

Опыт оказания аналогичных услуг оценивается по предоставляемым поставщиком услуг сведений о таких работах и анализу запросов о качестве услуг, направляемых в адрес предшествующих заказчиков или публичных отзывов о деятельности поставщика услуг.

Наличие аттестата соответствия требованиям безопасности или заключения независимых экспертов является свидетельством того, что система обеспечения безопасности информации поставщика услуг соответствует установленным требованиям по безопасности информации. При этом, необходимо оценить достаточность подтвержденного уровня защищенности информационной системы поставщика услуг требуемому для заказчика услуг.

⁶ Постановление Правительства Российской Федерации от 16.04.2012 г. № 313

⁷ Постановление Правительства Российской Федерации от 16.04.2012 г. № 313

⁸ Постановление Правительства Российской Федерации от 16.04.2012 г. № 313

⁹ ГОСТ Р 54869–2011, ГОСТ Р 54870–2011, ГОСТ Р 54871–2011, ГОСТ Р ИСО 9001–2015, ГОСТ Р ИСО/МЭК 2000, ГОСТ Р ИСО/МЭК 27001–2006

Субъективные требования к поставщику услуг

При выборе поставщика услуг должны учитываться также качественные показатели. К таким показателям относятся:

- ♦ сведения о владельцах и администрации поставщика услуг;
- ♦ специализация поставщика услуг;
- ♦ репутация (имидж) поставщика услуг;
- ♦ отсутствие негативных сообщений о нем в средствах массовой информации;
- ♦ кредитоспособность и финансовое положение поставщика услуг;
- ♦ конкурентное положение (рейтинг) поставщика услуг на рынке аналогичных услуг;
- ♦ способность к контакту и длительным доверительным отношениям;
- ♦ психологический климат в трудовом коллективе поставщика услуг, риск забастовок.

Негативная оценка хотя бы по одному из таких показателей может служить поводом в отказе от его услуг.

Мониторинг порядка и качества предоставления услуг

При аутсорсинге главное правило: доверяй, но проверяй! Поэтому вопросу мониторинга порядка и качества предоставления услуг поставщиком надо уделять особое внимание. Такой мониторинг может проводиться на основе:

- ♦ анализа отчетов провайдера услуг;
- ♦ опроса работников (потребителей) заказчика услуг;

- ♦ инспекционного контроля;
- ♦ мониторинга с привлечением третьей стороны.

Не будем забывать, что именно поставщик услуг должен организовать мониторинг предоставления услуги по оговоренным с заказчиком параметрам, это и в его интересах. Результаты мониторинга предоставляются заказчику периодически или по требованию.

Со своей стороны, заказчик должен организовать регулярный опрос работников (потребителей) с целью определения качества услуг, предоставляемых поставщиком и удовлетворенности ожиданий. Такой опрос проводится на основе заранее разработанных опросных листов (чек-лист), охватывающих основные параметры предоставляемой услуги и оценку ожиданий потребителя.

Инспекционный контроль проводится на основе договоренностей с поставщиком услуг и в объеме, установленном в договорных документах (не забудьте включить это в договор). Заказчик должен иметь возможность проведения внезапного инспекционного контроля.

При наличии возможности, контроль услуг может производиться заказчиком путем получения и анализа информации с использованием предоставленных поставщиком услуг консолей мониторинга и управления.

Для оценки выполнения порядка и качества предоставляемой услуги может привлекаться третья независимая сторона, которая осуществляет такую оценку на основе опроса работников поставщика и заказчика и анализа результатов

BIS-КОММЕНТАРИЙ

Алексей МАЛЬНЕВ
заместитель директора департамента ИБ
АМТ ГРУП

Уже несколько лет, развивая собственную услугу AMTSOC, мы активно участвуем в различных публичных мероприятиях, посвященных темам аутсорсинга ИБ, Security as a Service и SOC (Security Operation Center). По моим наблюдениям, у участников рынка формируется разное понимание сути и структуры типовой услуги информационной безопасности. Особенно это касается услуги SOC. Причина заключается в том, что значительная часть сервис-провайдеров услуг аутсорсинга ИБ работает «по наитию», то есть, отталкивается от текущих клиентских запросов. В то время как другие реализуют оптимальный подход с точки зрения бизнеса. Как это ни странно, в ре-

зультате вторые часто оказываются правы и становятся ближе к рынку.

В этом контексте Артём Михайлович и Сергей Викторович попытались решить важную задачу и сделать то, что давно назревало и было необходимо рынку: расставить все точки над i, фундаментально описав (насколько это возможно в формате статьи) структуру сервисов информационной безопасности через призму российской практики и нормативно-правовой базы.

Для дополнения картины к описанному авторами можно добавить рыночную оценку востребованности сервисов информационной безопасности. В терминологии авторов статьи у нас есть управленческие, операционные и технологические сервисы информационной безопасности. Говоря о рыночной оценке, я имею в виду анализ спроса и предложения на сервисы каждой из трёх групп. При этом я бы добавил в категоризацию разделение по периодичности использования услуги аутсорсинга ИБ:

- ♦ Единовременные сервисы;
- ♦ Периодические сервисы;
- ♦ Постоянные сервисы (перманентные).

Обращаю внимание, что я здесь рассмотрю только перманентно (постоянно) оказываемые услуги ИБ. Это свойственно, например, таким услугам, как SOC, и это же определяет состав данных услуг.

технического мониторинга, предоставляемого поставщиком услуг или проводимого самостоятельно.

Эпилог

Резюмируя все сказанное, можно отметить, что аутсорсинг безопасности информации возможен и даже где-то полезен. Да, особенности есть, их надо помнить и учитывать, но ничего невозможного нет. Хотя... В заключении несколько слов о проблемах применения аутсорсинга в госучреждениях и иже с ними. Встает вопрос, могут ли такие учреждения применять схему аутсорсинга? Вопрос не праздный. Теоретически — да, никто не запрещает. А на практике? Мы много говорили о том, что отношения между поставщиком и заказчиком услуг строятся на доверии, которое во многом зависит от изучения возможностей и репутации поставщика. И в то же время, законом прямо определено: не допускается включение в документацию о закупке требований к участнику закупки, в том числе требования к квалификации участника закупки, включая наличие опыта работы, а также требования к деловой репутации участника закупки, требования к наличию у него производственных мощностей, технологического оборудования, трудовых, финансовых и других ресурсов, необходимых для выполнения работы или оказания услуги, являющихся предметом кон-



тракта¹⁰. Вот и приплыли. Либо покупай кота в мешке, либо откажись от аутсорсинга...

¹⁰ Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», ст. 33, часть 3.

Во-первых, если глобально оценить рыночную ситуацию, то основной мотивацией бизнеса к использованию внешних услуг аутсорсинга ИБ является снижение издержек. В реалиях бизнеса это должно обеспечиваться весомым преимуществом OPEX-модели над CAPEX-моделью (порядка 30–50%) в течение четырех и более лет, вплоть до преимущества OPEX в любой перспективе. И это тот случай, когда правильное конструирование услуги способно создать на нее спрос.

Напрашивается два очевидных условия, при которых для провайдера обеспечивается экономическая эффективность permanently предоставляемой услуги:

1. Возможность эффективно разделять между клиентами время узкоспециализированных, высококвалифицированных специалистов;
2. Возможность эффективно разделять общие вычислительные ресурсы (например, «в облаке»), на которые будут переведены рутинные операции в рамках процессов ИБ.

С учетом описанных условий и перманентного характера оказания сервиса, на мой взгляд, реальным спросом будут обладать:

- Операционные сервисы:
- ♦ обучение персонала;

- ♦ расследование инцидентов (форензика).

Технологические сервисы:

- ♦ Оценка безопасности продуктов и ИС;
- ♦ Услуги по разработке прикладного ПО;
- ♦ Услуги по обработке защищаемой информации (в части «облачных» ресурсов, которые можно разделять между большим количеством абонентов услуги).

Собственно, SOC, как перманентно оказываемая услуга, постепенно сводится к узкому набору сервисов. И именно поэтому мы приходим к тому, что реальный состав SOC-сервисов, как правило, весьма мал: SIEM-аналитика и мониторинг + форензика, с рядом дополнительных опций в виде контроля защищенности и элементов реагирования. Как можно заметить, сервисов из управленческой группы здесь нет. Постоянно оказываемые услуги управленческого типа, в основном, будут дорогими и сопоставимыми по стоимости с содержанием собственных команд ИБ. А периодические управленческие сервисы (аудиты) — не входят в наше рассмотрение.

Что касается сервиса AMTSOC, то помимо указанного набора, нам удалось несколько расширить список экономически эффективных услуг в силу и за счёт наличия большого сервисного центра, функционирующего более 20 лет и оптимального набора используемых инструментов ИБ.



Игорь НОВИКОВ
начальник Центра
по информационной
безопасности
Сбербанка

ЯЗЫК, ПОНЯТНЫЙ БИЗНЕСУ

ОПЫТ ВЗАИМОДЕЙСТВИЯ ИБ И БИЗНЕС-ПОДРАЗДЕЛЕНИЙ В СБЕРБАНКЕ

Со времён строительства Вавилонской башни люди знают, как важно взаимопонимание при работе над крупным проектом. С тех пор, как первый небоскрёб был разрушен, разногласия встают на пути к эффективному сотрудничеству. Найти точки соприкосновения в команде — основа успеха. В сфере информационной безопасности, например, часто возникает задача наладить общий язык с бизнесом.

Если в маленьких организациях решение этой проблемы зависит от умения специалиста по информационной безопасности доносить до руководства необходимость во внедрении тех или иных технологий, то в крупных компаниях, где ИТ- и ИБ-департаменты насчитывают сотни человек, этот вопрос требует нетривиальных решений. Так, в Сбербанке для выстраивания диалога между бизнесом, ИТ- и информационной безопасностью создали центр взаимодействия службы ИБ с бизнес- и функциональными блоками.

КАК ПРЕОДОЛЕТЬ КРИЗИС РОСТА

Ещё десять лет назад служба ИБ была автономной, успешно функционирующей в вертикали территориальных подразделений структурой Банка. Её сотрудники участвовали в согласовании бизнес-процессов и проектов по внедрению новых технологий. Производили оценку рисков, формировали базу требований к разработке и сопровождению информационных систем и оснащению автоматизированных рабочих мест, вычислительных ресурсов, использованию криптографических средств и парольных политик. Бизнес- и ИТ-подразделения старались

следовать требованиям, которые предъявляются к обеспечению информационной безопасности. Особых сложностей во взаимодействии этих служб на тот момент не было: их специалисты общались по сложившимся рабочим каналам связи.

Проблемы при взаимодействии с бизнес-подразделениями стали возникать с началом роста цифровых технологий, ускорением бизнес-процессов и централизацией инфраструктуры Сбербанка. Границы Банка стали расширяться, появились сложные интеграционные решения, началось активное вовлечение сотрудников в оптимизацию производственных процессов в рамках внедрения технологий «бережливого производства». В разы расширилась проектная деятельность в бизнес-блоках. Одновременно было расформировано подразделение банковских технологий, которое занималось внедрением новых продуктов. Эта задача перешла в бизнес-подразделения Банка. Схема взаимодействия с банковскими технологами, которые понимали требования по обеспечению информационной безопасности и закладывали их при проектировании новых автоматизированных банковских систем (АС) и процессов, была нарушена.

НЕ В НОГУ!

Службы информационной безопасности Банка не сразу сумели перестроиться под новые условия работы, поэтому из-за недостатка коммуникаций сотрудники из бизнес-подразделений либо совсем не обращались в Департамент информационной безопасности, либо обращались в середине, а то и в конце разработки — на эта-



пе приёмки программных продуктов. Получалось, что некоторые информационные системы изначально проектировались и строились неправильно, без учёта требований информационной безопасности. Это приводило к проблемам на этапе сдачи АС в эксплуатацию. Некоторые доработки АС приходилось делать в виде накладок на готовый программный продукт, вносить изменения в практически готовые к запуску процессы. Продукт становился очень дорогим, а его внедрение задерживалось. Стало понятно, что работа службы информационной безопасности в существующем виде не попадает в новый ритм и тормозит развитие бизнеса. Бизнес- и ИТ-подразделения Банка начали высказывать недовольство взаимодействием со службой ИБ.

Кроме проблемы роста Сбербанк столкнулся с глобальными вызовами: распространением «облачных» технологий и мобильных приложений и, как следствие, ростом новых атак (Zero Day). Мы стали свидетелями того, каких невиданных мощностей достигли DDoS-атаки. На наших глазах начал формироваться и быстро набрал силу рынок АРТ (целевых атак). И мы, то есть банковский сектор, стали его основной

В СБЕРБАНКЕ ДЛЯ ВЫСТРАИВАНИЯ ДИАЛОГА МЕЖДУ БИЗНЕСОМ, ИТ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ СОЗДАЛИ ЦЕНТР ВЗАИМОДЕЙСТВИЯ СЛУЖБЫ ИБ С БИЗНЕС- И ФУНКЦИОНАЛЬНЫМИ БЛОКАМИ

мишенью. Рост новых угроз потребовал переключения части ресурсов ИБ-подразделений с решения задач бизнеса на противодействие кибермошенничеству.

КАК ПОСТРОИТЬ ПАРТНЕРСКИЕ ОТНОШЕНИЯ С БИЗНЕСОМ, ФУНКЦИОНАЛЬНЫМИ БЛОКАМИ И ИТ

В новых условиях требовалась трансформация информационной безопасности. Она должна была органично вписаться в концепцию развития Сбербанка, эффективно бороться с киберугрозами и стать полезной частью общего меха-

низма работы компании. Для оптимизации этих процессов нужно было наладить эффективное взаимодействие ИБ, ИТ и бизнеса.

Начались поиски ответа на вопрос, как решить проблему выстраивания коммуникаций с бизнесом и ИТ. Специалисты по информационной безопасности изучили лучшие практики Nationwide Building Society, Carphone Warehouse, Barclays Wealth, ВР и других крупнейших мировых финансовых, телекоммуникационных и нефтегазовых компаний. У нас был и собственный удачный опыт: за несколько лет до этого в Департаменте ИТ был создан институт СТО (технических специалистов), который стал успешно решать вопросы, возникающие при разработке, внедрении и эксплуатации новых информационных технологий. В итоге было принято решение создать центр взаимодействия с бизнес-блоками по информационной безопасности в рамках службы ИБ.

ЦЕНТР ВЗАИМОДЕЙСТВИЯ С БИЗНЕС-БЛОКАМИ

В 2015 году центр начал работу. В него вошли девять бизнес-партнёров по информационной безопасности (на англ. Business Information Security Officer — BISO). На эту должность Банк пригласил специалистов, которые ранее руководили департаментами ИБ в крупных банках, понимали и могли подстраиваться под задачи бизнеса, умели общаться и эффективно решать вопросы с бизнес-подразделениями.

С одной стороны, бизнес-партнёры должны погрузиться в проблемы бизнеса, реализуемые проекты, задачи, стоящие перед бизнес-подразделениями. Нам нужно находить наиболее эффективные способы предоставления клиентам безопасных сервисов и услуг, быстро и понятно информировать руководителей бизнес-подразделений об актуальных рисках ИБ, лучших практиках защиты, требованиях регуляторов и их влиянии на развитие бизнеса. Мы обяза-

ны использовать понятные специалистам бизнес-подразделений терминологию и аргументацию, владеть основными понятиями бизнеса, знать тонкости бизнес-процессов, понимать риски и возможные ограничения. Фактически нам необходимо чувствовать грань, когда безопасность начинает мешать, а не приносить пользу, превращается из помощника и защитника в тормоз для развития бизнеса.

С другой стороны, BISO — это высококвалифицированные ИБ-специалисты с обширным опытом работы в этой области. Совместно с подразделениями ИБ мы находим решения по информационной безопасности, которые учитывают интересы бизнеса. Иными словами, мы помогаем повысить защищённость бизнеса, не препятствуя его развитию.

НЕ ПРОСТО ПАРТНЕРЫ

При этом бизнес-партнёры по информационной безопасности играют несколько ролей одновременно. Во-первых, мы — стратегические партнёры. В этом случае BISO координирует ИБ-проекты с бизнес-стратегией. Во-вторых, мы — проводники изменений. Помогаем скорректировать бизнес-процессы, исходя из требований по информационной безопасности, и требования по информационной безопасности, исходя из потребностей развития бизнеса. В-третьих, BISO транслирует и разъясняет цели, которые преследует бизнес, своим коллегам в службе ИБ, и, наоборот, политики ИБ — сотрудникам бизнес-подразделений, выступая, таким образом, экспертом и операционным партнёром. И наконец, бизнес-партнёр по информационной безопасности — это своеобразная «скорая помощь». Мы помогаем расставить приоритеты и ускорить решения задач, которые ставят бизнес-подразделения перед службой ИБ, улаживаем конфликты, предлагаем решения, выгодные для всех участников процесса.

Каждый бизнес-партнёр курирует один или несколько основных бизнес-блоков Сбербанка, участвует в коллективном обсуждении бизнес-проектов и погружён во все проблемы своего блока. Сейчас в Сбербанке функционирует несколько бизнес-блоков: Розничный и Корпоративный блоки, Международный блок, Sberbank CIB (корпоративно-инвестиционный бизнес, который был создан в рамках интеграции Сбербанка России и инвестиционной компании «Тройка Диалог»). Также в этот список входит Блок управления рисками, блок «Финансы», объединяющий финансовую, налоговую и бухгалтерскую службы, блок «Управление благосостоянием», отвечающий за страховые, пенсионные программы и управление активами.

**СОВМЕСТНО С ПОДРАЗДЕЛЕНИЯМИ
ИБ МЫ НАХОДИМ РЕШЕНИЯ
ПО ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ, КОТОРЫЕ
УЧИТЫВАЮТ ИНТЕРЕСЫ
БИЗНЕСА. ИНЫМИ СЛОВАМИ,
МЫ ПОМОГАЕМ ПОВЫСИТЬ
ЗАЩИЩЁННОСТЬ БИЗНЕСА, НЕ
ПРЕПЯТСТВУЯ ЕГО РАЗВИТИЮ**

В структуре Банка есть поддерживающие блоки: на стыке бизнеса и ИТ находятся блок «Т» (Блок технологий) и блок «С», куда выделены все сервисы и обеспечивающие функции. Погружение в работу каждого бизнес-блока помогает BISO проактивно выявлять проблемные точки и заранее находить лучшие решения.

В ПРОШЛОМ ГОДУ

В 2016 году мы выстроили порядок участия службы ИБ в ИТ-проектах, а также её взаимодействие с офисами СТО по разработке, внедрению и развитию АС. Совместно с офисами СТО и отделом ИБ в ИТ-проектах Банка мы решали следующую задачу: добиться, чтобы ИБ-экспертиза в проектах была отлажена, процессы настроены, а бизнес-подразделения и разработчики получали быструю обратную связь.

Из-за дефицита ресурсов этот процесс проходил в два этапа. Сначала мы сгруппировали все поступающие на согласование документы по типам и направлениям бизнеса. У нас получился реестр запросов. Все документы встали в очередь на рассмотрение. При этом мы указали ориентировочный срок рассмотрения каждого документа и сотрудника, который с ним работает. Затем разместили этот реестр на внутрибанковском ресурсе, чтобы им пользовались сотрудники офисов СТО и бизнес-подразделений.

Таким образом, сроки рассмотрения проектных инициатив СТО и бизнеса стали прозрачными. Появилась возможность выделить необходимость срочного рассмотрения требуемого документа, а также собрать статистику, чтобы понять, сколько точно времени уходит на рассмотрение того или иного документа.

На втором этапе, основываясь на анализе полученных статистических данных по срокам рассмотрения документов, мы составили соглашение об уровне услуг (SLA) и активно работаем над его внедрением.

РАЗДЕЛЯЙ И ДЕЙСТВУЙ!

Опыт построения регламента участия специалистов по ИБ в ИТ-проектах подсказал нам разделить все проекты, которые ведут BISO, на несколько категорий, в зависимости от уровня интеграции с другими АС, критичности решаемых задач, влияния на риски банка. В итоге мы ранжировали все проекты по уровню сложности и степени участия специалистов по информационной безопасности. Получилось пять категорий. К проектам, которые входят в «лёгкие» категории, относятся, например, различные доработки отчётности, изменение пользо-

СЕЙЧАС МЫ ВНЕДРЯЕМ ЭТОТ МЕТОД РАБОТЫ ВО ВСЕХ БИЗНЕС-БЛОКАХ И ПЛАНИРУЕМ СОКРАТИТЬ ВРЕМЯ РАССМОТРЕНИЯ ПРОЕКТНЫХ ДОКУМЕНТОВ ИБ-СПЕЦИАЛИСТАМИ НА 30%

вательского интерфейса функционала внутри обеспечивающих АС и т.п., мы предъявляем формальные требования по информационной безопасности.

Пока работы по этой процедуре велись только над проектами всего двух бизнес-блоков. Как результат, экономия времени сотрудников ИБ-подразделений — 15%. Сейчас мы внедряем этот метод работы во всех бизнес-блоках и планируем сократить время рассмотрения проектных документов ИБ-специалистами на 30%.

ПРОВОДНИКИ КУЛЬТУРЫ

Центр взаимодействия службы ИБ с бизнес- и функциональными блоками — молодая структура. Пока мы нарабатываем опыт, которым планируем делиться с дочерними организациями Сбербанка и другими участниками рынка.

Трансляция лучших практик взаимодействия информационной безопасности с бизнес-подразделениями входит ещё в одну из важнейших задач BISO — внедрение культуры информационной безопасности. Она включает в себя подготовку высококвалифицированных кадров, распространение правил информационной безопасности среди сотрудников и клиентов Сбербанка, обмен опытом с другими организациями и многое другое. Мы стремимся к тому, чтобы Сбербанк накопил такие компетенции, которые помогли бы экономике в целом развиваться и нормально функционировать в условиях постоянного роста киберугроз.

* * *

За год работы мы выстроили работу центра. Результаты опросов бизнес-блоков и офисов СТО показывают, что благодаря нашим усилиям процессы стали более прозрачными и понятными, исчезли разногласия. Сотрудники знают, куда им обращаться за помощью, если возникает недопонимание между бизнесом и ИБ. Мы стали прослойкой, амортизатором, без которого невозможна реализация масштабных проектов по созданию работающих удобных и безопасных продуктов и услуг в такой крупной организации, как Сбербанк.

ОБРАТНАЯ СТОРОНА ПРИВИЛЕГИЙ

ПРОБЛЕМЫ КОНТРОЛЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ В КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ И ПУТИ ИХ РЕШЕНИЯ



Виктор СЕРДЮК
генеральный директор
АО «ДиалогНаука»



Михаил РОМАНОВ
директор по развитию
бизнеса ООО «Новые
технологии безопасности»

На сегодняшний день информационные системы кредитно-финансовых учреждений стали достаточно сложными и многокомпонентными. Создание и вывод на рынок различных банковских продуктов, как правило, требуют разработки новых информационных систем. Эти системы виртуализируются, консолидируются в специальных вычислительных центрах (ЦОДах), а определенные системы мигрируют в «Облака». И, если раньше было достаточно иметь одного-двух администраторов для управления банковскими приложениями, которые успешно обслуживали все информационные системы организации, то сейчас это невозможно ввиду сложности и многообразия современных ИТ-систем.

Сегодня на первый план выходят риски, связанные с неконтролируемым административным доступом к информационным системам и ИТ-инфраструктуре компаний. По данным ведущих аналитиков, более 70% нарушений ИБ происходят именно по вине привилегированных пользователей. Хакеры или злоумышленники также сначала ищут возможность повысить свои привилегии в системах, а затем, имея хороший контроль над целевой системой, делают несанкционированные действия по краже, изменению, удалению платежной и другой информации в финансовой организации. Обычные пользователи, как правило, контролируются достаточно серьезно — применяются средства аутентификации, механизмы разделения полномочий, системы регистрации событий безопасности и другие решения. Однако вопросы контроля того, что делают так называемые привилегированные пользователи, до сих пор остаются в стороне во многих организациях. А по сути эти пользователи по умолчанию имеют очень высокий уровень доступа в систему и к различным конфиденциальным данным.

Кроме того, для обеспечения работоспособности своих систем большинство кредитно-финансовых организаций предоставляют доступ к своим корпоративным ресурсам внешним специалистам в рамках контрактов по аутсорсингу или удаленной работе. К тому же количество внутренних администраторов в ряде банков может достигать до нескольких десятков. Кроме того, ряд задач ИТ-подразделений компании, например, задачи по настройке специализированного оборудования, часто осуществляются силами вендора. Данный подход экономически оправдан, однако он несет дополнительные риски информационной безопасности. Так, в частности, бывает невозможно определить, кто и что делал в системе, так как, например, учетная запись Суперпользователя (root, Administrator и др.) в системах часто одна, а доступ с её правами необходимо обеспечить и вендору, и администратору, и консультанту.

Рассмотрим простой пример — после новых настроек в ПО или применения очередного обновления «боевая» информационная система банка перестала работать. В данном случае для оперативного восстановления работоспособности системы необходимо понять, какие действия администраторов привели к сбою и кто именно допустил ошибку. Хорошо известно, что время простоя платежных и других систем банка является в прямом смысле «золотым». Журналы аудита, как правило, лишь в редких случаях помогают решить указанную проблему, так как протоколирование абсолютно всех действий в системе обычно не заложено в ПО. Даже если такие уровни журналирования и предусмотрены в ПО, то они не используются, так как их применение приведет к замедлению работы системы. Именно поэтому сейчас стали популярны системы контроля привилегированных пользователей (PIM, Privileged Identity Management). В настоящее время на

российском рынке представлено большое количество систем данного класса. Рассмотрим задачи, которые можно решить с помощью таких систем, на примере отечественного решения SafeInspect:

1. Необходимо обеспечить строгую аутентификацию привилегированных пользователей. Здесь существует масса проблем, вызванная тем, что администраторы часто используют специализированные протоколы, которые имеют собственные системы аутентификации. В качестве примера можно привести использование протокола SSH, который предполагает использование ключей SSH для доступа (имя — пароль мы не будем рассматривать). А это совершенно отдельная система, ключи не имеют ничего общего с сертификатами x.509, которые часто используются для аутентификации обычных пользователей и клиентов.

2. Необходимо определить и применить политику, которая обеспечивает доступ администраторов в строго определенное время (особенно важно для доступа внешних администраторов).

3. Крайне необходимо обеспечить правильное разделение полномочий по доступу к информационным ресурсам. Решение данной задачи осложняется тем, что администраторы имеют крайне «глубокий» доступ в систему и высокие полномочия. Как правило, во многих организациях администраторы имеют доступ в рамках своей системы ко всей ИТ-инфраструктуре организации и крайне болезненно относятся к какому-либо ограничению.

4. При работе с учетными записями типа Суперпользователя (root, Administrator и т.п.) важно обеспечить точный контроль над тем, кто именно и какие действия производил под этим аккаунтом, а это часто невозможно сделать штатными средствами.

5. Важно контролировать как пароли/ключи доступа, так и время доступа к разным системам и своевременно их менять или блокировать. В идеале стоит менять пароли или ключи сразу после завершения сеанса доступа.

6. Поскольку администратор может вводом неправильной команды случайно или преднамеренно нарушить работоспособность системы, крайне важно иметь возможность защиты от таких ошибок. Например, эту проблему можно решить путем запрета ввода определенных команд или системой быстрого оповещения, которая будет показывать, что определенные команды вводились в короткий промежуток несколько раз и имеется риск того, что в данном случае производились несанкционированные действия.

7. Кроме того, часто возникает необходимость проанализировать, что делалось в системе месяц назад с как можно наибольшей детализацией (как в случае исправления ошибок администрирования, так и в случае поиска несанкционированных действий). И тут такие системы являются незаменимыми.

8. Современные протоколы администрирования, даже самые базовые и популярные, сложны по своей природе, имеют т.н. субканалы, по которым передаются данные, и они зашифрованы. Контроль таких субканалов с точки зрения возможной утечки данных также является крайне важной задачей. В данном случае, например, решение SafeInspect позволяет полностью расшифровать данные и передать их в систему DLP или другую систему безопасности для последующего анализа.

9. Современные стандарты по безопасности, такие, как PCI DSS, СТО БР ИББС, в ряде случаев требуют наличия средств контроля привилегированных пользователей в финансовых организациях.

С учетом вышесказанного можно отметить, что внедрение системы контроля привилегированных пользователей позволит организации:

- ◆ выполнить соответствующие требования стандартов — СТО БР ИББС, PCI DSS, ISO 27001 и др.;
- ◆ снизить риск несанкционированного доступа привилегированных пользователей и утечки конфиденциальной информации;
- ◆ существенно снизить риск нарушения работоспособности и безопасности ИТ-инфраструктуры;
- ◆ создать архив записей сессий привилегированных пользователей для последующего проведения служебных расследований.

* * *

В настоящей статье были рассмотрены только основные возможности по применению систем контроля привилегированных пользователей. Как мы видим, затрагивается целый пласт проблем ИБ, которые в течение долгих лет не решались в полном объеме. Однако в современных условиях эти угрозы уже нельзя игнорировать, поскольку от безопасности в этой сфере может зависеть работоспособность ключевых бизнес-процессов финансовой организации. Использование решения класса SafeInspect позволит существенно повысить уровень безопасности кредитно-финансовой организации за счет снижения рисков, связанных с привилегированными пользователями.

КАК МЫ КОНТРОЛИРОВАЛИ РАБОТУ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ



Дмитрий МИХЕЕВ
ведущий эксперт
ООО «АйТи Бастион»

Современные условия создают серьезные вызовы для любого бизнеса, в том числе и для банковского. Даже если рассматривать только вопросы, связанные с ИТ-инфраструктурой и процессами, можно заметить изменения, которые раньше не были характерны для финансовых организаций.

Первое и основное, пожалуй, из таких наблюдений — обозначилось серьезное внимание к развитию ИТ-окружения бизнеса, крайне интенсивное внедрение сложных средств управления и автоматизации.

Второе — намного более активное, чем раньше, использование разных форм аутсорсинга для обеспечения эксплуатации инфраструктуры и приложений.

Причины развития в этих направлениях могут быть разными, но интересна именно складывающаяся ситуация. Она характеризуется следующим: усложнением информационных систем и ответственностей за них, эксплуатацией комплексных систем с высоким уровнем новизны для владельца, привлечением для обслуживания этих сложных систем (а мы говорим о системах класса CRM, BI) внешних специалистов, в том числе, не обязательно из России, неуклонное стремление к жестким условиям SLA.

Добавим в эту картину повышение требований регулирующих органов, требования соблюдать положения по защите ПД, PCI и других ценных хранимых данных, необходимость оптимизации затрат на персонал... и ситуацию можно смело называть «непростой».

Банковские организации укрупняются, на этом фоне процесс обеспечения необходимых контролей со стороны ответственных за ИБ становится постоянным, и появляется четкий запрос на оперативность изменений, что для банков и ИБ в банках до последнего времени тоже было не слишком распространено. Теперь нужно много и быстро делать за очень короткие промежутки времени, а не делать — нель-

зя. В таком контексте никто не хочет выступать откровенным «тормозом» изменений, даже ответственные за ИБ — порядок должен устанавливаться, поддерживаться, колеса должны крутиться.

Вполне естественно, что в такой непростой ситуации у разных ее участников возникает желание контролировать происходящее с инфраструктурой и другими компонентами ИТ-систем. Контроль может быть разным: от фиксации изменений в рамках необходимых процессов до обеспечения большей granularity при управлении доступом. В последние полтора года по результатам внешних аудитов эта тенденция получает ощутимую поддержку. Аудиторы обращают пристальное внимание на работу привилегированных пользователей, как внутренних, так и внешних.

Конечно, нелегко рассказывать про «настоящую жизнь» — проекты в области ИБ достаточно интимная сфера, но тем не менее.

Интересным случаем можно считать, например, такой. В рамках крупной банковской организации ведется внедрение CRM-системы. Все как полагается: распределенные ЦОД в широкой российской географии, развертывание инфраструктуры баз данных и серверов приложений, разработка самих приложений и АРМ. Необходимые мероприятия занимают долгое — более 3 лет — время. Система ответственная и напрямую регулирует рабочие процессы большого числа людей, завязана на работу с финансами и отчасти с персональными данными. Компоненты системы эксплуатируются разными подразделениями и несколько внешних компаний регулярно согласовывают доступ к этим компонентам для своих сотрудников — разработчиков, инженеров и экспертов по прикладному ПО. Конечно, в таком крупном проекте случаются и накладки — как технические, так и организационные. Чем больше система «входит в работу», тем менее терпимым становится руководство к проблемам с ней, тем больше

возникает сложностей с обеспечением должных условий функционирования и безопасности. К счастью, удалось избежать серьезного «раскручивания» конфликтов в проектной команде между интеграторами и сотрудниками банка, но для этого пришлось пойти друг другу навстречу.

Наша компания была выбрана как производитель системы по контролю действий привилегированных пользователей. Что оказалось полезным по результатам нашего участия?

Во-первых, мы были восхищены желанием сотрудников работать на результат. Требования, которые предъявлялись к системе, вполне отражали это желание. По опыту внедрений, как крупных, так и локальных, подобные желания можно назвать типовыми, наверное.

Инициаторами внедрения выступили сотрудники ИБ, так как именно они в сложившейся ситуации были ответственными за инциденты безопасности, и их основная задача была сформулирована как упорядочивание сложившихся не совсем корректных практик доступа к ключевым элементам инфраструктуры, в том числе — в режиме удаленного доступа. С их стороны требованиями к системе назывались: оперативность развертывания, возможность усиления контроля парольного доступа с перспективой перехода на двухфакторную авторизацию, документирование необходимых доступов для разных классов (ролей) сотрудников и реализация соответствующих ограничений. Возможность расследования происшествий также выступала как одна из основных — настолько, насколько подробная фиксация произошедшего инцидента в принципе возможна.

Со стороны службы ИТ вполне разумно было предъявлено требование гибкости внедрения системы и ее оперативной надежности, так как в сложившихся условиях переживать лишние ситуации отказов и запланированных даун-таймов им было крайне «не с руки». Предпочтение отдавалось сценарию плавного внедрения и возможности «откатиться назад» в любой момент, а также возможности не трогать никакой продуктивный поток данных. В качестве дополнительных пожеланий — возможность использовать в работе привычные инструменты. Это оказалось просто необходимо для внешних экспертов, которые применяют специализированное ПО для манипуляций с данными приложений. Такое ПО было развернуто в рамках сети и к нему предоставили доступ под запись действий.

Нельзя сказать, что внедрение системы ИБ в столь масштабном окружении — это легкая задача. Потребовались совместные уси-

лия и ИТ-, и ИБ-специалистов, чтобы результат удовлетворил их пожеланиям. Что приятно, в результате заметно изменилось отношение к службе ИБ, которая из «цербера» перешла в статус арбитра. Именно за счет возможности четко и подробно фиксировать происходящие работы на элементах инфраструктуры ИТ-специалисты банка и внешние сотрудники смогли координировать совместные работы и успешно разрешили несколько неприятных конфликтов с расчетом исключить их повторение в будущем.

Что можно отметить как характерные особенности в данном случае? ИТ-специалисты готовы работать в чуть более формализованном окружении, которое в ряде случаев скроет от них подробности инфраструктуры, если взамен получают простой и понятный набор правил работы, который, кроме всего прочего, прикроет им тылы, защитит собственных специалистов, если не от ошибок, то от долгого разбирательства. ИБ-специалисты хотят получать необходимые им инструменты для обеспечения достаточно жестких требований безопасности, которые недостаточны или отсутствуют в стандартных средствах. Это позволяет посвящать им больше времени решению сложных задач, переложив часть текущей на систему контроля. Возможность объединить систему контроля администраторов в рамках СУИБ с другими средствами безопасности также вызывает неподдельный интерес и готовность работать на результат. Не последним плюсом также является наличие сертификата соответствия РД НДВ, так как это отчасти снимает вопросы, связанные с соблюдением требований регуляторов.

Специалисты внешних компаний — инженеры, разработчики, аудиторы — в данной картине остаются наиболее ограниченными в своих возможностях. Но конфликтов, как правило, не возникает. В основном все согласны, что в банках так и должно быть: если нужно больше возможностей, то необходимо соблюдать процедуру принятия решений. Это не означает, что у них отбирают доступ — напротив, в некоторых случаях только работа через систему контроля действий позволила предоставлять доступ в принципе.

* * *

В заключение хочется отметить, что развернутая система контроля привилегированных пользователей была тепло принята руководством. Обеспечение бизнес-SLA стало возможным в значительной степени благодаря именно ее наличию.

ОБЛАЧНАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ

ИЛИ КТО РАЗРАБОТАЕТ УНИВЕРСАЛЬНЫЙ
МЕТОД ИДЕНТИФИКАЦИИ?



Александр БАРАНОВ
заместитель Генерального директора
АО ГНИВЦ, заведующий кафедрой
информационной безопасности НИУ ВШЭ

Что такое облачная электронная подпись в нынешнем понимании? С одной стороны, в законодательстве такого определения нет, с другой, облачная подпись довольно активно используется. Как правило, так называется механизм подтверждения подлинности, целостности авторства и неотказуемости от этого авторства. Этот механизм сосредоточен в квалифицированных руках, а пользователь квалифицирован минимально, но тем не менее периодически прибегает к услугам этого сервиса.

ЧТО ТАКОЕ ОЭП

В состав понятия облачная подпись обязательно входит электронная подпись. Какая? Существует два вида электронной подписи и два подвида. Первый вид — это простая электронная подпись, второй — усиленная. В усиленной подписи различаются квалифицированная и неквалифицированная.

Облачная подпись в нынешнем понимании относится к категории усиленная неквалифицированная подпись. Большинство задач, которые она выполняет, соответствует понятию, законодательно закреплённому как усиленная подпись. Но в то же время эта подпись не сертифицирована ФСБ как регулятор, отвечающим за безопасность подписей, основанных на криптографических методах.

По сути, усиленная подпись сегодня, в том числе и в облачном исполнении, — это фактически реализация квалифицированной подписи с некоторыми отклонениями от требований регулятора.

Усиленная подпись может и не быть основанной на отечественных криптографических примитивах. Например, подпись Microsoft — усиленная, но не квалифицированная. Она реализуется с помощью удостоверяющего центра Microsoft и основана на номере той копии, которую вам выдали. Именно она сопровождает вашу работу, заменяя ваше лицо и паспортные данные. Номер копии устанавливается на вашем компьютере и связывается потом с его mac-адресом. Дальше она удостоверяет вас как нормальная усиленная подпись: проверяет целостность, подписывает, проверяется в удостоверяющем центре Microsoft, причем, автоматически.

Однако, если вы скопировали программное обеспечение без разрешения производителя операционной системы, то происходит то же самое: вы работаете с дубликатом скопированного номера и не отличаетесь от легального пользователя с тем же номером. В этом, безусловно, заключается ее недостаток.

Наша усиленная неквалифицированная подпись использует отечественный криптопровайдер или криптографический примитив, ГОСТовский. Наши граждане и многие ведомства стараются быть максимально законопослушными, поэтому применяют именно ее.

Некоторые ведомства применяют ее, нарушая некоторые условия. Например, торговые площадки, у которых есть иностранные пользователи. Действительно, в условиях границы нашу квалифицированную подпись применить трудно.

Второй крупный потребитель усиленной неквалифицированной подписи — ФНС России. В личном кабинете физлица на сайте ФНС задействована именно эта подпись наряду с квалифицированной — так регламентировано Налоговым кодексом.

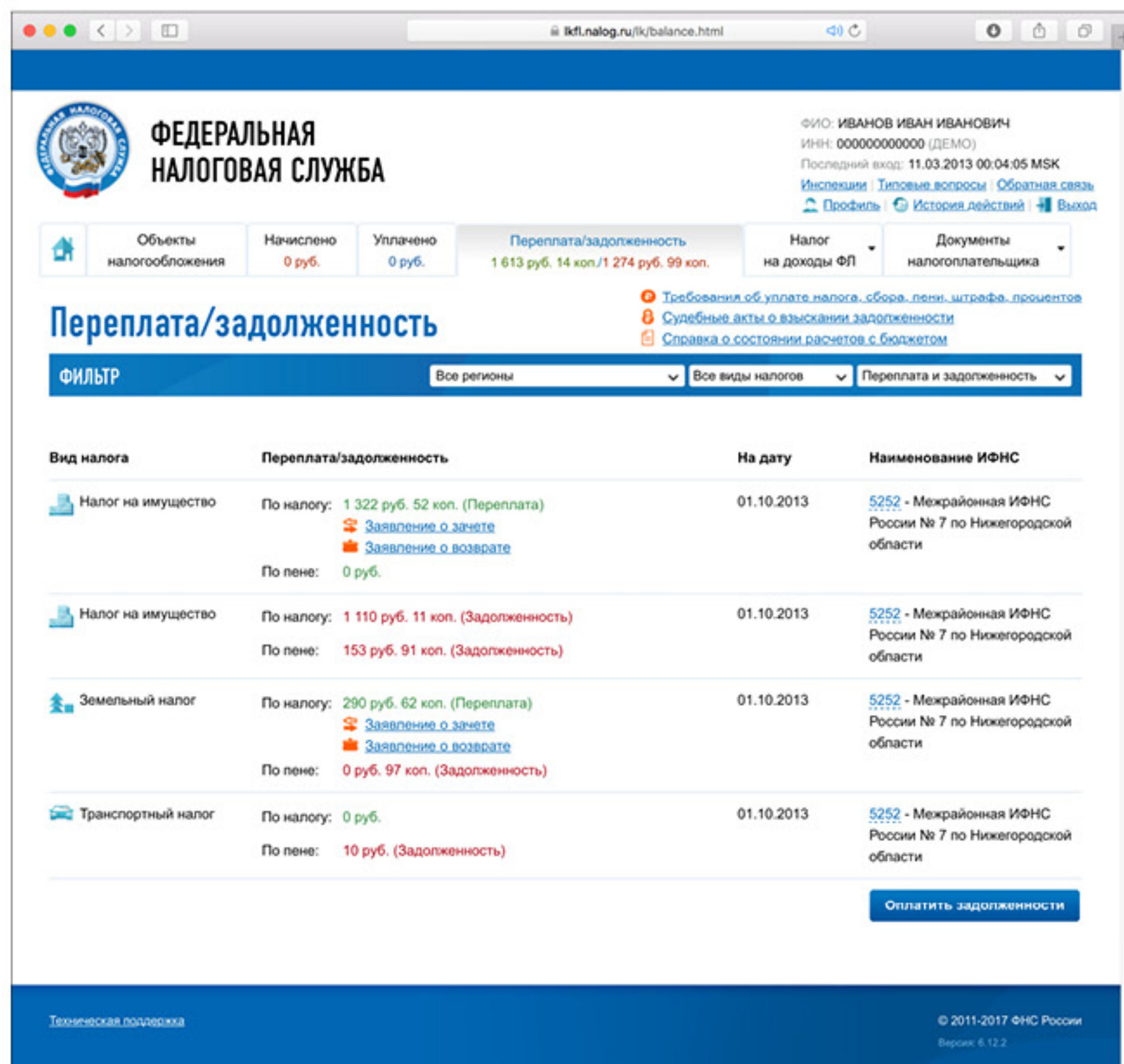
РЕАЛИЗАЦИЯ

Стоит заметить, что процедура выдачи и процедура дальнейшей технической работы с неквалифицированной подписью в налоговой службе несколько отличается от того, что требует регулятор для квалифицированной. В налоговой службе происходит закрепление за личностью номера-пароля, который держится в секрете. Когда потом человек входит в личный кабинет, ему предлагается заменить этот пароль на другой. Что он и делает, после чего к новому паролю создается персональный ключ, хранящийся в ФНС, который используется уже в алгоритме квалифицированной подписи, находящимся на сервере ФНС, где собственно и подписывается документ.

То есть в случае облачной неквалифицированной подписи документ подписывается не на рабочем месте пользователя, а в ФНС. Тем самым пользователь демонстрирует, что доверяет налоговой службе.

В личном кабинете есть и альтернативная возможность. Налогоплательщик может скачать себе бесплатно криптопровайдер от фирмы «ИнфоТеКС» (в облачном варианте используются криптопровайдеры фирмы «КРИПТО-

УСИЛЕННАЯ ПОДПИСЬ СЕГОДНЯ, В ТОМ ЧИСЛЕ И В ОБЛАЧНОМ ИСПОЛНЕНИИ, — ЭТО ФАКТИЧЕСКИ РЕАЛИЗАЦИЯ КВАЛИФИЦИРОВАННОЙ ПОДПИСИ С НЕКОТОРЫМИ ОТКЛОНЕНИЯМИ ОТ ТРЕБОВАНИЙ РЕГУЛЯТОРА



Личный кабинет физического лица на сайте Федеральной налоговой службы

ПРО»). В этом случае человеку приходится хранить ключ на токене или длинной бумажке у себя, и самому же при необходимости его вводить.

Тот, кто доверяет налоговой службе, пользуется облачным сервисом. При этом у него нет криптопровайдера на борту. Как в таком случае подписывается документ? Пользователь заполняет обращение или налоговую декларацию и направляет в ФНС. Там документ подписывается и направляется на подтверждение пользователю, если налогоплательщик отвечает: согласен, то налоговая служба может с полным правом работать с его документом.

В случае, когда криптопровайдер на борту, человек сам готовит документ, сам его подписывает (с помощью токена или вручную) и отправляет в налоговую службу, после чего документ поступает в работу. Кстати, пользователь может использовать как неквалифицированную подпись, так и квалифицированную. Сайт ФНС принимает и ту, и другую.

ДЕСЯТЬ ПРОТИВ ОДНОГО

Конечно, удобство облачной подписи очевидно, и пользователь на него тут же откликнулся. Соотношение между числом пользователей облачной подписи и подписи на борту — 10 к 1. То есть из 10 пользователей только один пользуется подписью на борту.

Объясняется это в первую очередь тем, что наши отечественные криптопровайдеры, к сожалению, плохо адаптированы к различным средам. У них отсутствует достаточная мультибраузерность и мультиплатформенность. Конечно, фирмы «КРИПТО-ПРО» и «Инфо-ТекС» стараются сделать побольше платформ, но за обновлениями не успевают. В результате большинство граждан с радостью пользуется облачной подписью, которая требует от них минимальной пользовательской квалификации.

С другой стороны, пользователь в массе своей вообще не хочет ни за что отвечать, в том числе и за безопасность. Ему это выгодно, в случае чего он всегда может оспорить проблему. Предположим, подписал он декларацию, а ее где-то изменили. Когда следом приходит реальная платежка, он, конечно, по ней не платит, а бежит в налоговую и начинает шуметь: что ж вы, ребята, с ума сошли, что ли? И там начинают разбираться и поправляют, потому что мошенников, действительно, хватает. Но такого сорта мошенничество не проходит на нашем сайте оплаты.

Потому что, когда вы получаете платежку с нашего сайта, вы получаете платежку банка — партнера ФНС. В таком банке обязательно проверят реквизиты платежки, назначение платежа и т.д., и платеж в любом случае придет в ФНС. То есть деньги к злоумышленникам не попадут. Вернуть их вряд ли получится, но, по крайней мере, их зачислят в счет будущих ваших платежей.

И это тоже движет миллионами пользователей, чтобы применять облачную подпись. Да, маленькие неприятности возможны, но деньги-то не пропадают.

ВЫНУЖДЕННАЯ МЕРА

Так ситуация выглядит со стороны пользователя, а как со стороны разработчиков ресурса? Почему мы стали использовать неквалифицированную подпись?

Все дело в массовой рассылке. Если у нас 10 млн пользователей, то представьте, какие затраты потребуются, чтобы их только выдать? Сколько денег, операторов, помещений, времени! Даже если затраты на одну подпись составят 100 руб., а пользователей у нас 10 млн, то общие затраты — минимум 1 млрд руб. в год. В каждый год! Потому что по требованию регулятора ключ нужно менять ежегодно или создавать итеративную систему на борту с проблемами криптопровайдера. То есть для массового пользователя редко применяемая квалифицированная подпись слишком громоздка в применении.

Стоит отметить, что облачная подпись оказалась выгодной и для банков, и для крупного бизнеса. Например, для большой компании,

у которой тысяча филиалов по стране и в каждый нужно раздать по несколько подписей, обучить людей ими пользоваться, регулярно по закону эти подписи менять... В общем, возни и затрат много. Гораздо проще сделать один сервер, чтобы документы там подписывались и отправлялись назад.

Правда, возникает возможность отказов с мест. А я не отсылал такой документ, не подписывал... Это юридическая проблема, решается она достаточно просто — с помощью взаимных договоров или издается внутренний приказ о работе нового сервиса, и все сотрудники-пользователи сервиса подписываются, что они доверяют этой системе. Все это соответствует принципам, заложенным в ФЗ-63 — законе об электронной подписи, где для юридического подтверждения усиленной подписи требуется соглашение между вами и тем, кто с вами взаимодействует с помощью электронной подписи.

ГЛАВНАЯ ПРОБЛЕМА

Теперь вопрос. Что нужно, чтобы электронная подпись была автоматической, юридически значимой? Законодательное зацепление. И тут, оказалось, самая большая проблема — в распознавании личности хозяина подписи. Вот вы живьем приходите в удостоверяющий центр, предъявляете паспорт, и вам из рук в руки выдают ключ. Теперь считается, что ключ — это ваш идентификатор. Ключ и вы — одно и то

же. Дальше, как полагается по закону, вы бережете этот ключ и используете его как собственный палец или глаз.

А если ключ у вас украли? Тогда вы должны позвонить в удостоверяющий центр и отозвать свой сертификат, отменить действие ключа. После этого ваша подпись становится недействительной. На этом, собственно, и основано применение усиленной подписи.

Но именно тут открывается простор для мошенников. Далеко не все специалисты удостоверяющих центров проверяют на подлинность паспорта клиентов. Кроме того, существует законодательная лазейка, позволяющая получить чужую подпись по простой рукописной доверенности.

Сколько подставных фирм открыто, сколько взято липовых кредитов, продано чужих квартир, — не знает даже МВД! Тем не менее, закон по-прежнему разрешает использовать рукописную доверенность для выдачи квалифицированной подписи.

КЛЮЧ — ЭТО ВАШ ИДЕНТИФИКАТОР. КЛЮЧ И ВЫ — ОДНО И ТО ЖЕ. ВЫ БЕРЕЖЕТЕ ЭТОТ КЛЮЧ И ИСПОЛЬЗУЕТЕ ЕГО КАК СОБСТВЕННЫЙ ПАЛЕЦ ИЛИ ГЛАЗ



Представляете, мошенник получил по такой доверенности токен и открыл управляющую компанию, которая дальше открывает все новые и новые фирмы. При этом удостоверяющий центр не имеет права отозвать подпись — только по заявлению владельца или решению суда. А такая судебная процедура занимает не менее полугод. И все это время мошенник занимается своим делом: открывает фирмы, проводит электронные платежи... Это, конечно, нонсенс!

Налоговая служба просто сбилась с ног, разбираясь с такими заявлениями. Я такая-то, ко мне пришло извещение, что я владелица электронной подписи и десяти фирм. Заявляю, что я не знаю, что такое электронная подпись. Доверенностей никому не давала. Фирм не открывала...

В таком контексте, конечно, облачная подпись оказывается более надежным инструментом. Там все-таки есть организация, которая берет на себя ответственность, заключаются договоры о доверии... Но тем не менее вопрос «какая подпись лучше?» остается открытым. И там, и там есть как достоинства, так и недостатки.

ПРОБЛЕМА СОХРАНЯЕТСЯ И ДЛЯ ОЭП

Основная проблема — идентификация личности пользователя — сохраняется и для облачной подписи. Выходя на облачный сервис, человек использует логин-пароль. Этого, конечно, мало. Нужно точно знать, кто вошел под этим логином-паролем: Иванов или Сидоров?

Одни говорят: давайте использовать отпечаток пальца или всей пятерни. Можно и так. Но нельзя забывать, что этот самый отпечаток нужно переправить по почте. Говорят, а мы его зашифруем! А чем вы его зашифруете, если у вас на борту нет криптопровайвера? Вы можете, конечно, использовать SSL Microsoft, но он не сертифицирован. И как тут решить проблему «доверия-не доверия»? Это первый вопрос.

Второй. Если мошенники перехватят ваш отпечаток пальца в почте или похитят каким-то

другим способом, они начнут его использовать и наделают много плохого от вашего имени. Пойди да разбери, кто в действительности химичил. То же самое относится и к фотографии, и к радужной оболочке... — к чему угодно.

В чем дефект? В том, что наш объект неизменен. Его нельзя определить как подвижный, живой, изменяющийся. Когда вы проходите пограничный контроль, например, в гипсовой маске, пограничник это мгновенно заметит. Он строго скажет: «Ну-ка, улыбнитесь», или «Снимите очки, я посмотрю, как у вас там глаза двигаются». То есть, он отличит живое от неживого. Конечно, перенести такую способность в теорию распознавания образов достаточно сложно. Но не невозможно.

НА СТЫКЕ НАУК И ОТВЕТСТВЕННОСТЕЙ

Тут парадокс. С одной стороны, методы распознавания образов, личности, частей тела продвинулись далеко вперед. С другой стороны, этим у нас никто серьезно не занимается. Пользуются само собой разумеющимся. Потому что ни одно ведомство за это не отвечает, никому это законодательно не поручено. ФСБ отвечает за криптографию, ФСТЭК — за техническую защиту информации, милиция — за выдачу паспорта и соответственно за идентификацию личности непосредственно в паспортном столе. Все!

А кто разрабатывает методы идентификации? Оказывается, только энтузиасты. Безусловно, толковые энтузиасты многое могут, но создать полноценный серийный продукт они не могут. Для этого нужен государственный заказ, контроль и квалифицированный исполнитель.

Так в чем проблема? Дело в том, что наш ожидаемый продукт произрастает на стыке наук и методологий: электроники, математики, биологии... Представители ФСБ заявляют: а мы-то тут при чем? Мы биологии не знаем. ФСТЭК туда же: мы технари. Мы только в компьютерах понимаем. Милиционеры наоборот: мы человека знаем, мы его регулярно воспитываем. А электронику не очень... Тогда Минкомсвязи? Нет, у нас одни юристы...

Получается, насущная потребность есть, а создать продукт некому.

Тема идентификации, конечно, очень актуальна для банков, но поручить им создание конечного продукта на государственном уровне не имеет смысла. Дело в том, что банки заинтересованы в очень простом варианте. Риск в 2% для них — хороший показатель, потому что экономия, которую они получают на уда-

**С ОДНОЙ СТОРОНЫ, МЕТОДЫ
РАСПОЗНАВАНИЯ ОБРАЗОВ,
ЛИЧНОСТИ, ЧАСТЕЙ ТЕЛА
ПРОДВИНУЛИСЬ ДАЛЕКО ВПЕРЕД.
С ДРУГОЙ СТОРОНЫ, ЭТИМ У НАС
НИКТО СЕРЬЕЗНО НЕ ЗАНИМАЕТСЯ.
ПОТОМУ ЧТО НИ ОДНО ВЕДОМСТВО
ЗА ЭТО НЕ ОТВЕЧАЕТ**



ленном банкинге — десятки процентов. Самая простая идентификация их пока устраивает. А если все же кто-то получил чужие деньги, украв идентификатор... Ну, и ладно, покроем за счет прибыли.

ТРЕБУЕТСЯ ГОСУДАРСТВЕННЫЙ ПОДХОД

На самом деле, если эту задачу поручить личной фирме, серьезно занимающейся разработкой средств защиты информации, ее можно решить довольно быстро. Безусловно, это потребует денежных вложений, контроля за исполнением и серьезной объективной экспертизы результата с открытым обсуждением научной общественностью. Тем не менее, за год такую работу вполне можно выполнить.

Нужно стандартным образом организовать конкурс без изначального указания и рекомендаций по выбору победителя, в котором примет участие ряд организаций. Создать комплексную комиссию, которая разработает условия конкурса, техническое задание и будет принимать результат. Пригласить в нее юристов, криминалистов, специалистов разных направлений, представителей ФСБ, ФСТЭК, МВД, Минкомсвязи... На эту подготовку с учетом бюрократической волокиты уйдет год.

Участники конкурса предложат свои программы, будет выбрана наиболее перспективная, и победитель за год выдаст продукт на гора. Решит проблему. Года для разработки вполне достаточно, так как ничего фундаментального в сфере идентификации не осталось, все фун-

даментальные проблемы в той или иной степени там решены. Да, возможно, полученный метод окажется не стопроцентно надежным, но он наверняка будет лучше, чем то, что есть сейчас. Кажется, что два года много, но сейчас нет ничего эффективного.

Напомню, что стопроцентно надежным не является и человек, как идентификатор другого человека. Если не говорить о близнецах, похожести лица, использовании париков и грима, то любой проверяющий элементарно устает. Еще в КГБ проводили исследование и пришли к выводу, что проверяющий документы офицер через полчаса начинает ошибаться. В пропуск вклеивали вместо фото гражданина собачью морду и так спокойно проходили через проходную. Возможно, найденный в результате конкурса метод идентификации поможет решить и эту проблему.

* * *

Мне кажется, путь решения проблемы идентификации личности требует именно тако-го — государственного подхода. Заказ — конкурс — результат. Затем законодательное закрепление полученного метода, в том числе и в использовании его в облачной подписи. Думаю, с таким подходом согласятся и регулирующие органы, которые будут этот законопроект согласовывать. А пока этого нет, мы будем иметь то, что имеем — экстенсивное, малоэффективное и малопредсказуемое развитие по мере крайней необходимости.

КАК ПЕРЕЙТИ НА НОВЫЕ СТАНДАРТЫ ЭЛЕКТРОННОЙ ПОДПИСИ



Владимир ИВАНОВ
директор по развитию
компании «Актив»

С принятием новых стандартов ГОСТ 2012 использовать старые алгоритмы электронной подписи можно до 31 декабря 2018 года. Эксперты из компании «Актив» решили разобраться, кого, в первую очередь, коснется переход на новые стандарты, сколько времени займет переходный период, и что нужно сделать удостоверяющим центрам и банкам для плавной миграции.

НОВЫЕ АЛГОРИТМЫ

Введение новых стандартов на криптографические алгоритмы — это неизбежный процесс, связанный со многими факторами, в частности, с повышением производительности компьютеров и исследованиями уязвимостей имеющихся алгоритмов. Новые криптографические стандарты вводились неоднократно и в мировой практике.

В России уже имеется опыт перехода на новые алгоритмы электронной цифровой подписи, когда ГОСТ Р 34.10–94 заменялся на новый ГОСТ Р 34.10–2001. В 2012 году были приняты новые стандарты на алгоритм электронной подписи ГОСТ Р 34.10–2012 и алгоритм хэширования ГОСТ Р 34.11–2012.

Электронная подпись (ЭП) широко используется во множестве информационных систем и приложений, поэтому простое «переключение» с одного стандарта на другой попросту невозможно и необходимо длительное время как на технические работы по переходу на новые алгоритмы, так и на организационные процессы.

За переходный период должны быть внесены изменения и в программный код систем, использующих алгоритмы подписи, разработаны

и сертифицированы новые средства криптографической защиты информации (СКЗИ), запущены в эксплуатацию новые средства удостоверяющих центров.

Параметры этого переходного периода были определены в документе ФСБ России «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования». В соответствии с ним, использование старых алгоритмов допускается вплоть до 31 декабря 2018 года.

На первый взгляд, времени много, однако на начало 2017 года заметных внедрений новых стандартов нет и времени на переход осталось очень мало. Поскольку типичный срок действия квалифицированного сертификата составляет 1 год, то с 1 января 2018 года пользователи уже должны иметь все возможности для использования новых алгоритмов. То есть на переход осталось меньше года.

УЦ И БАНКИ ПОД ПРИЦЕЛОМ

Давайте попробуем разобраться и оценить объемы работ, которые должны быть завершены к концу 2017 года.

Переход на новые стандарты коснется, в первую очередь, аккредитованных удостоверяющих центров, банков, операторов систем электронного документооборота, электронных торговых площадок, но что гораздо более масштабно — миллионов их пользователей, которым надо будет заменить СКЗИ, ключи и сертификаты.

Чтобы выдавать абонентам соответствующие новым требованиям СКЗИ, поставщикам услуг и разработчикам информационных систем необходимо заранее задуматься о покупке оборудования и приведении прикладного программного обеспечения в соответствие новым стандартам.

Процесс перехода на новые стандарты можно разделить на два больших этапа: обновление средств удостоверяющего центра (УЦ) и замена ключей электронной подписи. Весь этот процесс необходимо правильно спланировать, чтобы не попасть в авральный режим замены ЭП и не подвергнуть непрерывность бизнес-процессов клиентов риску остановки.

**ПРОЦЕСС ПЕРЕХОДА НА НОВЫЕ
СТАНДАРТЫ МОЖНО РАЗДЕЛИТЬ НА
ДВА БОЛЬШИХ ЭТАПА: ОБНОВЛЕНИЕ
СРЕДСТВ УДОСТОВЕРЯЮЩЕГО
ЦЕНТРА И ЗАМЕНА КЛЮЧЕЙ
ЭЛЕКТРОННОЙ ПОДПИСИ**

Этап, связанный с переходом УЦ на новые стандарты, по оценке компании «Крипто-ПРО», ориентировочно займет 7 месяцев (Рисунок 1). Его нужно завершить до 31 декабря 2017 года, соответственно, стартовать он должен не позднее июня 2017 года. Примерно 2 месяца потребуется на закупку нового программно-аппаратного комплекса УЦ, еще 2 месяца — на его развертывание и тестирование. Оставшееся время займет взаимодействие с Минкомсвязи, регистрация и кросс-сертификация нового корневого сертификата УЦ. По завершении всех необходимых действий УЦ будет готов выпускать сертификаты, соответствующие новым стандартам.

31 декабря 2017 года получается «красным днем календаря», чтобы с начала 2018 года УЦ уже могли выпускать сертификаты в том виде, в каком они смогут быть использованы в 2019 году в соответствии с новым стандартом. По сути остается один год, а не два, как может показаться, для перехода на новые правила.

Этот график описывает, если можно так сказать, идеальный случай, когда нет конкуренции за ресурсы поставщиков программно-аппаратных комплексов УЦ, например, когда требуются услуги команды внедренцев. Учитывая, что на начало 2017 года количество аккредитованных при Минкомсвязи удостоверяющих центров приближается к 450, «идеальный» случай маловероятен.

ГЛАДКИЙ ПЕРЕХОД

Второй этап, в течении которого конечным пользователям (клиентам банков, юридическим лицам, сдающим отчетность и участвующим в электронных торгах и т.п.) должны быть заменены СКЗИ, ключи подписи, сертификаты и прикладное ПО, представляется еще более интересным. Если количество УЦ, включая аккредитованные и банковские, не превышает 1000, то количество конечных пользователей средств электронной подписи исчисляется миллионами.

Следует учитывать, что ключи и сертификаты электронной подписи не существуют сами по себе. Чтобы их использовать, нужны средства ЭП и носители ключевой информации. К средствам электронной подписи и ключевым носителям относятся, например, USB-токены.

Давайте оценим количество токенов для ДБО, подлежащих замене, в масштабе банковской системы РФ. Учитывая, что на ТОП-50 банков приходится более половины от числа всех активных юридических лиц в стране, то количество пользователей систем ДБО — около



Рисунок 1. Что предстоит сделать удостоверяющим центрам?

1,5 млн юридических лиц и ИП. Количество носителей электронной подписи, находящихся в обращении — около 3–3,2 млн ед. из расчета по 2 подписи на каждое юридическое лицо.

Для плавного перехода на новые стандарты нужно решение, которое потребует минимальных затрат и будет поддерживать новые российские криптографические стандарты. Это аппаратное средство электронной подписи Рутокен ЭЦП 2.0 с реализацией ГОСТ Р 34.10–2012 и ГОСТ Р 34.11–2012. Рутокен ЭЦП 2.0 сертифицирован ФСБ России в качестве СКЗИ с аппаратной реализацией алгоритмов ЭП, хэширования и шифрования и средства ЭП, соответствующего требованиям 63-ФЗ «Об электронной подписи».

С учетом таких впечатляющих цифр время на внедрение ЭП по новому ГОСТ не кажется таким уж большим. Поэтому часть банков заранее начала переход на новый стандарт. Уже более 200 российских банков используют Рутокен ЭЦП 2.0 для защиты платежных операций своих клиентов.

Кроме времени, не последним фактором является финансовый. Проще говоря, каждый выдаваемый сейчас пользователю ДБО токен, не соответствующий новому ГОСТ, придется заменять, а это неизбежно потребует затрат. Поэтому чем позже начать проект, тем дороже он в итоге получится. Уважаемые господа банкиры могут произвести эти несложные расчеты самостоятельно.

Таким образом, оперативный перевод в ближайшее время конечных пользователей на Рутокен ЭЦП 2.0 гарантирует банкам существенную экономию средств при замене старых СКЗИ. При проектировании новых информационных систем и при реализации долгосрочных проектов необходимо использовать СКЗИ, соответствующие новым стандартам, замена которых в ближайшем будущем не потребуется.

Для ТОП-50 банков: количество пользователей систем ДБО — 830 тыс. организаций и ИП.

БАНКОВСКАЯ БЕЗОПАСНОСТЬ В БЕЛАРУСИ

НОРМАТИВНЫЕ МЕРЫ
ТРЕБУЮТ ТЕХНИЧЕСКИХ РЕШЕНИЙ



Елена ХАРЛАМОВА
корреспондент
BIS Journal в Минске

Банковская безопасность в Республике Беларусь является одним из ведущих направлений в плане приоритетного развития концепций информационной безопасности государства. При этом, техническая составляющая безопасности на банковских объектах не менее актуальна, нежели интеллектуальная её часть. Учитывая бурное развитие телекоммуникационных технологий, обеспечение безопасности в банковском секторе является одним из ключевых вопросов, стоящих на повестке дня профильных специалистов.

Национальный банк Республики Беларусь одной из ведущих функций предполагает реализацию государственной политики в сфере охранной деятельности банков. Как гласит статья 26 Банковского Кодекса Республики Беларусь, для банков должны быть установлены обязательные требования к безопасному функционированию объектов и безопасности оказания банковских услуг. При этом, устанавливаются отдельные требования к техническим возможностям банков для проведения банковских операций. Осуществление технического нормирования, а также стандартизации в области банковской деятельности также производится согласно регламенту отечественного банковского законодательства.

— Если говорить о масштабах практической работы, то они достаточно внушительны: сотрудниками Национального банка был проведен специализированный комплекс мероприятий по проверкам банковских объектов на соответствие требованиям законодательства, — отметил заместитель начальника отдела безопасности Центрального хранилища

Национального банка Республики Беларусь Максим Мазуров. — Также были усовершенствованы нормы обеспечения безопасности банковской деятельности. Одним из актуальных направлений данного процесса является постоянный анализ законодательства: как нормативных технических документов, регламентирующих основные аспекты технической укрепленности, так и освещение вопросов оснащенности техническими средствами охраны.

Большую помощь нам оказывают сами банки — как в предоставлении информации по основным аспектам реализации требований уже действующих нормативно-правовых документов, так и в оказании информационной и технической поддержки при их обновлении и создании новых. В целом же, если говорить о вопросах модернизации технического оборудования, то специалистами Национального банка были изучены предложения и опыт некоторых банков по применению новых технологий в обеспечении технической безопасности своих объектов.

Банки оказывают не только посильную информационную поддержку, но и помощь в техническом решении профильных вопросов. Была проведена комплексная рассылка на банковскую целевую аудиторию и получены предложения от специалистов как по спорным аспектам нормативных документов, так и по их актуализации и дополнению. Одним из актуальных вопросов банковской безопасности является подключение системы охранного телевидения банка к объединенным системам видеоконтроля. В рамках действующего законодательства обновлены принципы применения на банковских объектах интегрированных систем охраны. Оборудование объектов банков подобными

системами носит рекомендательный характер. Однако интегрированные защитные комплексы уже установлены и успешно функционируют во многих банках.

— Поскольку банковские учреждения желают повысить уровень безналичных платежей, соответствующими отделами банковских структур проводились специализированные мероприятия, позволяющие значительным образом улучшить состояние безопасности банковской сферы, — рассказывает **начальник управления по расследованию преступлений против информационной безопасности и интеллектуальной собственности Главного следственного управления Следственного комитета Республики Беларусь Александр Сушко**. — Очевидно, что совершаться преступления в сфере высоких технологий будут повсеместно, и обеспечить комплексную безопасность невозможно. Однако необходимо к этому стремиться.

Помимо этого, актуальным аспектом деятельности как банковских учреждений, так и представителей структур безопасности является обеспечение решения вопросов региональной кибербезопасности. Связано это, в первую очередь, с тем, что компьютерные злоумышленники полагают, что в регионах наказания им можно избежать. Однако, как показывает практика, злоумышленники могут быть установлены и привлечены к ответственности и в далеком маленьком городке.

Следует подробнее остановиться на отдельных негативных аспектах преступлений в сфере информационной безопасности, таких, как, например, фотографирование различных частей банковской карточки. Впоследствии с применением полученных реквизитов совершались хищения, в том числе и в ряде зарубежных интернет-магазинов.

Ключевым аспектом современной безопасности является продолжительность расследования данных преступлений. По мнению специалистов, при отсутствии реальной работы в банковских учреждениях обращение к профильным законопроектам положения дел не меняет. На сегодняшний день многие банки не имеют единой точки опоры: когда появляется информация о пострадавших, с ней работают и специалисты отдела банковских карт, и начальники служб безопасности, и юристы.

Еще один аспект, на котором хотелось бы остановиться — системы видеонаблюдения. Затрачивать большие средства на приобретение новых систем видеонаблюдения весьма нерацionalmente. Однако, подобная ситуация может коснуться любого банка. Следственным Комитетом РБ ведется аналитика и учёт работы по выявле-

нию условий и причин киберпреступлений, которые совершаются в банковской сфере. Сотрудники ведомства занимались расследованием технологических преступлений и прогнозировали их всплеск не только в сфере компьютерных технологий, но и в косвенно сопряженной высокотехнологичной среде.

Наличие данных преступлений тесно взаимосвязано с деятельностью банковских учреждений. Даже когда сотрудники правоохранительных органов узнают, что преступник применял банковскую пластиковую карточку, чтобы обналичить вырученные от продажи наркотиков средства, видеонаблюдение не всегда показывает достоверную картину. Системы видеонаблюдения позволяют установить, что сам потерпевший пользовался банковской пластиковой карточкой. Следовательно, исходить необходимо из того, что работники службы безопасности должны поднимать данные вопросы перед самым банковским руководством — для оперативного внедрения систем онлайн-мониторинга.

Конструктивное взаимодействие в сфере банковской безопасности позволяет значительно уменьшить количество совершаемых преступлений, а онлайн-банкинг, интернет-банкинг и прочие виды интерактивных банковских решений будут развиваться. Совершение преступления система видеонаблюдения предотвратить не может, однако существует деятельность по профилактике правонарушений. Если в банке отсутствует система видеонаблюдения — нельзя говорить о наличии целостной системы профилактики. Предоставленные при этом в правоохранительные органы материалы не являются самоцелью — целью можно назвать то, что банковское сообщество самостоятельно начинает заботиться о вопросах корпоративной безопасности.

* * *

Информационная безопасность банков складывается из организационных, технических и правовых мер. На сегодняшний день в банковской структуре Беларуси обеспечение вопросов информационной безопасности находится на надлежащем уровне. Проблема заключается лишь в том, что не окончательно обеспечены правовые аспекты. Банковская система должна представлять собой цельный комплекс, в котором будут отсутствовать данные недочёты. Понятно, что они всегда могут быть, поскольку уровень киберпреступности на сегодняшний день достаточно высок — поэтому необходимо вовремя приняты меры, способные эти преступления предотвратить или помочь в их раскрытии.



НАЦИОНАЛЬНЫЙ БАНК
РЕСПУБЛИКИ БЕЛАРУСЬ

Национальный банк
Республики Беларусь
одной из ведущих
функций предполагает
реализацию
государственной
политики в сфере
охранной деятельности
банков



Андрей ФРОЛОВ
вице-президент,
директор по IT
ПАО «Почта Банк»



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



ПРАКТИЧЕСКИЙ ОПЫТ ПОСТРОЕНИЯ VPN СЕТЕЙ В БАНКАХ

Одной из особенностей нашей страны является обширная территория, которая подталкивает бизнес к созданию распределенной корпоративной сети. Банковская сфера — не исключение: региональные филиалы, дополнительные офисы, банкоматы — обязательные атрибуты большинства банков. При этом необходимо защищать их взаимодействие как между собой, так и с головным офисом

и ЦОД. Традиционно, системы защиты каналов связи строятся на основе мирового стандарта IPsec VPN с шифрованием по западным алгоритмам. Но стоит учитывать еще одну особенность нашей страны — локальное законодательство. В соответствии с отраслевым стандартом СТО БР ИББС персональные данные необходимо защищать с помощью VPN-продуктов, сертифицированных ФСБ России.

В компанию «С-Терра СиЭсПи» регулярно поступают запросы от банковских организаций на приобретение продуктов для модернизации системы защиты сети. Вместе с Андреем Фроловым, вице-президентом, директором по IT ПАО «Почта Банк», который является нашим заказчиком, мы рассмотрим перечень требований, предъявляемых при выборе VPN-продуктов, и продемонстрируем спектр предлагаемых решений С-Терра, удовлетворяющих этим требованиям.

ТРЕБОВАНИЕ 1. Неизменная логика работы, т.е. модернизация с минимальным изменением структуры сети.

Если новое оборудование работает по тем же протоколам, что и старое, то изменения действительно будут минимальны. Продукты С-Терра реализованы на базе протокола IPsec в соответствии с RFC, поэтому заказчик имеет возможность плавной миграции.

Андрей Фролов: Изначально мы использовали шифрование на западных алгоритмах с резервированием оборудования и каналов связи. На первом этапе мы заменили оборудование на резервном канале — установили туда С-Терра. Временно сделали этот канал основным, провели пилотное тестирование. Для нас крайне важной была возможность в любой момент без проблем вернуться к старой схеме. Вторым этапом было заменено оборудование на основном канале.

ТРЕБОВАНИЕ 2. Соответствие законодательству и отраслевым стандартам.

Защита персональных данных регламентируется Федеральным законом № 152 «О персональных данных», Постановлением Правительства № 1119, приказом ФСБ № 378, приказом ФСТЭК № 21 и, конечно же, СТО БР ИББС.

Поэтому средства защиты информации (СЗИ) должны быть сертифицированы регуляторами — ФСБ России и ФСТЭК России, при этом уровни сертификации определяются на этапе проектирования. Продукты С-Терра поддерживают шифрование по отечественным ГОСТ-алгоритмам и сертифицированы ФСБ России как СКЗИ по классам КС1, КС2 (требование для ПДн в СТО БР), КС3, и как МЭ4 класса, а также во ФСТЭК России. Это позволяет реализовать систему защиты в соответствии с требованиями российского законодательства.

Андрей Фролов: При закупке сертифицированного оборудования мы обращали внимание не только на сам факт наличия сертификатов на момент закупки, а на наличие у поставщика дорожной карты по разработке и сертификации на 5 лет. Ведь сроки действия сертификатов составляют всего три года с возможностью продления до пяти. И этот срок редко отсчитывается от начала проекта, т.е. скорее всего в рамках обслуживания потребуются своевременное обновление до актуальной сертифицированной версии. Для продуктов С-Терра такая возможность предоставляется при использовании вендорской технической поддержки.

Также нам важно знать, в каком направлении движется компания-производитель, сможем ли мы использовать их решения в других проектах. Во время общения с коллегами из компании «С-Терра СиЭсПи» мы поняли, что к нашему мнению прислушиваются, для будущих проектов продукты могут быть доработаны с учетом наших пожеланий. Для нас это важно.

ТРЕБОВАНИЕ 3. Оптимальное соотношение цена / качество / функциональные характеристики.

Для типовых объектов требуются недорогие комплекты оборудования с базовым набором функций: межсетевой экран, криптозащита, доступ в интернет и т.п. Для продуктов С-Терра это могут быть как совместные решения с крупнейшими компаниями — производителями сетевого оборудования — Cisco и Huawei, так и полностью отечественный продукт — универсальный сервисный криптомаршрутизатор Eltex ESR-ST. Это позволяет выбрать оптимальный вариант для любой задачи.

Андрей Фролов: В продуктовой линейке С-Терра нас привлекла гибкость, компания готова сотрудничать с различными производителями сетевого оборудования для выработки оптимальных для нас решений. Таким образом, удалось сформировать несколько вариантов комплектов для типовых узлов.

ТРЕБОВАНИЕ 4. Удобное обслуживание.

Оборудование необходимо администрировать, следовательно, дополнительная нагрузка будет возложена на отделы ИБ и/или ИТ. Если средства защиты имеют собственный интерфейс и логику управления, то необходимо обучение сотрудников, которое требует временных и финансовых затрат. Продукты С-Терра, наряду с собственной системой управления, могут конфигурироваться через консоль с подмножеством команд Cisco IOS, знакомых большинству сетевых инженеров.

Андрей Фролов: Нам хотелось найти продукт с интуитивно понятным интерфейсом управления, уже известным администраторам, а также с возможностью интеграции в наши системы мониторинга. В продуктах С-Терра управление реализовано в виде «cisco-like» консоли, а для мониторинга можно использовать широкий перечень параметров SNMP.

Выводы

Банк — прагматичный заказчик, который подходит к проектированию системы защиты фундаментально, рассматривая как высокоуровневые задачи, так и разбираясь в деталях работы компонентов решения. У банков есть то, что нужно злоумышленникам — деньги. Ставки слишком высоки, чтобы экономить на защите. Специфика требований отрасли — интеграция с сетевой инфраструктурой, средствами управления и мониторинга, выгодное соотношение цены и качества, а также соответствие требованиям регуляторов.

Андрей Фролов: Проектирование и внедрение любых систем, и защита каналов связи не исключение, в крупной организации — процесс довольно долгий, ведь нам нужно учесть множество нюансов. Это является дополнительной проверкой производителя — он должен все время держать руку на пульсе, своевременно реализовывать новые требования, соблюдая соотношение цена-качество. С компанией «С-Терра СиЭсПи» мы работаем уже довольно давно и хорошо знаем их надежные, современные продукты, соответствующие требованиям российского законодательства.

ТОП-10 СРЕДСТВ ИБ,

НА КОТОРЫЕ СТОИТ ОБРАТИТЬ
ВНИМАНИЕ В 2017 ГОДУ



Александр ХЕГАЙ
директор по развитию
бизнеса АО «Cross
Technologies»,
MBA, CISM, CISSP

Из года в год, следуя трендам, на волне актуальности поднимаются те или иные средства и методы информационной безопасности. Как правило, они незаслуженно отодвигают на второй план не менее, а зачастую и более эффективные средства. Изучив отчёты крупнейших международных аналитических агентств, пытающихся предсказать, кто и что окажется на этой самой волне популярности в новом году, мы постарались выделить ключевые технологии, по которым мнения различных зарубежных и российских аналитиков сходятся. В результате мы составили свой, адаптированный к отечественным реалиям ТОП-10 средств информационной безопасности, на которые надо обратить внимание в 2017 году.

1 Анализ поведения пользователей (User and Entity Behavioral Analytics)

Защищаясь от множества внешних угроз, не стоит забывать и про внутреннего нарушителя. Системы класса UEBA представляют необходимый функционал для защиты от злоумышленников-инсайдеров и механизмов внутреннего мошенничества, а также таргетированных атак от имени ничего не подозревающего пользователя. В основе работы системы — механизмы статистического анализа, математические модели и оценка отклонений от стандартного шаблона поведения пользователей.

2 Управление процессом разграничения прав доступа (Data Access Governance)

По статистике, организация с тысячей сотрудников имеет не менее трёх файловых хранилищ, каждое из которых содержит суммарно несколько тысяч вложенных папок с неконтролируемыми исторически наслоившимися правами доступа, состоящими из наследованных прав, прав-исключений для сервисных учётных записей, прав-исключений для администраторов, прав-исключений для когда-то привлекавшихся удалённых сотрудников подрядных организаций и так далее до бесконечности.

Система данного класса позволяет реализовать принцип минимальных привилегий за счёт постоянного аудита, контроля и выстраивания корректного процесса согласования факта получения дополнительных прав доступа.

3 Несигнатурные методы анализа (Non-signature analysis)

С каждым годом скорость появления новых зловредных программ и методов, используемых нарушителями, увеличивается, и классический подход, при котором корпоративные системы защиты со временем «научаются» противостоять новому виду угроз, становится всё менее актуальным. Общий уровень рисков информационной безопасности можно значительно снизить, используя в дополнение к классическим средствам, методы, использующие механизмы защиты операционной памяти, основанные на применении белых списков и прочие.

4 Ловушки для хакеров (Honeypots)

Лучшее средство защиты — это нападение! А в нашем случае — ловушки для злоумышленников, предоставляющие возможность оценить их фактические действия, методы и цели с помощью изолированных от реальной инфраструктуры специальных программных комплексов, максимально похожих (для злоумышленника) на реальный уязвимый сервер.

5 Система обратной связи (Endpoint detection and response)

После обнаружения факта проникновения в корпоративную сеть реакция на инцидент должна быть быстрой, ответные действия эффективны в течение считанных минут. Системы класса Endpoint detection and response позволяют осуществлять постоянный мониторинг всех событий как на сетевом уровне, так и на уровне рабочих мест, непрерывно ведя поиск факта проникновения, а также предоставляя возможность моментально выполнить необходимое действие в корпоративной сети, например, завершить тот или иной запущенный процесс и удалить соответствующий зловредный файл.

6 Инструментарий для проведения криминалистической экспертизы (Forensic Toolkits)

Если нужно найти цифровые следы злоумышленника в его собственной аппаратуре, чтобы использовать их, скажем, в качестве доказательства в суде, то не



обойтись без обеспечения целостности исходных данных, на базе которых эти доказательства были получены. Лучше всего с этой задачей справляются решения класса Forensic Toolkits, способные достать в неизменном виде любые первоначальные данные: пароли, переписку, документы, фотографии, системные события и прочие данные почти с любого устройства, включая компьютеры, ноутбуки, серверы, мобильные телефоны, а также съёмные носители.

7 Система управления правами доступа на основе шифрования (Information Rights Management)

С глаз долой — из сердца вон! Не каждый CISO понимает, что ценная информация, выходя за рамки контролируемого периметра, по-прежнему должна быть защищена от несанкционированного доступа. Конечная ответственность за обеспечение целостности, конфиденциальности и доступности этой информации остаётся обязанностью её владельца, а не передаётся вместе с файлом.

Системы класса Information Rights Management предназначены для предоставления гранулированного доступа к документам, веб-страницам, письмам и прочим файлам путём использования шифрования даже после передачи данных файлов за границы контролируемой зоны.

8 Удалённый браузер (Secure Remote Browser)

Пытаясь бороться со следствиями, а не с источниками угроз информационной безопасности, компании игнори-

руют тот факт, что большинство угроз приходит в корпоративную сеть через Интернет, а основное средство доставки угроз в корпоративную сеть — браузер. Наиболее эффективным решением будет использование систем Secure Remote Browser, представляющих собой изолированную среду, в которой запускается браузер и осуществляется просмотр Интернет-порталов, что лишает зловредную программу малейшей возможности попасть на локальное рабочее место сотрудника.

9 Автоматизация процессов классификации информации (Classification Engines)

Как показывает практика, большинство организаций в погоне за количеством установленных систем безопасности не видят за деревьями леса. Сфокусировавшись на угрозах и возводя всё новые «непреодолимые» для злоумышленников «заборы», компании редко обращают внимание на то, вокруг чего эти «заборы» возводятся и по какую сторону находится то, что действительно надо защищать.

Гибридные средства автоматизации процессов классификации информации, такие как Docs Security Suite, позволяют не переплачивать за защиту информации, не имеющей ценности, забыть о перечнях информации, становящихся неактуальными в момент своего создания, обнаруживать всю ценную информацию на локальных рабочих местах и съёмных носителях, реализовать гранулированную настройку средств защиты информации, таких, как средства защиты от утечки. Плюс помогают

выстроить процесс жизненного цикла конфиденциальности информации в организации.

10 Защита бумажных носителей информации (Secure Managed Printing)

Вооружившись самыми современными средствами защиты от несанкционированного доступа к корпоративному компьютеру, мощной периметровой защитой на базе технологий нового поколения, системами защиты от утечек и прочими системами, невозможно защититься от злоумышленника, который по своим должностным обязанностям имеет доступ к печати ценной информации. Он элементарно положит распечатанные файлы в сумку и беспрепятственно покинет организацию.

Оптимальным решением будет использование систем класса Secure Managed Printing, способных обеспечить не только базовые функции управляемой печати, такие, как управление стоимостью, квотирование по стоимости, количеству, цвету (в том числе для локальных печатающих устройств), но еще и гранулированное управление доступом к печатным документам, автоматическую классификацию печатаемой информации на базе контентного анализа с соответствующей маркировкой, двухфакторную аутентификацию. А также при использовании таких решений, как PrinterGuard, имеющих возможность интеграции с системами электронной подписи, обеспечивает юридическую значимость изъятия бумажной копии документа из принтера или с территории организации.

МОЖНО ЛИ БАНКУ ОБОЙТИСЬ БЕЗ DLP-СИСТЕМЫ?



**Сергей
ОВЧИННИКОВ**
директор
по маркетингу
Центра защиты
информации
ГК «Конфидент»

Среди внутренних инцидентов информационной безопасности (ИБ) в организациях традиционно преобладают утечки информации. Для организаций кредитно-финансовой сферы это связано с особыми рисками, так как в результате намеренной или непреднамеренной утечки данных потери грозят и клиентам, и самим компаниям.

Ситуация осложняется еще тем, что каналов для утечки данных существует множество. Согласно рекомендациям Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации» (РС БР ИББС-2.9–2016), к потенциальным каналам утечки информации следует отнести электронную почту, Интернет и беспроводные сети (включая социальные сети и форумы), съемные накопители, телефон и факс, принтеры и другие периферийные устройства, фото- и видеокамеры и др.

ПРИНЦИП

«МИНИМУМА ПОЛНОМОЧИЙ»

Банк России рекомендует блокировать техническими средствами и организационными мерами потенциальные ка-

налы утечки информации, которые не требуются сотрудникам для выполнения служебных обязанностей, а в отношении разблокированных каналов — вести непрерывный мониторинг их использования и контроль. Эти рекомендации построены по принципу «минимума полномочий». Смысл его в том, что слишком широкий круг полномочий может стать причиной утечки информации. В зоне особого риска — администраторы, программисты, специалисты в области компьютерной техники и защиты информации. Особенно опасно, когда специалисты этого уровня входят в стовор с руководством подразделений и службы безопасности, с организованными преступными группами. В этом случае возможный ущерб и тяжесть последствий многократно возрастают. Разработчики документа ставят в приоритет работы по защите каналов передачи информации с помощью электронной почты, сервисов Интернета (социальных сетей и форумов), удаленного доступа по Интернету, съемных носителей, принтеров и копировальных устройств. Отдельно стоит отметить высокий приоритет по защите переносных носителей информации и средств вычислительной техники, которые могут быть использованы или утеряны за пределами информационной инфраструктуры.

ДВА НЕДОСТАТКА

Прежде всего, для защиты от утечек информации применяются DLP-системы. Эффективность работы DLP-системы достигается путем слаженного взаимодействия нескольких неотъемлемых составляющих, включая набор регламен-

тов, обучение сотрудников, мониторинг и анализ работы средств защиты информации. Для автоматизированной работы системы нужна точность фильтрации информационных потоков, четкий отбор того, какие сообщения могут быть пропущены, а какие нет. DLP-систему необходимо постоянно подстраивать, менять настройки в зависимости от возникающих новых бизнес-задач. В этом кроется один из недостатков DLP-систем: помимо затрат на внедрение она требует в дальнейшем существенных затрат на сопровождение. Еще один недостаток — это вероятностный подход, применяемый при настройке фильтрации. Когда система проверяет поток информации в соответствии со множеством загруженных в нее категорий и классов конфиденциальности, в разы возрастает вероятность ошибки определения класса, что приводит к утечке или лишает канал легитимности. Получается, что система защиты от утечек может не справиться должным образом со своим прямым предназначением.

ОГРАНИЧЕНИЕ ДОСТУПА

В отличие от DLP-систем, которые контролируют и анализируют потоки информации, системы защиты информации от несанкционированного доступа (СЗИ НСД) и средства контроля съемных машинных носителей информации (СКН) ограничивают доступ к информации. Такой подход наиболее органичен принципу «минимума полномочий». В пункте 9.1. рекомендаций Банка России по предотвращению утечек как раз идет речь о такой мере, как блокирование каналов, которые не требуются сотрудникам для выполнения

обязанностей. Другими словами, это и есть ограничение доступа, которое могут обеспечить СЗИ НСД и СКН. В ряде случаев оно наиболее предпочтительно, потому что проще и дешевле ограничить доступ, чем разрешить использование каналов информации сверх меры, а затем тратить дополнительные ресурсы на анализ этой информации с помощью DLP-системы.

ВОКРУГ СЪЕМНЫХ НОСИТЕЛЕЙ

Типовой набор функций СКН включает контроль подключения съемных носителей информации и разграничение доступа к ним, а также «теневое копирование». Главный недостаток таких СКН и их отличие от DLP-систем — это неспособность контролировать утечки информации. Дело в том, что в случае утери/кражи учтенного накопителя, информация может стать доступной злоумышленнику. Для решения этой проблемы на рынке есть специализированные решения с функцией преобразования на внешних накопителях. Однако их применение связано с дополнительными затратами для организаций, у которых уже внедрена СЗИ НСД.

Отметим, что ФСТЭК России установлены требования к использованию средств контроля съемных машинных носителей информации. Защитные меры включают в себя учет носителей, управление доступом, исключение несанкционированного доступа к хранящимся данным, контроль перемещения носителей, использования интерфейсов ввода/вывода, подключения носителей, уничтожение и контроль уничтожения информации при передаче носителей между пользователями и в сторонние организации. Требования по использованию съемных носителей также устанавливаются и Стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0–2014). В частности, в организации банковской системы РФ должен быть определен, выполняться и контролироваться порядок использования съемных носителей информации. Более того, устанавливаются требования по обработке персональных данных (ПДн) в организациях

ПРОЩЕ И ДЕШЕВЛЕ ОГРАНИЧИТЬ ДОСТУП, ЧЕМ РАЗРЕШИТЬ ИСПОЛЬЗОВАНИЕ КАНАЛОВ ИНФОРМАЦИИ СВЕРХ МЕРЫ, А ЗАТЕМ ТРАТИТЬ ДОПОЛНИТЕЛЬНЫЕ РЕСУРСЫ НА АНАЛИЗ ЭТОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ DLP-СИСТЕМЫ

банковской системы Российской Федерации, включая фиксацию и хранение ПДн на отдельных съемных носителях.

В 2014 году ФСТЭК России утвердила требования к средствам контроля съемных машинных носителей информации, профили защиты к каждому классу защиты. Требования касаются как контроля подключения носителей, так и контроля отчуждения информации, то есть предотвращения несанкционированного переноса информации ограниченного доступа с зарегистрированных (учтенных) съемных машинных носителей информации. Контролировать отчуждение информации необходимо для того, чтобы защитить данные даже в том случае, когда носитель используется вне доверенной среды, потерян или похищен злоумышленниками. Фактически, Регулятор определил требования к созданию доверенной среды внутри организации для безопасного использования съемных накопителей, что исключает утечки информации через съемные накопители.

ВЫХОД ЕСТЬ!

Таким образом, СЗИ НСД вместе с СКН по контролю подключения и контролю отчуждения (переноса) информации позволяют реализовать принцип «минимума полномочий», заложенный в рекомендациях Банка России по предотвращению утечек информации. DLP-система в режиме блокировки выполняет схожие функции в части контроля подключения устройств, однако, значительные ресурсы на системы такого класса тратятся заказчиками из-за наличия в них функций анализа информации, а не её блокирования.

На текущий момент на рынке СЗИ пока отсутствуют сертифицированные ФСТЭК России СКН по контролю от-

чуждения (переноса) информации, однако есть продукт, в котором реализован подход создания доверенной среды для безопасного использования съемных накопителей информации. Речь идет об СКН Dallas Lock разработки Центра защиты информации ГК «Конфидент» (ЦЗИ «Конфидент»). СКН Dallas Lock — это модуль в составе флагманского продукта СЗИ Dallas Lock 8.0. Пользователям СКН Dallas Lock не нужно беспокоиться за утерю или хищение съемных носителей — данные на них являются преобразованными. Функционал по работе с носителями реализован на основе требований ФСТЭК России к СКН уровня отчуждения. Помимо этого, для защиты от утечек информации реализован функционал по контролю подключения локальных и внешних устройств, запрет выхода в Интернет (работа с браузерами, «мессенджерами») с помощью мандатного доступа к устройствам (сетевой карте). Функция «теневого копирования» незаметно для пользователя сохраняет документы, отправляемые на печать или копируемые на съемные носители. Функционал СКН Dallas Lock позволяет вести централизованное управление.

* * *

СЗИ НСД и СКН в некоторых случаях более предпочтительны для защиты от утечек информации, чем DLP-системы, как экономически, так и с точки зрения реализации принципа «минимума полномочий». Функция преобразования данных, реализованная в СКН Dallas Lock компании «Конфидент», позволяет при этом защищать информацию на съемных носителях даже за пределами доверенной среды.



Мария ВОРОНОВА
ведущий эксперт
по информационной
безопасности, руководитель
направления консалтинга
ГК InfoWatch

КАК БЕЗОПАСНОСТЬ СОДЕЙСТВУЕТ БИЗНЕСУ?

Очень часто на вопрос «Какова цель информационной безопасности?» можно услышать классический ответ: «Обеспечение конфиденциальности, целостности и доступности бизнес-процессов». В принципе, это и верно, и неверно одновременно. Верно, потому что это одно из классических определений термина «информационная безопасность». Неверно, поскольку современный подход к ведению бизнеса требует иных специфик.

Итак, глобальная цель информационной безопасности — поддержание бизнес-стратегии, обеспечение должного развития бизнеса, снижение рисков, связанных с потенциальным нарушением данного развития. И информационные технологии, и информационная безопасность просто обязаны в текущей действительности оказывать существенное влияние на рост бизнеса и его сопутствующих процессов и процедур. Стратегии в области информационных технологий и информационной безопасности строятся на основе бизнес-стратегии и никак иначе.

Если одна из бизнес-целей стратегии компании, например банка — развитие цифровых технологий дистанционного банковского обслуживания, то какие же бизнес-цели должны быть поставлены перед информационной безопасностью? Во-первых, конечно же, обеспечение доверия клиентов, пользующихся цифровыми банковскими технологиями. За счет чего это может быть достигнуто? Превентивное обеспечение безопасности банковских сер-

висов, оперативное реагирование на инциденты информационной безопасности, если они все-таки произойдут. Во-вторых, обеспечение высокого уровня доступности банковских цифровых сервисов. Отказоустойчивость, стойкость к DDoS-атакам, отсутствие критичных ошибок в приложениях и сервисах. В-третьих, можно говорить о такой цели, как снижение экономических последствий от проблем с безопасностью в принципе: обеспечение должного, необходимого и достаточного уровня зрелости процессов информационной безопасности, внедрение комплексного антифрод-процесса и направления защиты от утечек и других внутренних угроз, комплексное реагирование на изменения, опять же — проактивное управление потенциальными угрозами информационной безопасности.

А теперь немного подробнее про цели, KPI (Key Performance Indicators, ключевые показатели эффективности) и индикаторы. Если целью бизнес-стратегии является обеспечение доверия клиентов, пользующихся цифровыми сервисами, она же транслируется как

высокоуровневая бизнес-цель для стратегии информационной безопасности. Ее интерпретация — наращивание количества клиентов банка, пользующихся цифровыми технологиями, и обеспечение их доверия. Индикатором может служить количество клиентов, упущенных в результате проблем с информационной безопасностью. А KPI могут быть примерно следующие:

- ♦ процент предотвращенных случаев утечки данных клиентов по электронным каналам;
- ♦ процент предотвращенных случаев хищения денежных средств клиентов;
- ♦ количество заявленных случаев потери клиентских данных (не более чем);
- ♦ сумма потерянных денежных средств в результате хищения (не более чем);
- ♦ количество случаев потери клиентских денежных средств (не более чем).

Конкретные показатели устанавливаются в соответствии с текущим уровнем информационной безопасности банка и планами/ожиданиями по его развитию.

**И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ,
И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ПРОСТО ОБЯЗАНЫ В ТЕКУЩЕЙ
ДЕЙСТВИТЕЛЬНОСТИ ОКАЗЫВАТЬ
СУЩЕСТВЕННОЕ ВЛИЯНИЕ НА РОСТ
БИЗНЕСА И ЕГО СОПУТСТВУЮЩИХ
ПРОЦЕССОВ И ПРОЦЕДУР**



Другой пример. Бизнес-цель, интерпретированная в цель для информационной безопасности — снижение экономических последствий от проблем с информационной безопасностью. Подцелями тут могут являться снижение влияния экономических последствий от проблем с информационной безопасностью и инвестирование в информационную безопасность с учетом бизнес-рисков. Индикаторы соответственно: снижение рисков, связанных с имеющимися уязвимостями и минимизация последствий от уязвимостей с учетом уровня бизнес-рисков. Возможные KPI:

- ♦ процент закрытых уязвимостей, прямо связанных с экономическими последствиями;
- ♦ средняя сумма возмещения из-

держек в результате инцидента (не более чем);

- ♦ количество уязвимостей, прямо связанных с влиянием на бизнес (не более чем).

На информационную безопасность в бизнесе влияет множество факторов — это как необходимость соответствия требованиям законодательства, всевозможным отраслевым стандартам, обеспечение должного уровня рисков информационной безопасности, прогнозирование и предотвращение внешних и внутренних угроз, также — соответствие уровня информационной безопасности потребностям бизнеса, обеспечение его роста: полная

готовность к масштабированию в случае появления такой необходимости. Это наиболее вероятно с точки зрения реализации, когда руководство (стейкхолдеры) вовлечено в существующие проблемы в области информационной безопасности и активно принимает участие в формировании соответствующей стратегии. В свою очередь, подобное тесное сотрудничество и понимание бизнес-целей помогает службам информационной безопасности эффективней для общих бизнес-целей распределять имеющиеся в их распоряжении ресурсы, обеспечивая при этом необходимый уровень безопасности и снижая действительно критичные для бизнеса риски, которые могут затормозить или даже отбросить назад его развитие.



Сергей ШЕРСТОБИТОВ
генеральный директор
группы компаний Angara

БУДУЩЕЕ — ЗА ПЕРСПЕКТИВНЫМИ ТЕХНОЛОГИЯМИ И СЕРВИСАМИ

Этот номер журнала выходит в январе — месяце, самом подходящем для того, чтобы подвести некоторые итоги развития отрасли в году минувшем и прикинуть, над чем предстоит потрудиться в ближайшем будущем. Генеральный директор ГК Angara Сергей Шерстобитов поделился результатами работы компании в 2016 году и поразмышлял о перспективных направлениях развития отечественной отрасли информационной безопасности.

Рынок информационной безопасности в России на сегодняшний день является весьма зрелым, все друг друга на нем отлично знают — и игроки, и заказчики, они даже иногда меняются местами. Денег на рынке становится все меньше, произошло уже практически полное насыщение рынка защиты инфраструктуры. Поэтому сейчас работающие в области ИБ компании фокусируются на защите данных и приложений. При этом заказчики все больше обращают внимание на то, насколько инвестиции в обеспечение информационной безопасности соотносятся с реальным и потенциальным ущербом от ИБ-инцидентов. Действительно, средства обеспечения информационной безопасности намного легче продаются в компании, которые уже подверглись внешним атакам или понесли ущерб от действий внутренних сотрудников.

Определенное влияние на развитие ИБ-рынка оказывает и импортозамещение. Западные игроки стали действовать более агрессивно, но не все из них решились бороться за наш рынок. Некоторые вовсе ушли с рынка, некоторые перевели все активности на российских партнеров, кто-то сократил

число сотрудников российских представительств. Отчасти зарубежных вендоров замещают отечественные.

Сейчас заказчики активно смотрят на новые технологии. На мой взгляд, наиболее востребованными на российском ИБ-рынке в ближайшее время будут: анализ больших данных, которых становится все больше и больше, а почерпнуть из них ценную информацию не всегда получается, и их безопасность; поведенческий анализ как на сетевом, так и на пользовательском уровне; threat intelligence-платформы и платформы для автоматического реагирования на инциденты.

Что касается группы компаний Angara, в 2016-м мы, как минимум, удвоили численность персонала относительно первого года жизни и утроили оборот. Отрадно отметить, что ряд новых специалистов обладает уникальной на российском рынке экспертизой. Осенью мы открыли дочернюю компанию — сервисный центр Angara Professional Assistance, став, таким образом, группой компаний. Центр будет заниматься предоставлением комплекса новых перспективных услуг в области информационной безопасности, выходить в сегмент SMB с новым уровнем

и объемом ИБ-сервисов, ранее предоставляемых интеграторами лишь Enterprise-компаниям и только на дополнительной платной основе. В 2017 году мы планируем запустить еще одно направление бизнеса. Все эти шаги направлены на поиск и развитие новых точек роста на зрелом и высококонкурентном рынке ИБ, которые должны обеспечить высокие темпы роста в нашем стратегическом горизонте.

О развитии информационной безопасности как услуги много будет говориться и на предстоящем в середине февраля IX Уральском форуме «Информационная безопасность финансовой сферы». Так, Angara 15 февраля проведет на форуме круглый стол, на котором мы поговорим с признанными экспертами отечественного рынка о том, как сделать ИБ-сервисы доступными не только для больших банков. Своими рецептами решения проблемы поделятся разработчики ИБ-систем и сервисов, а также представители банковского сектора. Приходите, будет интересно!

**РЫНОК ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ В РОССИИ НА
СЕГОДНЯШНИЙ ДЕНЬ ЯВЛЯЕТСЯ
ВЕСЬМА ЗРЕЛЫМ, ВСЕ ДРУГ ДРУГА
НА НЕМ ОТЛИЧНО ЗНАЮТ —
И ИГРОКИ, И ЗАКАЗЧИКИ, ОНИ ДАЖЕ
ИНОГДА МЕНЯЮТСЯ МЕСТАМИ**

ViPNet HSM PS:

НОВЫЙ УРОВЕНЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЛАТЕЖНЫХ СИСТЕМ



Дмитрий ГУСЕВ
заместитель
генерального директора
компании ИнфоТеКС

Популярность платежных систем в нашей стране стремительно набирает обороты. Сегодня в России общая сеть электронных устройств, принимающих банковские карты, состоит из 203,5 тыс. банкоматов и более чем из 1,7 млн электронных терминалов. По данным ЦБ РФ, в течение первой половины 2016 года с использованием карт на территории РФ и за ее пределами было совершено 8,2 млрд операций на общую сумму 23,4 трлн рублей.

Деньги переходят в онлайн, что, в свою очередь, несет новые угрозы для обеспечения безопасности платежных систем. Злоумышленники все чаще осуществляют несанкционированный доступ к конфиденциальным данным держателей банковских карт. С июля 2015 года по июнь 2016 года число несанкционированных снятий денежных средств со счетов банковских карт в нашей стране выросло в 5,5 раз.

В основу функционирования платежной системы заложен определенный алгоритм аутентификации. Чтобы предотвратить несанкционированный доступ к ключевой информации, которая необходима для аутентификации пользователей, ее хранение и передача производятся в зашифрованном виде. Платежные системы становятся все более популярными, количество пользователей и объемы ключевой информации увеличиваются. Это значит, что для защиты платежных систем требуются криптографические средства повышенной мощности, которые способны обрабатывать миллионы запросов в день от все большего числа пользователей. До сегодняшнего дня на российском рынке не было отечественных решений, которые соответствовали столь жестким требованиям к обеспечению информбезопасности платежных систем. Именно поэтому новый продукт компании ИнфоТеКС ViPNet HSM PS станет эффективным и во многом даже незаменимым инструментом для обеспечения информбезопасности в банковском секторе.

Сегодня для защиты платежных систем используются так называемые аппаратные модули обеспечения безопасности — HSM (Hardware Security Module), которые создают защищенную и устойчивую к взлому среду для безопасной криптографической обработки данных, а также защиты и управления криптографическими ключами. Новейшей разработкой на этом рынке является продукт компании ИнфоТеКС — ведущего российского разработчика программно-аппаратных решений в сфере информационной безопасности.

Продукт ViPNet HSM PS является российским аналогом зарубежных аппаратных криптомодулей. Помимо функционального соответствия зарубежным аналогам, в ходе тестирования ПАК ViPNet HSM PS показал более высокую производительность: на развернутом стенде производительность была повышена в 1,3 раза.

В 2016 году компания ИнфоТеКС получила выписку из положительного заключения ФСБ России о соответствии программно-аппаратного комплекса ViPNet HSM, предназначенного для криптографической защиты прикладных электронных сервисов, требованиям к СКЗИ для защиты информации, не содержащей сведений, составляющих государственную тайну по классу КВ и эксплуатируемые на территории Российской Федерации. Как результат, решение ViPNet HSM получило продолжение, и ИнфоТеКС создал сервис для банковских электронных систем платежных карт ViPNet HSM PS, который найдет эффективное применение в российской банковской системе в качестве альтернативного решения зарубежным аналогам и может эффективно использоваться заказчиками по программе импортозамещения. В настоящее время ViPNet HSM PS проходит завершающую стадию сертификации в ФСБ России.

В 2016 году компания ИнфоТеКС получила выписку из положительного заключения ФСБ России о соответствии программно-аппаратного комплекса ViPNet HSM, предназначенного для криптографической защиты прикладных электронных сервисов, требованиям к СКЗИ для защиты информации, не содержащей сведений, составляющих государственную тайну по классу КВ и эксплуатируемые на территории Российской Федерации. Как результат, решение ViPNet HSM получило продолжение, и ИнфоТеКС создал сервис для банковских электронных систем платежных карт ViPNet HSM PS, который найдет эффективное применение в российской банковской системе в качестве альтернативного решения зарубежным аналогам и может эффективно использоваться заказчиками по программе импортозамещения. В настоящее время ViPNet HSM PS проходит завершающую стадию сертификации в ФСБ России.

ViPNet HSM PS — первое российское решение для надежной и эффективной комплексной защиты процессов эмиссии банковских карт и обработки платежных транзакций с производительностью до 4000 операций в секунду в режиме проверки PVV/CVV. ViPNet HSM PS обеспечивает безопасность финансовых операций национальной платежной системы «Мир» в соответствии с требованиями российских регуляторов, а также платежных систем Visa и MasterCard.

* * *

В 2016 году компания ИнфоТеКС получила выписку из положительного заключения ФСБ России о соответствии программно-аппаратного комплекса ViPNet HSM, предназначенного для криптографической защиты прикладных электронных сервисов, требованиям к СКЗИ для защиты информации, не содержащей сведений, составляющих государственную тайну по классу КВ и эксплуатируемые на территории Российской Федерации. Как результат, решение ViPNet HSM получило продолжение, и ИнфоТеКС создал сервис для банковских электронных систем платежных карт ViPNet HSM PS, который найдет эффективное применение в российской банковской системе в качестве альтернативного решения зарубежным аналогам и может эффективно использоваться заказчиками по программе импортозамещения. В настоящее время ViPNet HSM PS проходит завершающую стадию сертификации в ФСБ России.

**ДЛЯ ЗАЩИТЫ ПЛАТЕЖНЫХ СИСТЕМ
ТРЕБУЮТСЯ КРИПТОГРАФИЧЕСКИЕ
СРЕДСТВА ПОВЫШЕННОЙ МОЩНОСТИ**

«КИБЕРУГРОЗЫ МНОЖАТСЯ, СРЕДСТВА ЗАЩИТЫ ТОЖЕ...»

НА ВОПРОСЫ BIS JOURNAL
ОТВЕЧАЕТ ЭКСПЕРТ КОМПАНИИ
ICL-КПО ВС АЛЕКСАНДР ЧЕЧУЛИН



Александр ЧЕЧУЛИН
руководитель проектов
отдела серверных
технологий компании
ICL-КПО ВС

— Многие эксперты прогнозируют рост хакерских атак на банки в 2017 году. Согласны ли Вы с данным утверждением? Какие кредитные организации представляют особый интерес для злоумышленников?

А. Чечулин: На наших глазах зародилась и стремительно развивается новая интернет-отрасль финансовых сервисов: дистанционное банковское обслуживание, платежные сервисы, полностью «виртуальные» банки и финансовые организации, электронные деньги. Каждый новый канал взаимодействия банков с потребителями услуг — это новые возможности для злоумышленников. Поэтому опасения относительно роста числа хакерских атак вполне обоснованы.

Полагаю, что наибольший интерес хакеры станут проявлять к организациям-новаторам, которые запускают новые сервисы и являются первопроходцами в вопросах их безопасности.

Пока можно констатировать, что регуляторика банковской сферы отстает от действительности. Обусловлено это объективными причинами. На подготовку любого стандарта необходимо время, а ИТ-ландшафт изменяется настолько стремительно, что регуляторы зачастую просто не успевают за новыми технологиями. Нельзя не отметить, что ЦБ ведет постоянную работу в области ИБ, и те новые аспекты, которые

не регламентированы в «стандартах», закрываются за счет целевых предписаний и распоряжений.

Но выполнение стандартов не гарантирует полной защиты от актуальных угроз, а лишь позволяет сформировать некий минимум, основу. Дальнейшее развитие систем информационной безопасности полным грузом ложится на соответствующие подразделения банков, и каждый справляется с этой проблемой сам, в меру своих возможностей.

Альтернативой решению задач ИБ только собственными силами может служить новый тренд, который сейчас завоевывает рынок, когда к процессу ИБ подключается внешняя организация — по аналогии с ИТ-аутсорсингом. При таком подходе банки-новаторы снижают свои риски за счет того, что получают экспертизу и опыт сторонней компании в условиях необходимости «быстрого старта» новых услуг. Банки могут значительно снизить нагрузку на бюджет ИБ, т. к. могут получить современные, актуальные решения с минимальными капитальными вложениями и тем самым снизить свои риски.

Наша компания сейчас активно прорабатывает это направление, в частности, мы готовимся открыть собственный SOC-центр для предоставления услуг по мониторингу информационной безопасности.

— Самое болезненное для любого банка — это потеря денежных средств. По данным ЦБ, за три квартала 2016 года хакеры попытались вывести из российских банков более 5 млрд рублей, из них около 2 млрд в итоге удалось похитить. Давайте остановимся на ключевых, самых неприятных для банков и самых популярных у злоумышленников видах хищений и рассмотрим методы борьбы с ними.

А. Чечулин: Существует множество видов атак. Давайте остановимся на «внешних» атаках, которые совершают злоумышленники, не являющиеся работниками банков.

Самые распространенные — это атаки на конечные точки получения услуг: атаки на системы ДБО юридических и физических лиц, взлом банкоматов, мошенничество с использованием данных банковских карт, поддельные интернет-сервисы, отмена операций при снятии денежных средств в банкоматах. И если раньше основной интерес для злоумышленников составляли слабо защищенные рабочие места клиентов, то сейчас направление атак смещается на сами банки, считавшиеся до этого неприступной цитаделью. Зафиксированы атаки как на АРМ КБР — программное обеспечение, отвечающее за отправку платежей с корреспондентского счета Банка, так и непосредственно на АБС, в которых производится учет всех банковских операций.

Чтобы добиться устойчивости к кибератакам, финансовым организациям необходимо применять комплексный подход. Начать стоит с выполнения отраслевых стандартов, но, как я уже го-

**НАПРАВЛЕНИЕ АТАК СМЕЩАЕТСЯ
С РАБОЧИХ МЕСТ КЛИЕНТОВ НА САМИ
БАНКИ, СЧИТАВШИЕСЯ ДО ЭТОГО
НЕПРИСТУПНОЙ ЦИТАДЕЛЬЮ**

ворил, в стандартах учтено далеко не все, поэтому специалистам по ИБ необходимо смотреть шире и проводить собственную оценку угроз, актуальных для организации.

Основные направления атак и меры противодействия:

- ♦ Мошеннические действия с клиентами банка. Все банки так или иначе проводят мероприятия по повышению осведомленности своих клиентов, но этого явно недостаточно. В этом смысле банк может «гарантированно» действовать только на «своей» стороне и пытаться выявлять мошеннические действия в своих системах, т.е. применять так называемые антифрод-решения. Хорошо спроектированный и правильно настроенный антифрод будет незаметен для легитимных пользователей, но выявит нехарактерные операции (транзакции из Африки и Японии с разницей в 1 час, смена номера телефона для одноразовых паролей и затем отправка платежа на всю сумму остатка по счету новому получателю и многие другие критерии). К тому же на рынке есть решения, которые сами обучаются типовому поведению пользователей и отправляют на дополнительную проверку платежи, не соответствующие типовому поведению этого клиента.

- ♦ Заражение ключевых узлов зловредным ПО (в т.ч. целевые атаки) и получение контроля. Здесь все зависит от действий специалистов банка. Базовый набор мероприятий достаточно типовой — максимально возможная функциональная и сетевая изоляция ключевых узлов, рекомендуемая вендором, безопасная настройка всех элементов системы, антивирусная защита, интеграция с антифрод-решениями для выявления нетипичных операций в целевых финансовых системах. Также рекомендуется применение специализированных решений по выявлению целевых атак (APT). С их помощью проводится изучение разноплановой информации о нормальном поведении узла и выявление отклонений от штатного функционирования, что позволяет обнаружить заражение, которое не было предотвращено иными средствами защиты.

- ♦ Эксплуатация уязвимостей в сервисах, опубликованных в Интернет,

СОВРЕМЕННЫЙ СОС — ЭТО ИНСТРУМЕНТ НЕ «БУМАЖНОЙ», А РЕАЛЬНОЙ БЕЗОПАСНОСТИ, КОТОРЫЙ ПОМОГАЕТ БАНКАМ ЭФФЕКТИВНО ПРОТИВОДЕЙСТВОВАТЬ КИБЕРУГРОЗАМ

в том числе атаки на отказ в обслуживании и атаки на НЕ финансовые сервисы банка с целью получения «плацдарма» в сети финансовой организации для развития атаки. Тут базовый набор мероприятий тоже не секрет — правильно выстроенный периметр сети (извне доступно только то, что необходимо), использование специализированных решений по обнаружению и предотвращению атак (IDS/IPS, WAF, решения по защите от DDoS-атак и т.п.), постоянный мониторинг опубликованных сервисов и случаев нарушения периметра, периодические инструментальные и «ручные» проверки на наличие уязвимостей. Большое внимание уделяется оперативному устранению выявленных несоответствий.

Очень важным элементом системы защиты является корректная эксплуатация внедренных решений и четко отлаженные, работающие процессы реагирования в банке. Многие атаки достигают цели по причине несвоевременного или неправильного реагирования внутренних служб.

В этой гонке вооружений нет финиша, но есть проигравшие. Поэтому система обеспечения безопасности должна расти и развиваться вместе с самими сервисами.

— Вы упомянули о новом тренде — аутсорсинге ИБ-услуг и создании так называемых Центров мониторинга ИБ (SOC). В чем их преимущество?

А. Чечулин: Современный SOC — это точка концентрации технологий, ресурсов и знаний для выявления, реагирования и расследования всех нарушений, инцидентов и атак, связанных с информационной инфраструктурой финансовой организации. Это инструмент не «бумажной», а реальной безо-

пасности, который помогает ИТ и ИБ службам банка эффективно противодействовать современным киберугрозам и атакам злоумышленников.

В последнее время набирает популярность модель использования услуг внешних SOC-центров, каковым как раз и будет Центр мониторинга ИБ, который открывает компания ICL-KPO BC. Такая модель дает банкам возможности сконцентрироваться на профильной деятельности и наиболее актуальна для средних и небольших финансовых организаций, у которых нет значительных ресурсов для построения собственных высокотехнологичных SOC-центров.

Использование сервисов внешнего SOC-центра дает финансовой организации целый ряд преимуществ. В первую очередь, это снижение затрат на организацию мониторинга информационной безопасности, поскольку не требуется нанимать дополнительный персонал, арендовать помещение, проводить закупки вычислительной техники, программного обеспечения и средств защиты информации. При этом сокращается и время ожидания запуска SOC-центра в действие — не нужно тратить время на установку и настройку программно-технических средств для SOC-центра и заниматься организацией процессов его работы. Кроме того, поставщик услуг в данном случае гарантирует банку четко заданный уровень услуг (SLA — Service Level Agreement) и независимый внешний мониторинг процессов обеспечения безопасности.

Для самого банка использование внешнего ресурса, как правило, означает снижение нагрузки на существующие подразделения ИТ и ИБ, высвобождение их ресурсов в целях развития сервисов банка.

КАК «ГОТОВИТЬ» ИБ-ВИЗУАЛИЗАЦИЮ



Михаил ЛАРИН
ведущий инженер
департамента ИБ АМТ-ГРУП

Для оперативного принятия верных решений необходимо обеспечить максимально эффективное восприятие информации специалистами ИБ и руководством. По этой причине в любой деятельности по обеспечению ИБ и, особенно, в работе центров мониторинга и реагирования (SOC'и, CERT'ы) аналитика всегда являлась фундаментальным компонентом. В связи с этим естественным было стремление расширить возможности аналитики за счет применения новых методов и приёмов. Одним из важнейших методов, который получил распространение в мировой практике ИБ, явился анализ с применением средств визуализации информации. Под визуализацией при этом понимается комплексный, и даже научный, подход к выбору и реализации визуального представления отчетов ИБ и информационных панелей средств ИБ.

В отечественной индустрии ИБ о визуализации начали говорить несколько лет назад. Например, АМТ-ГРУП подняла тему Security Intelligence как инструмента аналитики и визуализации в ИБ на SOC-Форуме в 2015 году, а в 2016 BIS Journal опубликовал статью моего коллеги на эту тему. Если судить по такому мероприятию, как SOC-Форум, то число докладов о визуализации в 2016 году увеличилось по сравнению с 2015 годом. Это не может не радовать, однако массового охвата тема, к сожалению, еще не получила. В данной статье я не буду углубляться в детали специфических кейсов, а расскажу о «кирпичиках фундамента» визуализации, некоторых её базовых принципах.

ПРЕИМУЩЕСТВА ВИЗУАЛИЗАЦИИ

Может возникнуть вопрос: а зачем вообще визуализировать информацию, неужели недостаточно текстового представления? Для ряда случаев, конечно, так и есть. Однако графическое представление более естественно для человека и позволяет гораздо лучше раскрыть возможности зрительного канала поступления информации¹. Среди основных преимуществ визуализации можно выделить следующие:

- ♦ ответ на вопрос в краткой форме;
- ♦ возможность создать и задать новые вопросы на основе графического представления;
- ♦ возможность дать новые знания и видение на основе существующих данных (т.е. визуальное представление одних и тех же данных в различных аспектах);
- ♦ улучшенная поддержка принятия решений ввиду возможности быстрого анализа огромных объемов данных;
- ♦ общее повышение эффективности представления.

ПРОЦЕСС СОЗДАНИЯ

Рассмотрим процесс создания визуального представления данных. В целом он схож для любой предметной области, не важно, ИБ это или нет. Можно выделить шесть основных шагов:

- ♦ определение проблемы;
- ♦ оценка существующих данных;
- ♦ обработка данных;
- ♦ выбор опций визуализации;
- ♦ преобразование визуализации для достижения фокуса на нужных элементах;
- ♦ интерпретация визуализации и принятие решений.

¹ Just V., Ludtke M., «Watching the Human Brain Process Information», Nieman Reports, 29 июня 2010 г.

ПРИНЦИПЫ ВИЗУАЛЬНОГО ОТОБРАЖЕНИЯ

Чтобы корректно выбрать размер, положение, оформление и тип, обратимся к «фундаменту», т.е. теории визуализации. Отображаемая картинка должна строиться по следующим правилам:

- ♦ использование свойств подпорогового внимания для соответствующего выделения цветом, формой, расположением важных элементов. Например, не рекомендуется использовать интегральные измерения для отображения нескольких характеристик (сочетание ширины и высоты — плохое, гораздо лучше — позиция и цвет);
- ♦ соответствие критериям Макинлея². Один из основных критериев подразумевает минимальную достаточность отображения, когда мы отображаем все факты из данных и только эти факты без добавления лишнего;
- ♦ использование принципов создания графиков, таких как:
 - ♦ улучшение соотношения данные/чернила и максимизирование использования значащих элементов (чем менее «загроможден» график, тем лучше читается);
 - ♦ использование не более чем 5 отдельных атрибутов при отображении нескольких измерений на диаграмме (не более 5 оттенков цвета, форм и т.д.);
 - ♦ использование принципов Гештальт-теории:
 - ♦ близость — объекты, расположенные близко друг к другу, воспринимаются как единый объект;

² Mackinlay J.D., «Automatic Design of Graphical Presentations» диссертация Ph.D., Факультет компьютерных наук, Университет Стэнфорда, Стэнфорд, Калифорния, 1986 г.

- ◆ замкнутость — объекты, форма которых почти закрыта (неполный круг и др.), воспринимаются как полная форма. Не злоупотребляйте закрытыми рамками;
- ◆ похожесть — мы объединяем похожие выглядящие объекты. Например, можно использовать выделение красным цветом атакующего узла на всех диаграммах;
- ◆ непрерывность — элементы, которые подогнаны друг к другу, воспринимаются одним целым;
- ◆ ограждение — ограждение элементов рамкой или расположение их в какой-либо форме группирует элементы;
- ◆ соединение — соединенные элементы группируются;
- ◆ подчеркивание исключений — выделение цветом или формой применяется для привлечения внимания к элементам;
- ◆ показ в сравнении — мощный метод для анализа, основанный на сравнении диаграмм, когда отображаются две диаграммы со значениями как было/как должно быть и как сейчас;
- ◆ комментирование информации — используйте комментарии настолько, насколько нужно, но не больше;
- ◆ показ причинности — коррелирование данных там, где это возможно (простой пример — график отказа серверов в связи с ростом температуры).

Среди перечисленного содержатся основные аспекты (но не все), на которые можно ориентироваться. Несмотря на кажущуюся очевидность и простоту этих правил, в них заложены основополагающие принципы эффективного и грамотного представления информации.

ОСОБЕННОСТИ ПОСТРОЕНИЯ ДИАГРАММ

После того, как определены основные правила построения диаграмм, можно рассмотреть их особенности. Но прежде всего нам нужно понимать, что мы визуализируем, т.е. иметь знания о типах данных. Для этого я предлагаю использовать классификацию шкал данных, предложенную в 1946 году С.С. Стивенсом³. В зависимости от типа шкалы измерений применяется та или

иная диаграмма, например, для номинального типа лучше использовать круговую диаграмму, в то время как диаграмма рассеивания совсем не подойдет.

Типы шкал измерений

- ◆ *Номинальный тип* используется для измерения данных, содержащих качественные признаки. Хороший пример — флаги TCP, действия (permit/deny) в логах межсетевого экрана;
- ◆ *Порядковый тип* используется для измерения тех данных, которые можно ранжировать. Например, критичность события (низкая, средняя, высокая);
- ◆ *Интервальный тип*. Как пример данных можно привести размер пакета, номера TCP sequence;
- ◆ *Абсолютный тип* — то же, что и интервальный, только для данных с явно существующим нулевым значением. Например, размер файла.

При этом данные, измеряемые по первым двум шкалам, являются неметрическими, а по последним двум — метрическими. Над метрическими данными возможно совершать математические операции. Данные для последних двух типов также зовутся непрерывными.

Также существует разделение на основные (независимые) переменные и зависимые переменные. Зависимая переменная — это та, изменение которой связывают с изменениями независимой переменной. Данное разделение влияет на то, где и как мы отображаем тот или иной тип переменной (чаще всего, независимая переменная идет по X, зависимая — по Y).

Цвета

Нельзя недооценивать важность выбора используемой цветовой палитры. Основная проблема — цвета близких оттенков трудноразличимы. По этой причине стоит использовать цвета на небольшом наборе данных номинального типа. Если не использовать легенду — убедитесь, что цвета на графике очевидны (красный — нечто опасное и плохое и т.д.). Нельзя использовать цвета только для украшения.

Формы

Кодировать измерения можно и через формы/расположения, однако чаще

всего цветовое кодирование является более предпочтительным.

Оси графиков

- ◆ Если метки на оси X тяжело читаются, часто помогает разворот графика на 90 градусов (инверсия);
- ◆ Отсчет на осях обычно должен начинаться с нуля;
- ◆ В ряде случаев оправдано применение нелинейной градации на осях (логарифмической).

ПРАВИЛА СОЗДАНИЯ ИНФОРМАЦИОННЫХ ПАНЕЛЕЙ

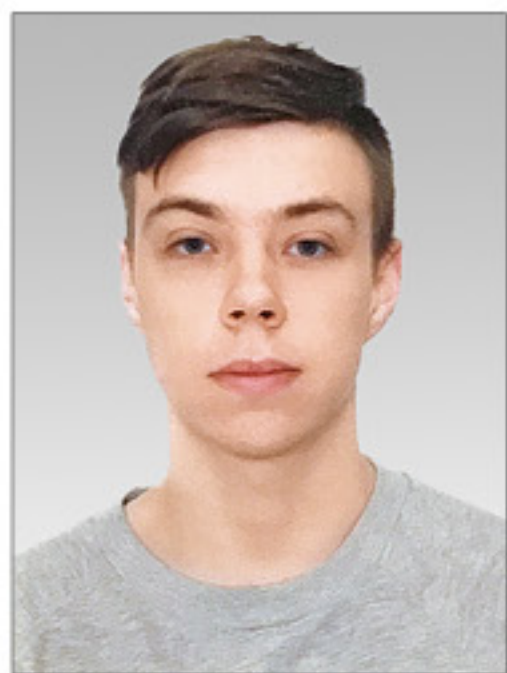
Кроме упомянутых принципов существуют несколько простых правил для создания качественной и полезной информационной панели.

- ◆ Один экран — один дашборд — законченная картина. При необходимости смотреть на несколько разных панелей или прокручивать одну большую панель очень сильно рассеивается внимание;
- ◆ Оптимальное число элементов на один дашборд — не более 5–6. Это нестрогое правило, для оперативных и аналитических дашбордов можно добавлять и больше диаграмм, однако важно не перегрузить их;
- ◆ Необходимый уровень детализации. Например, округление больших чисел;
- ◆ Нежелательно перегружать фон и добавлять лишние украшения;
- ◆ Для лучшего восприятия необходимый контекст может быть представлен в виде аннотаций или сопроводительных диаграмм.

* * *

Существуют специалисты, разбирающиеся в визуализации и специалисты, разбирающиеся в информационной безопасности. Количество специалистов с пониманием и квалификацией одновременно в этих двух сферах, пока, к сожалению, невелико. Но с ростом числа подобных людей индустрия ИБ выиграет в целом, т.к. существенно повысится качество анализа данных и, как результат, возрастет эффективность процессов.

³Stevens S.S., «On the Theory of Scales of Measurement», 7 июня 1946 г.



Никита КЕЛЕСИС
исследователь ИБ,
департамент аудита
защищенности
Digital Security

ЧУЖОЙ В БАНКЕ: ГОСТЬ, КОТОРОГО НЕ ЖДАЛИ

РЕАЛЬНЫЕ КЕЙСЫ ВЗЛОМА ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Исходя из практики проведения аудита защищенности, социальная инженерия является одним из наиболее эффективных векторов атаки, поскольку человеческий фактор — наиболее трудно контролируемый при обеспечении безопасности. Рядовые сотрудники банка, уровень технической осведомленности которых ниже, чем у работников информационных отделов, чаще всего доверчивы, и не подозревают, чем может грозить открытие фишинговых писем и запуск вложений. Злоумышленники способны найти почтовые адреса сотрудников из открытых источников и составить такое письмо, которое заинтересует пользователя скачать вредоносный файл или перейти на фишинговый сайт и ввести туда свои корпоративные учетные данные. При этом, письмо может быть оформлено в корпоративном стиле, что не вызовет подозрения.

БДИТЕЛЬНОСТЬ, БЫВАЕТ, ПРИТУПЛЯЕТСЯ

Помимо этого, есть сотрудники, работа которых связана с тем, что они обязаны открывать файлы из интернета (сотрудники кадрового отдела, менеджеры, техническая поддержка и т.д.). Вполне возможно, что ближе к концу рабочего дня их бдительность ослабевает, и злоумышленники могут воспользоваться этим.

В процессе подготовки атаки злоумышленники могут зарегистрировать доменное имя, схожее с легитимным названием, сформировать вредоносные вложения, которые при запуске закрепятся в системе и предоставят им

полный доступ к зараженной машине, проверят почтовые серверы на некорректную конфигурацию. Если они настроены неправильно, то при подключении к ним появляется возможность рассылать письма сотрудникам банка от любого имени (коллеги, руководителя, бухгалтера).

ПОД КОНТРОЛЕМ ТРЕТЬЕГО ЛИЦА

Наш опыт проведения тестов на проникновение с использованием социальной инженерии демонстрирует, что в подавляющем большинстве случаев хотя бы один сотрудник запускал вредоносное вложение, вследствие чего его компьютер оказывался под контролем третьего лица (в частности, нашего специалиста).

Как показывает практика, безопасность внутренней сети организаций находится на низком уровне и, как правило, получив доступ на одной или нескольких машинах, используя уязвимости ПО, словарные пароли, некорректную настройку групповых политик и т.д., нам удавалось захватить контроллер домена, а значит, мы получили возможность влиять на целостность, доступность всей инфраструктуры.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ ЯВЛЯЕТСЯ ОДНИМ ИЗ НАИБОЛЕЕ ЭФФЕКТИВНЫХ ВЕКТОРОВ АТАКИ, ПОСКОЛЬКУ ЧЕЛОВЕЧЕСКИЙ ФАКТОР — НАИБОЛЕЕ ТРУДНО КОНТРОЛИРУЕМЫЙ ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ

ЦЕПОЧКА УЯЗВИМОСТЕЙ

Еще одним случаем, когда удалось получить доступ к ключевым компонентам системы, являлась ситуация, при которой администраторский сегмент сайта использовал стандартные учетные данные. Его функционал позволял администраторам системы выполнять различные скрипты, а также произвольный код на уровне ОС. Просканировав внутреннюю сеть и выявив уязвимые компоненты, нам также удалось захватить контроллер домена, используя цепочку уязвимостей.

УСТАРЕВШЕЕ ПО

Нередко встречаются случаи, когда система использует устаревшее ПО с общеизвестными уязвимостями. Так, в ходе одного из аудитов защищенности было выявлено, что сайт банка подвержен уязвимости MS 15-034, позволяющей удаленно считывать фрагменты памяти веб-сервера, в одном из которых были обнаружены несколько корпоративных учетных записей, использованных в дальнейшем для развития атаки во внутреннюю сеть.

Не редки ситуации, когда банки используют не готовые решения, а собственное ПО с небезопасным кодом.



Найденные в них веб-уязвимости (DirectoryTraversal, SQL-injection) позволяли получить доступ к базам данных и совершать любые действия с ними (развивать атаку внутрь сети, контроль файлов, баз). В ряде случаев, из-за избыточных привилегий учетной записи, которая взаимодействовала с базой данных, нам удавалось получить выполнение произвольных команд на уровне ОС.

ЗАМЕТАЮТ СЛЕДЫ

Обычно атака разделена на несколько этапов: проникновение, закрепление и вывод денежных средств. После того, как работа закончена, злоумышленники старательно «заматают» следы, удаляя из системы вредоносное ПО, логи и прочие «отметки», которые могут привести к ним. Поэтому очень часто невозможно найти убедительное подтверждение того, что именно так или иначе была произведена атака.

ОСНОВНЫЕ ЦЕЛИ

Одной из основных целей для злоумышленников, попавших внутрь системы конкретного банка, является АРМ КБР, SWIFT (международная система совершения платежей), АБС (содержащая все данные о счетах клиентов), ДБО (системы, процессинг).

Стоит рассмотреть пример с атакой на АРМ КБР. Суть её — в простой подмене входных данных для АРМ КБР — платежного XML документа. FinCERT дает статистику попыток хищения данным методом на конец 2015 — начало 2016 года на сумму 2,87 млрд руб.

Сценарий, завязанный на подмене передаваемых данных, возможно реализовать в отношении SWIFT. Либо, учитывая, что данные из АБС всегда попадают на АРМ КБР, захватив контроль над АБС, у злоумышленника появляется возможность подделывать информацию о платежных переводах, которые будут попадать в АРМ КБР. Количество различных вариантов атак на внутренние связи между банками, различные варианты систем переводов, связей с банкоматами и т.д. очень велико.

Защита на уровне внешних атак не имеет смысла, если внутренний сегмент сети остаётся практически беззащитным. Особенно в таких критичных точках банка, как АРМ КБР, SWIFT и т.д. Под удар данные системы ставит невыполнение простых базовых рекомендаций, включая создание отдельного сегмента сети для данных критичных систем, использование электронных цифровых подписей, аппаратных токенов для АРМ КБР, вывод информации из корпоративного домена и т.д.

НАБОР ПРОБЛЕМ

Стоит отметить, что против таргетированных атак антивирусные системы практически бессильны. Основные проблемы, которые встречаются в ходе аудита защищенности, — это наличие избыточных привилегий пользователей на рабочей станции, отсутствие сегментации сети, устаревшее ПО, самописные сервисы, имеющие множество уязвимостей, отсутствие

средств защиты (ids/ips). Поскольку они нередко существуют в банках разного уровня, захват контроллера домена в большинстве случаев не представляет собой большой проблемы для атакующих. Далее, злоумышленники получают возможность завладеть контролем над всей инфраструктурой (серверами, базами данных, банкоматами, терминалами), создавать мошеннические платежные поручения, выводить деньги, изменять данные в базах данных, заражать банкоматы и многое другое.

* * *

Резюмируя вышесказанное, можно отметить, что ключевым моментом является не то, что злоумышленнику удалось проникнуть внутрь системы, а то, насколько правильно и безопасно построена инфраструктура. Не всегда злоумышленнику нужно ломать банк снаружи, он может устроиться совершенно легально в данный банк сотрудником и иметь доступ во внутреннюю сеть. Обязательно должна быть сегментация сети, которая избавит от множества проблем, и строгая фильтрация между сегментами. К примеру, даже если серверный сегмент использует уязвимое ПО, но доступ к нему имеют только администраторы сети, то нарушителю будет крайне трудно проэксплуатировать уязвимости, поскольку изначально ему нужно будет получить контроль над машиной администратора. Помимо этого, основными рекомендациями также являются корректное разделение привилегий у учетных записей, обновление всего ПО до актуальных версий, внедрение антивирусных и мониторинговых средств и регулярное проведение аудита защищенности как своими силами, так и при помощи привлечения аутсорсинга. Неотъемлемой частью в обеспечении безопасности также является организация тренингов для сотрудников с целью повышения уровня технической осведомленности, на которых стоит показывать, как безопасно работать с поступающими письмами, вложениями.

АНТИФРОД НА ПОРОГЕ МАШИННОГО ОБУЧЕНИЯ



Алексей СИЗОВ
руководитель направления
противодействия мошенничеству
Центра информационной безопасности
компании «Инфосистемы Джет»



Сегодня Machine Learning (ML) используется во многих достаточно сложных моделях аналитики: от прогнозирования погоды до анализа биржевых котировок, от медицинских исследований до контекстной рекламы. А что обуславливает необходимость применения ML в области борьбы с фродом? Первое — несовершенство других существующих технологий. По данным IDC, объем данных, хранимых в цифровом виде, удваивается каждые два года. То же можно сказать и о большинстве банковских продуктов или услуг. В реальности темпы роста объемов данных гораздо выше. Причина в том, что современные организации уделяют все больше внимания не только критическим операциям, но и вообще любым действиям клиента в дистанционном канале или сотрудника в офисе обслуживания.

К этому стоит добавить пополнение информации о клиентах. Основные игроки рынка ведут внутренние и партнерские процессы по обогащению данных о клиенте — «Know Your

Customer!». А это подтверждает справедливость и другой оценки аналитиков ИТ-отрасли: связанность данных возрастает на 50 % в год.

Суммируя два показателя, можно говорить о коэффициенте увеличения объемов информации, равном 4. Это можно считать грубой оценкой степени ежегодного усложнения работы фрод-аналитиков и офицеров систем фрод-мониторинга. И это без учета тренда к построению единых кросс-канальных систем фрод-мониторинга. Сохранять необходимое качество выявления фрода с каждым годом становится все сложнее, особенно если это делается лишь за счет человеческих ресурсов и простой автоматизации. К тому же задача поиска квалифицированного сотрудника год от года усложняется.

Вторым фактором, в какой-то мере субъективным, можно назвать решение крупнейших игроков банковского и платежного рынков о применении методов ML и систем на их основе. Так, в декабре 2016 г. MasterCard объявила о начале построения такой системы ввиду снижения качества классических,

почти 15 лет используемых методов обнаружения мошенничества. К слову, на рынке РФ антифрод с режимом самообучения существует еще с 2012 г., правда только в виде «черного ящика», эксплуатация которого порой вызывает много вопросов у конечных пользователей.

Означает ли все сказанное, что решение комплексных задач по принятию решений в области противодействия мошенничеству пора переложить на плечи искусственного интеллекта или, по крайней мере, автоматизировать этот процесс до такой степени, что участие в нем человека сведется к роли контролера и оператора при решении внештатных ситуаций? Скорее нет. Человек пока является ключевым звеном, в том числе, при построении моделей ML. Но вот решение частных задач оценки риска и перестроения моделей под изменяемые параметры входящего потока операций, а тем более регистрации новых случаев мошенничества — задача, с которой компьютер, снабженный математическим аппаратом, справится быстрее и гораздо качественнее.

**АНТИФРОД:
КРИТЕРИИ ВЫБОРА**

Каким критериям традиционно отдавались предпочтения при выборе антифрод-решений?

♦ *Гибкость интеграции с различными источниками.* Сейчас это устойчивый базис для всей антифрод-индустрии.

♦ *Функциональность настройки и ее доступность относительно применяемой аналитики.* Но на практике это диаметрально противоположные понятия. Повышение доступности при высоком уровне реализации правил и политик неизбежно приводило компании-производители к повышению сложности внесения корректировок, вплоть до необходимости работы с системой на уровне языка программирования.

♦ *Удобство пользовательских интерфейсов.* Но с годами этот критерий перерос лишь в требования к управлению, и относительная простота для операторов была почти полностью нивелирована в угоду созданию в банках централизованных систем управления инцидентами или обращениями клиентов.

Какие же характеристики сегодня является обязательным критерием выбора? На наш взгляд, их только две: **скорость и точность**.

Скорость — это не только скорость обработки операций, но и скорость создания и тестирования правил — ведь это ключевой показатель способности системы быть настроенной. Время создания правил под новые типы фрода — тот интервал, когда риск реализации мошенничества, особенно нового типа, максимально велик. Требование скорости распространяется и на принятие решения по формированию в антифрод-системе уведомлений о тех или иных зафиксированных рисках. В первую очередь, оно основывается на интерпретируемости результата работы антифрода и достаточности данных для ручного анализа оператором системы. И, наконец, одна из наиболее актуальных в последнее время характеристик — скорость масштабирования решения.

Точность — за этот показатель отвечают множество метрик. Две ключевые — false positive (FP) и false negative (FN), метрики, напрямую влияющие на

финансовый результат. Важно обеспечить возможность максимально точного управления этими параметрами системы еще на стадии создания правил и выбора аналитиком моделей решения. Если скорость — это технологическая платформа, а уже потом ML, то инструменты контроля и гарантии уровней FP и FN — это целиком и полностью задачи методов машинного обучения.

**АНТИФРОД
НОВОГО ПОКОЛЕНИЯ**

Что мы сегодня понимаем под применением ML в антифроде? Все более распространенными становятся системы помощи при создании правил и политик анализа с заданными FP и FN, работающих на базе интерпретируемых моделей ML, например, деревьев решений. Но достаточно ли этого для полноценной работы, и что скрывается за применением полного спектра моделей?

На наш взгляд, оптимальный подход — открытая платформа для работы с моделями машинного обучения. Мы реализовали фабрику, которая самостоятельно анализирует данные и генерирует оптимальную модель. Фабрика использует наиболее успешные подходы, которые применяются на сегодняшний день в области ML — оптимизацию гипер-параметров, сложные ансамбли моделей, нейронные сети. В результате мы получаем подготовленную модель, описанную в международном стандарте PMML.

Так мы решаем несколько важных задач — обеспечиваем открытость полученного результата, полную совместимость с продуктами сторонних вендоров, возможность полного контроля над процессом выявления мошенничества. Компании могут изменять математическую модель, не боясь потерять работоспособность системы, и использовать собственные наработки в удобных для них инструментах.

В то же время модели должны отвечать и требованиям скорости. В нашем понимании, это работа антифрод-системы в режиме online со скоростью анализа в 0,1–0,2 секунды на пике плюс возможность обучения модели в минимальные дискретные промежутки времени — не дни, а часы, а при необ-

ходимости и минуты между полными циклами обучения.

Однако абстрактная потребность в ML не говорит о том, как правильно выбрать схему использования таких моделей.

Мы выбрали 3 основных направления:

1. Классические обучаемые алгоритмы, целью которых является выявление ранее зафиксированного фрода, т.е. обучение «с учителем»;

2. Обучаемые модели по выявлению аномалий. От предыдущих они отличаются в двух ключевых аспектах. Первый: их цель — выявить не одну операцию или маленькую группу, а распознать глобальный объект (клиента, счет, платежный инструмент), подверженный рискам мошенничества. Второй: механизмы обучения применяются лишь на вершине цепочки модели — аномалии формируются без учителя, экспертно-статистическими методами, а обучение используется для выбора доверительных интервалов определения аномалий, которые формируются в виде инцидентов. При этом ни одна аномалия не будет полностью отвергнута как нерискованная;

3. Контроль информационных технологий. Это направление детального анализа последовательности операций в рамках некоторого процесса: формирования платежного поручения клиентом, заведения заявки на перевыпуск карты и т.д. Цель — выявление риска совершения отдельных действий в последовательности операций. Как показывает практика, такой анализ позволяет обнаруживать аномалии в банковских процессах, в том числе, признаки реализации мошеннических или противоправных действий.

Среди других особенностей созданного нами решения — платформа, свободная от использования реляционных СУБД, очень гибкая схема выбора аппаратной платформы, уникальные инструменты управления решением и инцидент-менеджмент, созданный специально для полноценного и удобного контроля кроссканальных схем мошенничества. Но главным преимуществом является высокая точность выявления фрода с минимальными показателями ложных срабатываний.

КАК ЗАЩИТИТЬ БАНК ОТ КИБЕРУГРОЗ?



Максим ФИЛИПОВ
заместитель
директора
по развитию
бизнеса компании
Positive Technologies
в России

Кибератаки уже превратились в серьезную проблему для финансовых учреждений. По данным Банка России, за 11 месяцев 2016 года хакеры украли у российских банков и их клиентов 2 млрд руб. В этот период были зафиксированы 23 масштабных попытки хищения средств в различных кредитных организациях, а число атак за второй и третий кварталы выросло в шесть раз. По оценкам Сбербанка, к 2018 году число киберпреступлений может вырасти почти в 4 раза, а ущерб от них может превысить 2 трлн руб.

При этом все чаще интерес для злоумышленников представляет банк целиком со всеми его уязвимостями: на периметре, в серверной части ДБО, в АБС, в системах обработки внешних платежей (АРМ КБР, SWIFT). Киберпреступники проникают в сеть банка, взламывают процессинговые центры и выводят деньги через банкоматы или торговые терминалы. Для эффективного противодействия таким угрозам банкам необходимо существенно повысить уровень защищенности приложений на различных уровнях.

БЕЗЗАЩИТНЫЕ САЙТЫ

Банковская отрасль лидирует по количеству веб-приложений с уязвимостями высокого уровня риска, реализация которых чревата более чем существенными потерями. Например, благодаря

веб-уязвимости был взломан банк JP-Morgan Chase, после чего расходы на информационную безопасность банка были увеличены на 250 млн долларов. Недостаток безопасности в веб-приложении привел к утечке данных 70 млн клиентов американского ритейлера Target, банкам пришлось перевыпустить более 17 млн карт. При этом наш опыт проведения аудитов безопасности демонстрирует постоянное выявление таких ошибок, как недостаточное разграничение доступа, возможность получения доступа к backend-системам и системам администрирования. Самые распространенные из таких уязвимостей встречаются практически в каждом банке и банковском приложении.

Сами по себе механизмы вторжения во внутреннюю сеть хорошо изучены: по нашим данным, в 60 % случаев вектор проникновения основывается на уязвимостях в коде веб-приложений. Однако традиционные средства защиты не способны обнаружить подобные атаки: интернет-приложения слишком интерактивны и многообразны для систем IDS, IPS, Next Generation Firewall. Для борьбы с веб-угрозами был разработан новый класс продуктов — web application firewalls (WAF), защитные экраны уровня приложений, осуществляющие передачу данных через HTTP, HTTPS, XML. К этому классу относится и PT Application Firewall, предназначенный для выявления и блокирования современных атак на веб-порталы, ERP-системы и облач-

ные приложения. Он может, к примеру, определить и заблокировать скачивание сайта банка с помощью робота, что, как правило, предшествует созданию фишингового клона. Или вычислить и заблокировать шаблонную активность по переводу денег, в том числе с помощью подделки запросов (CSRF), когда жертва заходит на сайт, созданный злоумышленником, и запрос от ее лица тайно отправляется на легитимный сервер.

УМНАЯ ЗАЩИТА ОТ DDOS

В контексте массированных DDoS-атак на финансовые организации России следует остановиться на одной из важных особенностей системы PT Application Firewall — продвинутой защите от DDoS-атак на прикладном уровне. В этом ей помогают алгоритмы машинного обучения. По данным Gartner, сегодня до 70 % DDoS-атак нацелены на уровень веб-приложений. Защиты на сетевом уровне уже недостаточно, так как боты маскируют свой трафик под легитимный, поддерживают веб-протоколы и эмулируют браузеры. Такие атаки протекают малозаметно и не требуют больших ресурсов: парализовать работу крупного веб-сайта можно с одного ПК, отправляя несколько десятков запросов в секунду. Эффективным решением для защиты сайта является комбинация традиционных средств противодействия DDoS с межсетевыми экранами прикладного уровня.

БАНКОВСКАЯ ОТРАСЛЬ ЛИДИРУЕТ ПО КОЛИЧЕСТВУ ВЕБ-ПРИЛОЖЕНИЙ С УЯЗВИМОСТЯМИ ВЫСОКОГО УРОВНЯ РИСКА, РЕАЛИЗАЦИЯ КОТОРЫХ ЧРЕВАТА БОЛЕЕ ЧЕМ СУЩЕСТВЕННЫМИ ПОТЕРЯМИ

ПРОВЕРКА КОДА НА УЯЗВИМОСТИ

Выявлять и устранять уязвимости на этапе промышленной эксплуатации в десятки раз дороже, чем это было бы на начальном этапе. Борьба с уязвимостями на этапе разработки отвечает требованиям не только здравого смысла, но и последним нормативам регулирующих организаций, таких как Банк России, ФСТЭК и PCI Council.

Система анализа исходного кода RT Application Inspector позволяет упростить и автоматизировать процесс безопасной разработки. В ней реализован уникальный гибридный подход, сочетающий преимущества статического, динамического и интерактивного анализа, а также используется огромная база знаний уязвимостей, накопленная экспертами Positive Technologies. Осенью 2015 года испытательная лаборатория ФСТЭК России внедрила RT Application Inspector для тестирования и сертификации средств защиты информации.

НА ОСТРИЕ АРТ-АТАКИ

В сложных инфраструктурах банков отдельные инструменты не способны эффективно противостоять комплексным атакам. Например, традиционные межсетевые экраны способны закрыть ненужные порты и заблокировать нежелательный входящий сетевой трафик, но не могут обнаружить и анализировать пакеты, содержащие вредоносные программы или справиться с атаками, которые проходят не через них. А системы предотвращения вторжений (IPS) позволяют исследовать потоки сетевого трафика, однако бессильны против атак на приложения на стороне клиента. Высокая сложность систем защиты делает задачу ручного сопоставления данных практически невозможной. Для человеческого восприятия событий слишком много — и только система SIEM на ранней стадии сможет сообщить о вторжении.

Из отчета FinCERT видно, что в 2015–2016 годах российские банки атаковали двумя основными способами — подменой файла для АРМ КБР и с помощью отмены транзакции. Атаки по первому сценарию, связанные с проникновением в сеть банка и формированием

ИЗ ОТЧЕТА FINCERT ВИДНО, ЧТО В 2015–2016 ГОДАХ РОССИЙСКИЕ БАНКИ АТАКОВАЛИ ДВУМЯ ОСНОВНЫМИ СПОСОБАМИ — ПОДМЕНОЙ ФАЙЛА ДЛЯ АРМ КБР И С ПОМОЩЬЮ ОТМЕНЫ ТРАНЗАКЦИИ

подложного XML-документа, направляемого в Банк России, напоминали эпидемию: с октября 2015 г. по март 2016 г. FinCERT зафиксировал 21 инцидент. Банкам удалось «отбить» у злоумышленников только 1,6 млрд руб. из 2,87 млрд руб.

Что может противопоставить этой атаке MaxPatrol SIEM? С помощью дополнительных средств предупредит о том, что нескольким сотрудникам банка поступили одинаковые вложения. Если с этих компьютеров одновременно начнут уходить SMB-запросы, то это будет уже подозрительно. Сопоставление событий на двух первых этапах могло бы помочь остановить атаку. Но можно подождать и третьего события — загрузки ботов на зараженные ПК. Сам факт того, что с нескольких компьютеров по HTTP кто-то «отлучался» одинаковыми запросами, а содержимое веб-страницы, куда заходили боты, было нехарактерно для человека, позволяет поднять тревогу.

Вторая атака связана с отменой транзакции: громкий случай, соответствующий этому сценарию, произошел в 2015 году. Преступники взломали банк «Кузнецкий», получили доступ к АРМ КБР человека, ответственного за отмену транзакций, и от его имени в автоматическом режиме отменили около 3 тысяч операций. Злоумышленники снимают деньги в банкоматах, после чего отправляют платежной системе запрос о прекращении операции. Мошенникам за короткий срок удалось опустошить свыше 200 банкоматов, принадлежащих различным банкам.

Даже если SIEM-система пропустила бы все шаги злоумышленников при входе в банк, то количество операций — это явная аномалия, и сигнал тревоги поступил бы уже после первого десятка таких событий. Отмена тран-

закции — довольно редкая и не самая элементарная операция, и человек не может выполнять ее дважды в секунду. К тому же при правильной настройке SIEM прекрасно дополняет антифрод-решения и может спасти деньги и деловую репутацию кредитной организации. Важно и то, что такие продукты помогают выстроить процесс управления инцидентами ИБ в соответствии с рядом стандартов — как опубликованными (СТО БР ИББС 2.5 Банка России), так и только вступающими в силу.

* * *

В условиях прогрессивно растущего интереса со стороны киберпреступников, современным банковским организациям со всем разнообразием их информационных и прикладных систем, приложений и пр. необходима комплексная система безопасности, включающая множество решений. Продукты Positive Technologies сегодня защищают информационные активы более 1000 компаний в 30 странах мира. Система MaxPatrol 8 заслужила доверие крупнейших кредитных организаций, в числе которых Intesa Sanpaolo, Societe Generale, Россельхозбанк. Несколько ведущих производителей банковского ПО используют RT Application Inspector для автоматизации процессов безопасной разработки, система RT Application Firewall обеспечивает безопасность веб-сервисов таких компаний, как «Связной», «МегаФон», «РосЕвроБанк», а возможности MaxPatrol SIEM уже оценили в нескольких банках, коммерческих и государственных структурах — с помощью этого продукта, в частности, была обнаружена деятельность ряда АРТ-групп.

БЕЗОПАСНОСТЬ КАК ДВИГАТЕЛЬ ДИСТАНЦИОННЫХ СЕРВИСОВ



Денис
КАЛЕМБЕРГ
генеральный директор
SafeTech

НОВЫЙ УРОВЕНЬ УДОБСТВА И МОБИЛЬНОСТИ ПРИ
СНИЖЕНИИ РИСКОВ КЛИЕНТОВ

Развитие дистанционных банковских сервисов — сложный и многогранный процесс, в который одинаково глубоко вовлечены и бизнес-подразделения банков, и департаменты, отвечающие за информационные технологии (ИТ) и информационную безопасность (ИБ). С одной стороны, бизнес-подразделения формулируют свои предпочтения и ставят техническим экспертам задачи, которые затем сообща решаются проектной командой. С другой стороны, департаменты ИТ и ИБ зачастую находят и предлагают к внедрению новые решения, способные снять ранее существовавшие «стопоры» и кардинальным образом улучшить банковские сервисы, сделать их более удобными для клиентов и прибыльными для банка.

Какие технологии являются приоритетными в настоящее время? Какие преимущества эксперты в области ИТ и ИБ могут предложить своим бизнес-подразделениям сейчас?

БИЗНЕС-ПОДРАЗДЕЛЕНИЯ, ИНИЦИИРУЯ ПРОЕКТЫ РАЗВИТИЯ ДИСТАНЦИОННЫХ БАНКОВСКИХ СЕРВИСОВ, ОБЫЧНО ОПЕРИРУЮТ ТЕРМИНАМИ КОЛИЧЕСТВА КЛИЕНТСКИХ ТРАНЗАКЦИЙ И ПРИБЫЛИ, КОТОРУЮ БАНК ОТ НИХ ПОЛУЧАЕТ

УДОБСТВО, ПРОСТОТА, БЕЗОПАСНОСТЬ. ЧЕГО ХОЧЕТ БИЗНЕС?

Довольно естественно, что бизнес-подразделения, иницируя проекты развития дистанционных банковских сервисов, обычно оперируют терминами количества клиентских транзакций и прибыли, которую банк от них получает. Тем не менее, безопасность информационных технологий зачастую становится ключевым фактором при реализации задуманного. Судите сами:

1. Высокий процентный доход по удаленным сервисам. Как правило, это ожидание бизнес-подразделения можно реализовать, снизив риски клиентов и, как следствие, увеличив лимиты на оплату и переводы денежных средств.

2. Возможность для клиента совершать как можно большее число транзакций. Логичное пожелание бизнес-подразделения. Чем больше оборот клиента в дистанционном банкинге, тем более эффективными и экономически выгодными становятся сервисы.

И в этом отношении подразделения ИТ и ИБ также способны помочь: возможность работы клиента и на стационарном рабочем месте, и на мобильном устройстве, а также удобное подтверждение операций позволят в хорошем смысле «приручить» его к дистанционным сервисам и способствовать повышению числа операций.

3. Общение с клиентами только на «приятные» и простые для их понимания темы. Конечно, бизнес-подразделения хотели бы упростить общение с пользователями и по возможности исключить такие вопросы, как установка и использование СКЗИ, драйверов, сторонних приложений и прочее-прочее. В данном случае департаменты ИТ и ИБ должны выбрать такие решения, которые не потребуют от клиентов специфических знаний и навыков. Чем проще и понятнее будут дистанционные сервисы, тем больше клиентов их выберут.

4. Сохранность денег Банка. Это краеугольное ожидание бизнес-подразделения банка. В этом отношении бизнес ожидает, что, с одной стороны, сама система ДБО будет устойчивой к атакам злоумышленников, а с другой, в случае возникновения инцидентов банк не проигрывал бы судебные иски и не терял собственные деньги. Таким образом, для сохранности денег банка дистанционные сервисы должны соответствовать требованиям законодательства в области информационной безопасности.

5. Дополнительный непроцентный доход. Как правило, бизнес банка ожидает, что безопасность станет не «затратной» статьей в обслуживании клиентов, а наоборот — ее можно будет продать пользователю и получить дополнительный доход. В этом смысле эксперты ИТ и ИБ в банке могут создать самостоятельные продукты «продвинутой» безопасности, которые заинтересуют клиентов, окажутся востребованными и будут активно продаваться вместе с самими дистанционными сервисами.

Перечисленные ожидания бизнес-подразделений и возможности департаментов ИБ и ИТ вполне логичные и реальные. Главное — остановить свой выбор на тех решениях и технологиях, которые позволят эти требования выполнить.

СОВРЕМЕННЫЕ РИСКИ ИНТЕРНЕТ-БАНКИНГА И МОБИЛЬНОГО БАНКИНГА

В настоящее время риски в целом и целом остаются прежними — это возможность кражи денег со счетов пользователей. Она существовала и в Интернет-банкинге, но за счет активного использования клиентами смартфонов и планшетов, объединения на мобильном устройстве каналов создания и подтверждения документов эта операция для мошенников существенно упростилась.

Кроме того, много нареканий вызывает уже традиционное подтверждение операций с помощью SMS. С чем это связано? Дело в том, что SMS-канал изначально не был предназначен для передачи конфиденциальной информации. Сообщение может быть перехвачено как в канале оператора связи, так и в самом смартфоне. И мошенники отлично научились это делать! Долгое время SMS были самым дешевым «транспортом» до клиента, и банки этим активно пользовались. Теперь необходимо реализовать в дистанционных сервисах удобную и безопасную альтернативу.

Чтобы в настоящее время кардинально снизить риски кражи денег со счетов пользователей, необходимо соблюсти два главных условия:

- ♦ не передавать коды подтверждения транзакций по незащищенным ка-

налам связи, а генерировать их на стороне клиента;

- ♦ коды подтверждения должны формироваться в привязке к реквизитам каждой транзакции: то есть если мошенники как-то и перехватят пароль, то его нельзя будет использовать для подтверждения другого документа.

Эти условия можно выполнить при помощи аппаратных средств (MAC-калькуляторов), но этот вариант довольно затратный и требует сложной логистики. Второй способ — использовать программные средства подписи банковских транзакций, которые могут быть установлены на смартфон или вообще интегрированы в приложение мобильного банкинга. В идеале, это должна быть усиленная неквалифицированная подпись и даже квалифицированная электронная подпись.

«КЛАССИКИ» И «СОВРЕМЕННОСТИ» В ДИСТАНЦИОННОМ БАНКИНГЕ. ЧТО ИМ ПРЕДОСТАВИТЬ?

Среди пользователей дистанционного банкинга с определенными упрощениями можно выделить «классиков» — относительно консервативных клиентов, много лет использующих традиционные сервисы и средства их защиты, а также «современников» — клиентов, стремящихся использовать самые передовые технологии и сервисы на вновь выпускаемых устройствах. Бизнес-подразделения банков, как инициаторы развития дистанционных банковских сервисов, заинтересованы в охвате и «классиков», и «современников».

Для клиентов-«классиков» хорошо подходит технология «доверенный экран», используемая при подтверждении транзакции (в частности, отлично зарекомендовавшее себя решение SafeTouch от компании SafeTech). Данная технология защищает от всех известных на сегодняшний день удаленных атак, так как обеспечивает визуальный контроль данных, передаваемых в токен, и операции подписи блокируются до момента нажатия кнопки подтверждения.

Клиентам-«современникам» наилучшим образом подойдут решения

для безопасной и удобной замены SMS-паролей, обеспечивающие аутентификацию, визуализацию реквизитов платежа и подтверждение транзакций на мобильных устройствах (в частности, решение PayControl от компании SafeTech). Решение совмещает в себе удобство смартфона и безопасность MAC-калькулятора: реквизиты платежа (или даже PDF-документ) загружаются в смартфон автоматически, детали совершаемой операции удобно просматриваются на экране, а транзакция подтверждается усиленной неквалифицированной подписью.

НАЗАД В БУДУЩЕЕ. КРИПТОСЕРВИСЫ В ОБЛАКАХ И В МОБИЛЬНЫХ УСТРОЙСТВАХ

По нашему мнению, новый импульс развитию дистанционных банковских (да и не только банковских) сервисов может придать синергия, возникающая от сочетания мобильных и «облачных» технологий аутентификации и подписи транзакций. Хорошим примером может служить комплексное решение на основе PayControl и облачного сервиса электронной подписи «КриптоПро DSS».

Совместное решение позволит подтверждать платежные документы квалифицированной электронной подписью прямо на смартфоне. Решение уже передано на сертификацию в ФСБ России и, с нашей точки зрения, идеально подходит системам мобильного банкинга для юридических лиц. Теперь банки с минимальными затратами могут реализовать подтверждение платежных документов на мобильных устройствах квалифицированной подписью. С появлением интегрированного комплексного решения PayControl и «КриптоПро DSS» это стало реальностью. Для клиентов решение будет означать кардинальное снижение порога использования квалифицированной электронной подписи, существенное снижение затрат за счет отсутствия аппаратных носителей ключей, а также так желанную «полную мобильность» при сохранении юридической значимости электронного документа.

СМЕНА СУБД

КАК НЕ НАЛОМАТЬ ДРОВ ПРИ ИМПОРТОЗАМЕЩЕНИИ



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



Александр ДОДОХОВ
руководитель отдела
защиты баз данных
компании «Аладдин Р.Д.»

Информационная инфраструктура практически каждого банка имеет в своём составе базы данных, содержащих сведения, составляющие коммерческую и банковскую тайну, а также персональные данные. Значительное количество хранилищ данных функционирует под управлением СУБД Oracle, как одной из самых распространённых и зарекомендовавших себя с наилучшей стороны. Как по надёжности и масштабируемости, так и по удобству работы. Использование подхода, предлагаемого в статье, позволит минимизировать потери данных, времени и финансовых средств при решении одной из главных задач информационного противостояния — предотвращения утечек критически важной для банков информации за рубеж.

ТРУДНОСТИ ПЕРЕХОДА

Тенденция на скорейший переход с широко применяющейся СУБД Oracle на платформу неамериканского происхождения продолжает набирать обороты. Трудностей перехода настолько много, что их перечисление займёт всё отведённое на статью место. Приведём только некоторые из наиболее существенных.

Во-первых, подобрать полноценную замену по базовому функционалу, масштабируемости, надёжности, доступности, отказоустойчивости, поддержке определённого набора аппаратных платформ и программного обеспечения достаточно затруднительно. Во-вторых, существует недостаток квалифицированных разработчиков и специалистов по сопровождению. Как правило, СУБД используется в виде ключевого компонента в прикладных системах. Эти и не-

которые другие проблемы выбора для миграции целевых СУБД достаточно полно были рассмотрены ранее [1]. Кроме того, как показано в исследовании [2], из всех наиболее распространённых СУБД в Oracle штатным образом встроены самый полный набор сервисов безопасности. Другие СУБД, в том числе и отечественного производства, существенно отстают. Но проблема замещения программного обеспечения зарубежного производства состоит не только в отсутствии встроенных в СУБД и одобренных отечественными регуляторами механизмов защиты информации.

Эксплуатируемый в настоящее время парк информационных систем банков — это огромное количество хранящейся информации и кода, написанного за долгие годы поколениями программистов. Перенос данных в иную СУБД «в лоб» зачастую просто невозможен, так как СУБД может попросту не иметь возможности обрабатывать некоторые типы данных из другой [1]. Как правило, миграция данных на новую программную платформу предполагает полную ревизию и изменение практически всего объёма кода. От подобной работы не спасают даже декларируемые многими производителями СУБД «автоматизированные процедуры» миграции. Но и это только «вершина айсберга».

Например, широко распространённое программное обеспечение процессинга от компании OpenWay написано, в основном, на PL/SQL — процедурном языке Oracle. Предположим, нашёлся банк, который всё это переписал и стал работать в другой программной среде. Понятно, что теперь поддержка программного обеспечения является

«головной болью» самого банка, и рассчитывать на обновления и поддержку от производителя в данном случае глупо. Кроме того, не каждая организация может позволить себе содержать штат сотрудников для столь масштабных работ.

ИЩЕМ ВАРИАНТЫ

Вместе с тем необходимо отметить, что подход «разрушим до основания, а затем...» себя не оправдывает и нужно попытаться найти иные, более приемлемые варианты снижения зависимости от иностранных производителей. Ведь основная идея импортозамещения заключается не в «освоении бюджетов» на быстрое создание российских ОС, СУБД и других программных продуктов, а в обеспечении безопасности информационных систем, базирующихся на импортных программах. В данном случае уместно говорить не только о надёжности программного и аппаратного компонентов информационной инфраструктуры, но и об обеспечении информационной безопасности, прежде всего конфиденциальности циркулирующей в информационных системах банковской информации.

Важность обеспечения безопасности информации в государственных информационных системах, в том числе в финансовом секторе, не вызывает сомнений. И не секрет, что программы иностранного производства зачастую «грешат» закладками и прочими неприятными особенностями. Логично было бы в первую очередь обеспечить оснащение информационной системы набором средств защиты информации отечественного производства, прошедших соответствующую проверку. При-

менение данных «наложенных» средств должно быть направлено, в том числе, и на «введение в заблуждение» возможных закладок путём применения методов, неизвестных для существующего программного обеспечения.

ПОДХОД С ГАРАНТИЕЙ

Самый очевидный пример — применение шифрования с использованием российских криптографических алгоритмов. Внедрение средств защиты должно проходить поэтапно, с обязательным поиском в них возможных уязвимостей. И начинать следует с совершенствования или даже полной замены в СУБД штатных механизмов аутентификации. Далее необходимо обеспечить защиту каналов передачи данных между серверной и клиентской частью СУБД — потребителями и поставщиками информации. И, наконец, защитить данные в хранилище. Такой подход к построению защиты информационной системы и её «грамотная» эксплуатация могут дать гарантию безопасности обрабатываемой информации на значительном временном отрезке, в течение которого можно будет ожидать появления отечественного инфраструктурного программного обеспечения.

РЫНОК НЕ БЕДЕН

В настоящее время на рынке имеется много предложений от производителей по сертифицированным средствам аутентификации, в том числе аппаратным, которые могут быть адаптированы для работы с различными СУБД. Достаточно широко представлены средства защиты каналов передачи данных. Вместе с тем, из средств защиты баз данных, использующих российские криптографические алгоритмы, известно только одно — программно-аппаратный комплекс «Крипто БД» компании «Аладдин Р.Д.». Являясь наложенным средством защиты информации, предназначенным для внедрения в существующие информационные системы, комплекс «Крипто БД» решает широкий спектр задач. Прежде всего — шифрование данных, содержащихся в столбцах таблиц баз данных. Кроме того, комплекс обеспечивает надёжную защиту ключей шифрования, в том числе с помощью аппаратных ключевых носителей.

Первая версия комплекса «Крипто БД» была сертифицирована по требованиям ФСБ РФ в 2010 году, а затем срок действия сертификата был продлён в соответствии с правилами системы сертификации. Впоследствии, в рамках развития комплекса в соответствии с пожеланиями заказчиков появлялись новые функциональные возможности. Последняя версия комплекса «Крипто БД» поддерживает шифрование в таких СУБД, как Oracle, MSSQL, Tibero и PostgreSQL. В комплексе реализовано формирование и проверка электронной подписи, в том числе по недавно введённым ГОСТ 34.10–2012, ГОСТ 34.11–2012 для распределения ключей шифрования, а также собственно шифрование данных с помощью симметричных алгоритмов по ГОСТ Р 28147–89 и ГОСТ Р 34.12–2015. Кроме того, при создании комплекса были учтены все известные рекомендации профильных комитетов по стандартизации. В настоящее время выполнены тематические исследования комплекса «Крипто БД» и проводится экспертиза их результатов в ФСБ России.

КОВАРНЫЙ ФАКТОР

Необходимо отметить, что организации, прежде всего финансовые структуры, банки, опасаются внедрять средства защиты, связанные с шифрованием данных. Опасения связаны главным образом с двумя факторами: риском полной потери данных при утере ключа шифрования и риском значительной деградации производительности информационной системы в целом. Первый фактор достаточно субъективный: строго выполняя приложенные к продукту инструкции по резервному копированию ключей шифрования, риск потери данных сводится к нулю. Второй фактор более коварный: пока владелец инфор-

мации лично не убедится в том, что производительность его самой важной информационной системы не пострадает, он будет относиться к любым заверениям настороженно. Именно поэтому каждое внедрение комплекса «Крипто БД» предваряется пилотным проектом, в течение которого отрабатывается функционирование информационной системы с использованием шифрования зашифрованных данных и оценивается её производительность. Например, тестирование комплекса «Крипто БД» на процессинге Way4 в одном из крупных столичных банков не выявило заметных задержек при работе оператора с базой данных, в том числе при выполнении поиска по зашифрованным данным. Тестирование массовых операций класса пакетных загрузок/выгрузок, массовых начислений и пр. показало временные потери в пределах 10%. В самой трудоёмкой операции «закрытие операционного дня» максимальная временная задержка составляла до 40%. Безусловно, последняя цифра весьма приличная, но и она является приемлемой для разовых операций. Приглашаем банки, заботящиеся о сохранности своих данных, к пилотированию и внедрению с помощью широкой сети партнёров.

* * *

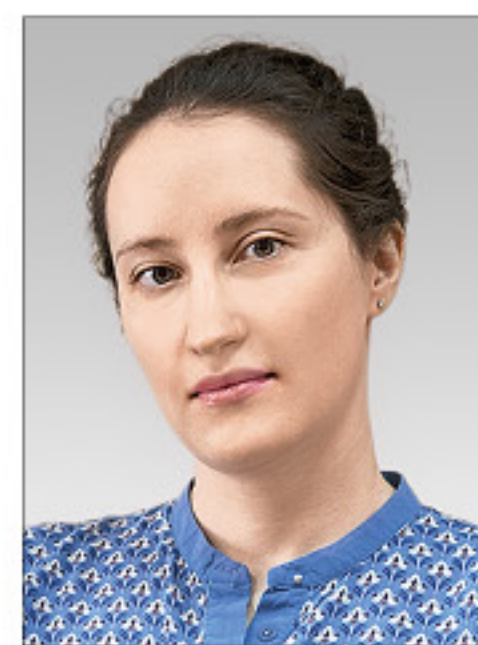
Подводя краткий итог, можно сказать, что предлагаемый подход к внедрению отечественных средств защиты информации в СУБД иностранного производства реализует основную идею импортозамещения — обеспечение безопасной работы информационных систем, критичных для деятельности организации. Ну и, конечно, будем ждать от наших разработчиков достойных аналогов известных СУБД.

ЛИТЕРАТУРА

1. Муравьев С., Дворянкин С., Насенков И. СУБД: проблема выбора // <http://www.osp.ru/os/2015/01/13045322>
2. Додохов А.Л., Сабанов А.Г. Исследование применения СУБД Oracle для защиты персональных данных // Доклады Томского государственного университета систем управления и радиоэлектроники. 2011. № 2(24). С. 267–270.

ТРУДНЫЙ СТАНДАРТ

КАК ПОСЛЕДНИЕ ТРЕНДЫ PCI DSS ВЛИЯЮТ НА ВАШ БИЗНЕС?



Анна АНТОНОВА
руководитель
направления отдела
безопасности банковских
систем компании
«Информзащита»

Выпущенный более десяти лет назад, стандарт PCI DSS является одним из наиболее развитых и проработанных документов в сфере информационной безопасности. Несмотря на это, совет по стандартам безопасности данных PCI ежегодно уточняет положения стандарта PCI DSS и выпускает дополнительные методические материалы. Так, в 2016 году вышла версия 3.2. Она вносит уточнения в существующие требования, самое важное из которых — перенос дедлайна по прекращению использования SSL и ранних версий TLS на июль 2018 года. Помимо этого, версия 3.2 содержит другие масштабные требования.

Стоит отметить, что все новые требования версии 3.2 вступят в силу 1 февраля 2018 г. Фактически, у организаций, попадающих под действие PCI DSS, остается всего один год на реализацию этих требований.

АУДИТОР — СВИДЕТЕЛЬ

Как показывает практика проведения аудитов на соответствие требованиям стандарта PCI DSS, а также результаты исследований компрометаций данных платежных карт, организации продолжают испытывать сложности в попытках достижения и поддержания соответствия PCI DSS. Одними из самых проблемных остаются требования по ежедневному мониторингу событий информационной безопасности, реагированию на инциденты, контролю уязвимостей, в том числе проведению

внутренних и внешних ежеквартальных сканирований уязвимости для всех системных компонент в области действия PCI DSS.

Помимо выполнения проблемных требований стандарта PCI DSS, многие организации не справляются с построением процесса, обеспечивающего непрерывное соответствие требованиям стандарта, и продолжают рассматривать задачу соответствия требованиям PCI DSS как срез на момент проведения аудита. Совет PCI SSC давно обращает внимание организаций, попадающих под действие PCI DSS, на необходимость поддержания соответствия требованиям стандарта в промежутке между аудитами. Так, в версии 3.0 PCI DSS, опубликованной в 2013 году, внедрение процессов BAU (Business-as-Usual) являлось одним из основных тезисов, хотя и не было обязательным требованием стандарта.

ВЕРСИЯ 3.2

Очевидно, что совет PCI SSC счел рекомендательный характер BAU недостаточно эффективным, и элементы BAU в версии 3.2 были добавлены в виде обязательных требований. Например, для соответствия требованию 12.11 сервис-провайдеры должны будут ежеквартально проводить мини-аудиты выполнения требований стандарта. Показательно, что под такой аудит должны попадать те самые проблемные требования PCI DSS — выполнение ежедневного мониторинга событий информационной безопасности и ана-

лиза логов, реагирование на инциденты, процесс управления изменениями и так далее.

Другое изменение в новой версии PCI DSS — требование по использованию многофакторной аутентификации при неконсольном доступе администраторов к среде данных платежных карт. С момента опубликования данного требования вызвало горячее обсуждение, как среди QSA-аудиторов, так и среди компаний-обработчиков данных платежных карт. Результаты многочисленных тестов на проникновение, проведенных «Информзащитой», подтверждают слабость паролей как единственного фактора аутентификации. Поэтому мы приветствуем добавление этой меры защиты.

УТОЧНЕНИЯ ПРОДОЛЖАЮТСЯ

Помимо очевидных затрат, которые несет в себе внедрение многофакторной аутентификации, стоит отметить, что совет PCI SSC продолжает вносить уточнения в само понятие многофакторной аутентификации и возможные методы ее реализации. Например, совет PCI рекомендует отказаться от использования SMS-сообщений в качестве одного из факторов аутентификации.

Еще одно интересное требование в новой версии PCI DSS было добавлено для сервис-провайдеров: этим организациям необходимо будет как минимум два раза в год проводить тестирование на проникновение для средств обеспечения сегментации. Требование еще раз подчеркивает важность подхода BAU для соответствия

PCI DSS, так как поддержание в актуальном состоянии области действия PCI DSS — один из важнейших его элементов.

ОБЛАСТЬ ДЕЙСТВИЯ

Вернемся к вопросу определения и подтверждения области действия стандарта PCI DSS. Правильное определение области действия является основополагающим моментом в достижении соответствия требованиям PCI DSS. Надо сказать, что, несмотря на более чем десятилетнюю историю существования стандарта, эта задача до сих пор представляет сложность для многих организаций.

В декабре 2016 года совет PCI SSC предпринял существенный шаг в разъяснении вопроса определения области действия, опубликовав официальные рекомендации на эту тему. Эти рекомендации должны помочь и проверяемым организациям, и QSA-аудиторам в нахождении общего языка как при первоначальном определении области действия, так и при ее подтверждении на сертификационном аудите.

Ключевым понятием в вопросе определения области действия PCI DSS является среда данных платежных карт (CDE). Повторяя определение, приведённое в стандарте, среда данных платежных карт — это люди, процессы и технологии, реализующие хранение, обработку и передачу данных платежных карт.

НЕ МЕНЯЮТ, А ДОПОЛНЯЮТ

В целом, опубликованные в декабре рекомендации не меняют существовавшие ранее определения, а дополняют их. Так, документ закрепляет 3 категории системных компонент — системы среды данных платежных карт (CDE systems), подключенные системы и системы, влияющие на безопасность CDE (Connected-to and/or Security-Impacting Systems), системы, исключенные из области действия PCI DSS (Out-of scope systems). При этом, новые рекомендации вносят небольшие уточнения в эти понятия. Например, любые системные компоненты, находящиеся в одном сегменте с системами, обрабатывающими данные платежных карт, отнесены к системам CDE, независимо от их назначения и причины размещения в данных



сегментах, тогда как ранее многие организации считали такие системные компоненты или подключёнными, или и вовсе исключёнными из области действия.

Новые рекомендации также обращают внимание на то, что во многих случаях компрометации данных платежных карт, нарушители получали доступ к среде данных карт через исключенные из области оценки системы. Поэтому организациям не стоит полагаться на реализацию мер обеспечения безопасности только для области действия PCI DSS — распространенные меры защиты должны быть внедрены и в остальной сети организации. К таким мерам защиты относятся своевременная установка обновлений безопасности, защита от вредоносного кода, управление доступом. Кроме этого, организациям стоит подумать об использовании дополнительных средств контроля доступа (например, хостовых межсетевых экранов и систем обнаружения вторжений) между подключёнными системами и системами вне области действия PCI DSS.

НЕ ОБЯЗАТЕЛЬНЫЕ, НО ПОЛЕЗНЫЕ

Совет PCI SSC продолжает обращать внимание на то, что некоторые средства защиты, хотя и не являются обязательными для соответствия требованиям PCI DSS, могут значительно облегчить достижение и поддержание соответствия. К таким средствам относятся, на

пример, DLP-системы, средства Data Discovery и Computer Forensics. Использование средств Data Discovery позволит проводить автоматизированный поиск мест хранения данных платежных карт во всей сети организации, вместо гадания о возможных местах хранения данных и ручного поиска с помощью регулярных выражений. Использование DLP также повышает степень уверенности и проверяемой организации, и QSA-аудитора в правильном функционировании механизмов сегментации. Например, совет PCI SSC рекомендует при использовании терминального доступа к среде данных платежных карт, контролировать с помощью DLP отсутствие утечки данных из CDE.

Как неоднократно обсуждалось, банкоматы и другие терминальные устройства, с точки зрения PCI DSS, являются таким же системным компонентом, как серверы и рабочие станции, и поэтому они должны соответствовать всем применимым требованиям стандарта. Данная точка зрения подтверждена и международными платежными системами.

В заключение хочется отметить, что постоянная консультационная поддержка QSA-аудитора поможет поддерживать соответствие требованиям PCI DSS в течение года, а также облегчит реализацию новых требований и рекомендаций совета PCI SSC.



FINOPOLIS 2016

ФУТУРИСТИЧЕСКИЕ КАРТИНЫ БУДУЩЕГО НЕ МОГУТ
ЗАСЛОНИТЬ НАСУЩНЫХ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ

Второй форум FINOPOLIS 2016 в Казани (организаторы — Банк России и Правительство Республики Татарстан) был посвящен перспективам развития финансовых технологий и стал крупнейшим событием банковской сферы России. В течение двух дней представители компаний финансового рынка, консалтинговых и IT-компаний, органов государственной власти, организаций, работающих в сфере обеспечения кибербезопасности и разработки программного обеспечения на 17 секционных заседаниях и круглых столах обсуждали вопросы регулирования инновационных финансовых технологий и бизнес-моделей, а также развитие конкретных техно-

логий, таких как блокчейн, инструменты Big Data, искусственный интеллект, Open API и многое другое.

Второе пленарное заседание было посвящено проблемам обеспечения кибербезопасности, что определило значимость этой темы в иерархии обсуждаемых вопросов. Предлагаем читателям сокращенную стенограмму этого заседания.

АЛХИМИКИ XXI ВЕКА

Евгений Касперский (АО «Лаборатория Касперского»): У нас на дворе цифровое средневековье. Компьютерные технологии пришли в нашу жизнь, мы к ним привыкли, радуемся... Но мы не научились делать их безопасными. Мы как средневековые алхимики,

которые уже умеют смешивать химические элементы, но все еще уверены, что вот-вот получится золото, а вместо этого то и дело получается взрыв. Алхимики не знали основ химии, которые знаем мы. Пройдет совсем немного времени — 200–300 лет, мы многому научимся, и компьютерные системы станут удобными и безопасными.

А пока цифры и их динамика следующие. Первый компьютерный вирус появился в 1986 году. За 20 лет непрерывного коллекционирования — с 1986 по 2006 год — я собрал примерно один миллион разных зловредных вирусов. Сейчас за одну неделю наша компания собирает в сети более двух миллионов различных образцов. Каждый день — больше 300 тысяч уникальных зловредов!



Президент Республики Татарстан Рустам Минниханов, Председатель Центрального банка Российской Федерации Эльвира Набиуллина и председатель Правления ПАО «Сбербанк России» Герман Греф на форуме FINOPOLIS 2016

В прошлом году по нашей статистике 100% бизнесов и 60% индивидуальных пользователей хотя бы один раз побывали под кибератакой. Много это или мало? Для сравнения, с уличной преступностью в том же прошлом году непосредственно столкнулось 3–5% населения планеты. Киберпреступность в разы агрессивнее: 52, 56, 62%... И эта цифра только растет!

Что такое 300 тысяч новых вирусов в день? Столько мы должны собрать, проанализировать, выпустить апдейт, протестировать его и доставить пользователям. Естественно, подавляющая часть этой работы делается автоматически. У нас стоят роботы, группы инженеров их тренирует, и роботы делают свою работу хорошо. Киберпреступники жалуются, что выпускают нового зловреда, а через несколько минут он уже детектится. У них времени не хватает, чтобы что-то украсть.

Тем не менее крадут. Из операционных систем главной жертвой была и остается Microsoft Windows, но с 2011 года произошли качественные изменения — начался стремительный рост атак на платформе Андроид. Объясняется просто. С одной стороны, новые киберпреступники на компьютерах уже не работают, они сидят в смартфонах. С другой, именно в 2011 году появились мобильные банковские сервисы. А преступники всегда идут туда, где деньги.

Какой ущерб наносит киберпреступность? Шесть лет назад мы провели собственные исследования — посчитали только ту часть, которую мы видим. У нас получилось 100 миллиардов долларов в год. Недавно подобные, но более широкие, исследования провели два независимых агентства. У одного получилось 400 миллиардов в год, а у другого 500. В целом я этим цифрам верю.

Что такое 500 миллиардов в год? Большой андронный коллайдер — гигантский международный проект — стоит 9 миллиардов. Так вот, киберпреступность стоит мировой экономике больше 50 таких коллайдеров в год. За десять лет можно всю физику с ног на голову перевернуть и открыть порталы в соседние Вселенные!

Как вообще можно украсть столько денег? Оказывается, можно. Первый пример: группа хакеров Carbanak с помощью компьютерного червя за два года обчистила около 100 банков в 30 странах на сумму более 1 миллиарда долларов. Многих поймали, но не всех. Это пример того, как криминальные группировки становятся все более профессиональными и масштабными, способными не просто атаковать, а вести долговременную войну с финансовыми организациями.

Такие группировки ведут осаду банка месяцами, незаметно проникая

все глубже, и в конце концов получают контроль над ключевыми, самыми боевыми частями организации. Увы, подобных инцидентов становится все больше и больше.

Второй пример — атака на Центробанк Бангладеш с целью украсть 1 миллиард долларов. 80 миллионов украли, и они исчезли, а транзакции еще на 870 миллионов были отклонены. Причина смешная — орфографическая ошибка или опечатка при заполнении формы.

Но банки — это только часть проблемы. Кибертерроризм, атаки на критическую инфраструктуру — энергетику, транспорт, телекоммуникации, средства связи... Пока без глобальных катастроф — потрогали дамбу в Америке, станцию по очистке воды в Европе, отключили электричество в некоторых регионах Украины, остановили домну в Германии... Подобные атаки происходят все чаще и чаще. Пока без разрушений. Пока.

Так почему мы живем в таком цифровом средневековье? Я называю это циклом инноваций: сначала что-то изобрели, потом порадовались, потом выяснили «ой, а оно же не безопасно», потом докрутили где нужно и сделали так, чтобы все было удобно, полезно и безопасно. Это относится ко всем технологиям: и к колесу, и к электричеству, и к пару... Некоторые изобретения не доживают до конца цикла по причине



Евгений Касперский, генеральный директор АО «Лаборатория Касперского»

небезопасности. Например, дирижабли. Начали падать, взрываться... Самолеты оказались надежнее. Так вот, цифровые технологии сейчас находятся на третьей стадии цикла. Они изобретены, мы ими пользуемся, радуемся, но уже начинаем понимать, что проблема кибербезопасности — это объективная и, более того, угрожающая реальность. И вот в приоритетах компаний этот пузырь кибербезопасности постепенно выплывает наверх.

Модератор Александр Галицкий (Almaz Capital Partners): Евгений, прямой вопрос. Вы давно занимаетесь этими вредоносными. Возможно ли их победить вообще, и как?

Евгений Касперский: Задайте этот вопрос тем, кто лекарствами торгует. Можно ли создать таблетку, которая победит все болезни? Наверное, нет. Так и у нас. Но у меня лично есть определение: достаточная или стопроцентная безопасность. Стопроцентная безопасность — это когда атака дороже, чем потенциальный ущерб. То есть атакующие должны вложить в разработку атаки больше ресурсов, чем та выгода, которую они в результате получают.

Можно ли достичь такого уровня? Я думаю, что не просто можно, а необходимо, если речь идет о критической инфраструктуре — энергетике, транспорте, связи и финансовых сервисах. Мы — как страна, как мировое сообщество — обязаны и можем сделать кри-

тическую инфраструктуру стопроцентно защищенной.

Модератор: А как? Что нужно делать?

Евгений Касперский: Рецепт известен, но почему-то не применяется. Необходимо все новые цифровые системы проектировать сразу с учетом возможных атак, а не так, как сейчас: сначала сделали, а потом вспомнили про безопасность и сверху — вжик! — антивирус прилепили. Надо безопасность продумывать и встраивать сразу, на стадии проектирования.

САМОЕ ГЛАВНОЕ НА БИРЖЕ

Модератор: У меня один вопрос ко всем участникам по очереди: назовите в трех пунктах, что для вас лично самое главное, если говорить о кибербезопасности ваших учреждений как о вашей личной ответственности?

Сергей Поляков (группа «Московская биржа»): Для нас, честно гово-

ря, множественные атаки, когда кто-то бездумно бродит по интернету и горстями разбрасывает вирусы, сегодня несущественны. Достаточно стандартное обеспечение легко с этим справляется. Реальная проблема — целевые атаки, когда ваша компания становится объектом специфического внимания, и вирусы строятся конкретно для вас.

Такие злоумышленники используют социальную инженерию, инсайдеров, пробираются внутрь системы и месяцами сидят в засаде. Украденную информацию сами они не используют, а продают или заказчику, или просто тому, кто купит. Классические варианты защиты тут не помогают.

У биржи своя специфика. Например, взаимодействие с клиентами меняется на глазах. Сейчас мы переходим к модели, когда доминантным способом взаимодействия становится программное взаимодействие. Как предприятие, мы даже не знаем, откуда приходит тот или иной запрос, кто за ним стоит. Вокруг разрастается целая экосистема программ и связанных компонентов. Поэтому защищать непосредственно периметр откровенно недостаточно. Надо защищать каждый элемент этой экосистемы.

В такой ситуации действия регуляторов, которые формируют требования и стандарты для подобных экосистем, гораздо важнее, чем наши конкретные действия в области программной защиты. Также резко возрастает необходимость сквозного идентификатора. Нет идентификатора — вы не знаете, кто к вам пришел. Есть идентификатор — необходимо гармонизировать эту систему в международном масштабе, иначе преступник сменит юрисдикцию и сможет работать под другим идентификатором.

«НЕОБХОДИМО ВСЕ НОВЫЕ ЦИФРОВЫЕ СИСТЕМЫ ПРОЕКТИРОВАТЬ СРАЗУ С УЧЕТОМ ВОЗМОЖНЫХ АТАК, А НЕ ТАК, КАК СЕЙЧАС: СНАЧАЛА СДЕЛАЛИ, А ПОТОМ ВСПОМНИЛИ ПРО БЕЗОПАСНОСТЬ И СВЕРХУ — ВЖИК! — АНТИВИРУС ПРИЛЕПИЛИ»



Станислав Кузнецов, заместитель председателя Правления ПАО «Сбербанк России»

СЕМЬ ПРОБЛЕМ ОТ СБЕРБАНКА

Станислав Кузнецов (ПАО «Сбербанк России»): Я хотел бы сфокусироваться не на трех, а на семи пунктах.

Первый. Нам необходимо — всем вместе — понять, что у нас нет никакой координации ни между кредитными организациями, ни между правоохранительными, ни между государственными институтами. Даже не понятно, кто лидирует в этой области: Министерство связи и массовых коммуникаций, Роскомнадзор или ФСБ? Нам нужно объединиться и научиться координировать свои действия.

Не секрет, что у нас нет никакого обмена информацией. Каждый банк имеет стоп-листы, у каждого есть своя база данных, но единой базы данных сегодня не существует, и те же самые преступники, протестировав Сбербанк, идут в ВТБ, потом в Бин и так далее. Создание системы обмена информацией — это первое, что необходимо. Лидерство тут за регулятором, мы все вместе должны помочь ему это сделать. В каком формате? Что-то вроде Бюро кредитных историй, возможно, как-то по-другому. Но такой инструмент стране необходим.

Второй. Регулирование с точки зрения законодательства. Почему преступники чувствуют себя комфортно в нашей стране? Потому что мы их даже преступниками не считаем. У нас нет понятий «киберпреступление», «кра-

жа с электронного счета»... Есть только одна смешная статья «мошенничество». Нам необходимо срочно всем вместе продвигать пакет законодательных инициатив в этой области.

Третий. Я лично противник регулирования, если говорить о коммерции, я за конкуренцию, но кибербезопасность — особая статья. Это та самая область, которая требует регулирования, причем, активного, оперативного. Если у нас срываются банкоматы, давайте сделаем стандарты, чтобы банкоматы имели автоматические системы защиты. Почему производители у нас диктуют заказчику? Почему с появлением технологии взлома black box регулятор не запретил подверженные ей банкоматы как класс? Почему страдают банки, которые ранее такие банкоматы купили? И таких примеров много.

Четвертый. Образование. Статистика: 35 процентов должностей в мировых компаниях в сфере кибербезопасности вакантны. Кадров нет. Говорить о переизбытке высоких профессионалов у нас в стране тоже не приходится. Надо объединяться и готовить специалистов, работать с вузами, влиять на образовательные стандарты. Сбербанк пытается что-то делать, мы заключили соглашение с передовыми вузами, собираем по субботам студентов, читаем им свои лекции, но это частный случай, как системная кадровая проблема и близко не решается.

Пятый. Международное сотрудничество. Мы все никак не осознаем, что у киберпреступников сегодня нет границ. Бессмысленно ГУБЭПу считать число кибергруппировок в России, они не только в России — давно рассыпались как горох по миру. Но если для них не существует границ, почему же границы существуют между нашими службами? Почему мы не объединяемся в различные международные ассоциации, мы же одним делом занимаемся!

Шестой. Новые технологии. Что из них сегодня в приоритете? Нам представляется, идентификация. Если появится надежная мгновенная идентификация нашего клиента по голосу, лицу, другим признакам, то это решит пусть не все, но почти все проблемы на уровне построения системы противодействия.

Седьмой. Культура. Действительно, мы живем словно в Средневековье, не понимая, что пришло новое время, требующее новой культуры. Нужно приучить себя относиться к гаджетам не как дикари к побрякушкам, а ответственно, научиться как минимум менять пароли. Люди сами отдают преступникам 99% информации. Даже дискуссия возникла: одни банки считают, что в случае преступления по технологиям социальной инженерии они ничего не теряют — это клиент виноват, он сам свои пароли отдал. Другая позиция — банки должны разделять ответственность, в том смысле, что клиент теряет, потому что продукт не совершенный.

Мы сторонники второго подхода. Например, с ноября в Сбербанке работает центр фрод-мониторинга, который останавливает и возвращает обратно на счета до 500 миллионов рублей, выводимых с помощью социальной инженерии.

НАС ЖДЕТ КИБЕРНАШЕСТВИЕ

Reinhold Wochner (Raiffeisen Bank International): Три года назад для банкоматов существовали всего один-два вируса, а сейчас их количество не поддается исчислению. Представляете картину, в три часа ночи все ваши банкоматы вдруг выдают все свои деньги неизвестно кому. В такой ситуации мы готовы перейти на виртуальные деньги, но наши клиенты привыкли полу-

чать наличные из банкоматов, у нас гигантская инфраструктура, и естественно, что нам остается только уповать на ужесточение стандартов. И роль регулятора тут самая главная.

В Австрии, конечно, далеко не все идеально, но у нас есть министерство, которое отвечает за кибербезопасность, это очень удобно. Например, не так давно регулятор получил рекомендации из Польши и принял решение усилить там кибербезопасность. К концу года там появятся специальные центры, потому что так прописано в законодательстве. Не важно, сколько это будет нам стоить, мы должны это сделать, и все. Так было в свое время и в Сингапуре. Результат положительный.

В Беларуси сейчас также формируется комитет по этим вопросам, но там есть проблемы. Мы не можем платить нашим людям больше, чем установлено белорусским регулятором. В европейских и американских компаниях там платят в долларах и евро, а мы не можем, так как мы — банк, находимся под регулированием. В результате специалисты по кибербезопасности уходят туда, где платят больше. Проблема с кадрами серьезно осложняет ситуацию.

Опять же по закону у нас принят определенный формат обмена информацией. И этот закон работает на пользу дела. Кроме того, Райффайзен активно взаимодействует международно. Мы вошли в ассоциацию 500 крупнейших банков и обмениваемся информацией в стандартизированном формате, долговременная ли это программа или оперативная работа по инцидентам. К сожалению, от России там нет представителей.

Согласен с Евгением Касперским, применительно к безопасности мы все еще находимся в мирке дирижаблей. Но нельзя забывать, что где-то уже летают самолеты. Например, в 2015 году из 10 беспилотных, абсолютно автоном-

ных автомобилей только один прошел дистанцию от Лас Вегаса до Сан-Франциско. В прошлом году уже 9 из 10. Технологии искусственного интеллекта — это не мечта, а вполне практические вещи!

И хакеры тоже их осваивают. Очень скоро нас ждет глобальное противостояние: искусственный интеллект киберпреступников против искусственного интеллекта киберзащитников. Мы забудем про русского хакера, немецкого или китайского, потому что будем иметь дело с гигантскими международными командами из 100–200 и более человек, конструирующими свои версии искусственного интеллекта, причем, не для кибератак, а для кибернашествия.

МОЖЕТ, КАК В МАЛАЙЗИИ?

Amirudin Bin Abdul Wahab (Cyber-Security Malaysia): В Малайзии наше агентство является правительственной компанией в области инноваций и технологий, и мы рассматриваем кибербезопасность как комплексное явление. Тут и управление, и технологии, и кадры... И мы координируем весь этот комплекс вопросов на государственном уровне. Мы отчитываемся перед двумя министерствами: Министерством науки и инноваций и Министерством обороны, отвечающим за кибербезопасность.

Мы разработали политику кибербезопасности, за ее осуществлением наблюдает Государственный Совет, который в свою очередь отчитывается непосредственно перед премьер-министром. Политика ориентируется на десять критических секторов, включая правительственный, финансовый, энергетический, транспортный и т.д. Каждый из этих вертикальных секторов имеет свой регулятивный орган. Например, в банкинге и финансовом секторе — это Центральный банк Ма-

лайзии, который работает с коммерческими банками. Все секторы тесно связаны как с генеральным офисом, так и с правоохранительными органами. При такой организации легко обмениваться информацией, получать общие улики, расследовать и пресекать киберпреступления.

В дополнение к этому мы предоставляем технические услуги и обеспечиваем обучение киберрейнджеров, из которых состоят спецподразделения по борьбе с хакингом. У нас также есть криминальная лаборатория по киберпреступлениям, и мы часто помогаем правоохранительным органам в раскрытии преступлений.

Случается, что уровень знаний наших оперативников и специалистов недостаточен, тогда мы взаимодействуем с другими игроками этого рынка, и они становятся нашими коллегами. Мы также активны в международном сотрудничестве, например, подписали меморандум о сотрудничестве с Лабораторией Касперского. Таким образом, мы формируем мощный защитный альянс, и это только часть наших инициатив.

ОТВЕТ РЕГУЛЯТОРА

Артем Сычев (Банк России): Сначала статистика. По нашим данным, объем покушений на хищение денежных средств со счетов российских банков и их клиентов за девять месяцев 2016 года составил 5 миллиардов рублей, из которых более 2 миллиардов удалось украсть. Сравнительно немного. Но тревогу вызывают не столько похищенные суммы, сколько динамика роста киберпреступности. А она на протяжении последних 3 лет увеличивается на 30% в год.

Два наблюдения. В 3 квартале 2015 года в России был отмечен максимум хищений со счетов юридических лиц, и резкое сокращение хищений в 4 квартале с последующим сокращением в 2016 году. В чем причина? В том, что на конец 3 и начало 4 квартала 2015 года пришелся пик внедрения системы антифрод в большинстве крупных коммерческих банков. Дело в том, что три года назад, еще на Уральском форуме, Центральный банк инициировал обсуждение этого вопроса,

«ОЧЕНЬ СКОРО НАС ЖДЕТ ГЛОБАЛЬНОЕ ПРОТИВОСТОЯНИЕ: ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КИБЕРПРЕСТУПНИКОВ ПРОТИВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА КИБЕРЗАЩИТНИКОВ»

после чего были приняты решения, технология антифрода прошла обкатку и, наконец, заработала. Результат налицо. Да, мы до сих пор не имеем законодательного или хотя бы нормативного закрепления работы по антифроду, но об этом позже.

Второе наблюдение. Физические лица. Тут другая ситуация: всплеск хищений в 1 квартале 2016 года. Почему? Ответ тоже простой. На конец 2015 года пришелся резкий подъем внедрения инновационных технологий в ряде кредитных организаций. Злоумышленники успели их прощупать, нашли подходы и стали активно осуществлять мошеннические схемы по извлечению клиентских денег. Безусловно, безопасники сработали оперативно, поэтому во 2 квартале такого всплеска уже не было. Но его могло не быть вообще, если бы система безопасности была заранее включена в новые финансовые технологии.

Возвращаясь к тому, что мы обсуждаем стандарты, хочу акцентировать совершенно правильно прозвучавший тут тезис: безопасность не должна быть наложенной, она должна быть включена в систему сразу — на стадии проектирования.

Это что касается технологий безопасности. А что происходит по ту сторону баррикад? На сегодняшний день киберпреступность — это давно уже не отдельно взятая банда, а развитая индустрия, которая, как и любой другой бизнес, имеет главной целью извлечение прибыли. Правда, прибыль там извлекается противозаконным способом, но, надо понимать, там есть и узкие специализации, и управление, и распределение полномочий. Например, те люди, которые пишут вредоносные программы, никогда не получают тех денег, которые уводятся у клиентов, они зарабатывают исключительно от продажи своего инструментария третьим лицам.

С отдельными бандами мы научились бороться, есть хорошие примеры — в мае прошлого года взяли большую группу злоумышленников, но к сожалению, инструментарий, которым они пользовались, до сих пор находится в продаже, и эта опасность не устранена.



Артём Сычев, заместитель начальника ГУБ иЗИ Банка России

Что делать в такой ситуации нам — регуляторам? Опять же, согласен, надо объединяться. Но объединиться в рамках какой-то одной государственной структуры, которая получила бы все полномочия, в наших условиях не реально. Тем не менее три года назад мы создали центр мониторинга и реагирования на инциденты — FinCERT, и теперь стараемся, чтобы его работа была направлена на то, чтобы коллективным разумом, коллективным оповещением банков решать проблему безопасности во всем ее многообразии.

Безусловно, полностью мы ее не решим, но давать полезную информацию коллегам о болевых точках уже получается. Безусловно, мы работаем не одни, у нас есть координирующий орган, его возглавляет первый заместитель председателя Банка России, в него входят все министерства, имеющие отношение к обеспечению безопасности.

Также совершенно правильно коллеги говорили о законодательстве. Мы прекрасно знаем, что его надо менять, и соответственно продвигаем две инициативы. Первая — это изменение уголовного кодекса с точки зрения переквалификации преступных деяний и увеличения наказаний, чтобы преступление и наказание были приведены в соответствие. Когда воруют миллиардами, а за это дают три года условно, и потом тот же человек, вернее, та же группа лиц, продолжает воровать миллиардами... тут возникает вопрос: а правильно ли это?

Вторая инициатива — это попытка узаконить обязанность любого банка работать с антифродом. Сейчас антифрод — дело добровольное, но деньги теперь путешествуют быстро, оказываются на новых счетах моментально, и нужно, чтобы они попадали к своим хозяевам, а не преступникам. Знаете, почему Тиньков заявляет, что он в своем мобильном банке не ощущает проблемы с киберпреступностью? Потому что воруют не у его клиентов, но именно через его клиентов ворованные деньги выводятся. А как только у этого банка появятся серьезные остатки по счетам клиентов, поверьте, он тут же сам станет объектом мошенников.

Далее я хотел бы обратить внимание на проблему кадров. У нас есть проект рекомендаций по стандартизации квалификационных требований к специалистам по безопасности. Это настольная книга, во-первых, для руководителей кредитных организаций, чтобы понимать, кого нанимать, какие предъявлять требования. Во-вторых, для учебных заведений, чтобы понимали к чему готовить студентов. Сейчас проект обсуждается в Техническом комитете, и мы очень надеемся, что он станет действительно рабочим документом. В принципе мы можем пойти и по довольно распространенному в мире пути обязательной сертификации хотя бы одного человека в финансовой организации.



СОС-ФОРУМ: ПОСЛЕВКУСИЕ

БЫЛО ВКУСНО, НО НА СТОЛЕ МНОГОГО НЕ ХВАТАЛО



Алексей ЛУКАЦКИЙ
эксперт информационной
безопасности

Уже второй год в Москве проходит SOC-Форум, целиком посвященный одной теме — центрам мониторинга кибербезопасности. Этим мне этот форум и нравится — он сфокусирован на конкретной теме, которую можно рассматривать с разных сторон на достаточно глубоком уровне. Вы можете себе представить очень конкретную и очень специфическую тему «Отчетность в SOC» на каком-нибудь Инфофоруме или InfoSecurity Russia? Я — нет, потому что оба эти мероприятия «обо всем сразу и ни о чем конкретно». У них размытая программа, которая хочет охватить сразу всё и в итоге все темы рассматриваются по верхам (хотя кому-то и этого достаточно). У SOC-Форума четкая специализация (если не рассматривать регулярное смещение тем SOC и SIEM), что и позволяет погружаться в совершенно различные темы, связанные с центрами мониторинга — визуализация, threat hunting, расследование инцидентов, приоритезация событий, измерение эффективности и другие. В России таких фокусных мероприятий не так уж и много — Рус-Крипто, PKI-Форум, AntiFraud Russia, ИБ АСУ ТП КВО... Вот, пожалуй, и все.



Но вернемся к SOC-Форуму. Не буду оценивать организацию, которая была на высоте, выросшую выставочную часть, возможность для кулуарных обсуждений — все это было хорошо. Опишу пленарную часть, которую мне довелось модерировать и в которой я сконцентрировался на дискуссии с двумя регуляторами — ФСТЭК и ФСБ, тремя аутсорсинговыми СОСами, представленными Игорем Ляпуновым (Solar Security), Евгением Климовым (Информзащита), Романом

Кобцевым (Перспективный мониторинг), и представителем заказчика — Алексеем Плешковым из Газпромбанка.

НЕЗРЕЛОСТЬ ОТЕЧЕСТВЕННОГО РЫНКА СОС

Первый мой вопрос касался такой материи как время. Почему тема СОСов стала активно развиваться именно сейчас? Это происки отдельной компании, которая продвигает свои услуги? Или есть другие причины, приведшие к та-

кой активности? По версии Алексея Новикова из 8-го Центра ФСБ и Дмитрия Шевцова из ФСТЭК, задача непрерывного мониторинга стала важной сейчас по причине развития технологий ИТ, развития технологий нападения, а также усиления требований по скорости реакции на современные угрозы. Именно поэтому помимо темы СОСов стала именно сейчас развиваться ГосСОПКА, стали появляться требования по обязательному уведомлению госорганов об инцидентах, ФСТЭК меняет подходы

к аттестации от дискретных трехлетних периодов к непрерывной оценке защищенности.

При этом аутсорсинговые СОСи тоже развиваются не на пустом месте — возросла зрелость тех, кому не хватает своих систем мониторинга, и они хотят повысить эффективность процесса обнаружения и отражения угроз. Об этом говорили и Игорь Ляпунов, и Евгений Климов. А Роман Кобцев привел интересную аналогию с морковным соком, который в семьях пьют по разным причинам. Кто-то потому что вкусно, кто-то — потому что полезно, а кто-то — потому что мама заставляет. Так и СОСи. Кого-то заставляет ГосСОПКА и FinCERT, а кто-то реально созрел до выделения этой задачи в отдельный процесс, который и можно было бы назвать СОС. Хотя и ответ «так звезды сошлись» тоже был упомянут среди причин возросшей активности темы СОС-Форума 2.0.

Также мне был интересен портрет типичного заказчика аутсорсингового СОС (включая ГосСОПКУ). У Solar Security это преимущественно банки, хотя Игорь Ляпунов неоднократно упомянул и зрелость заказчиков, которые отдают свою «святая святых» на аутсорсинг. У Информзащиты и Перспективного мониторинга клиентами являются преимущественно свои же клиенты, которые уже пользуются услугами и продуктами этих (а также материнской в случае с Перспективным мониторингом) компаний. К ГосСОПКЕ подключены сейчас 10 крупных органов власти, а в перспективе должны подключиться все федеральные органы исполнительной власти, а также, возможно, и госкорпорации. В частности, Росатом и Ростех со своим КЦОПЛ, уже проявили интерес к интеграции своих центров мониторинга с ГосСОПКОЙ; по приме-



Алексей Плешков (Газпромбанк) и Алексей Новиков (ФСБ России)

ру уже подключившегося FinCERT Банка России. Малого и среднего бизнеса нет ни у кого среди клиентов и пока непонятно, как это сделать. Solar Security пока не видит среди своих клиентов малый бизнес, а Перспективный мониторинг считает, что малый бизнес должен обслуживаться у операторов связи, которые таким образом могут расширить пакет своих услуг и поднять свой ARPU. Муниципальные предприятия пока не попадают в прицел ГосСОПКИ, но в перспективе их можно будет подключать через региональные центры ГосСОПКИ, которые сейчас в процессе строительства.

Интересной, но так и незавершенной мне показалась дискуссия об обмене информации между СОСами. Пока каждый работает только на себя и не очень готов делиться своими наработками с другими игроками рынка, по сути, конкурентами. Об этом говорил и Алексей Плешков из Газпромбанка, который поделился своим опытом и посветовал на то, что пока у нас отсутствует формализованный стандарт обмена информацией

об угрозах, что усложняет автоматизацию подключения различных источников Threat Intelligence. Хотя в мире есть и STIX, и TAXII, и CIF, и многие другие стандарты, есть подозрение, что Россия пойдет опять своим путем и будет изобретать велосипед. Об этом косвенно говорит и законопроект о безопасности критических инфраструктур, в котором весь обмен информации требуется осуществлять через Национальный координационный центр по компьютерным инцидентам по разрабатываемому сейчас регламенту.

Есть проблемы и с бесплатными услугами у наших СОСов. Пока этот рынок находится в самом зачатке и никаких бесплатных услуг (например, фидов с индикаторами компрометации) отечественные игроки не предоставляют. Игорь Ляпунов упомянул о том, что у Solar Security есть какие-то услуги за нулевую стоимость, но какие, так и не сказал. Остальные игроки на вопрос о том, что у них есть для компаний, которые хотят знать об угрозах, но не готовы платить за услуги СОС, скромно промолчали. Идея с центрами, аналогичными западным ISAC, которые часть информацию раздают бесплатно, пока у нас не реализована, что обусловлено, на мой взгляд, незрелостью самого рынка и низкой конкуренцией. Те же Информзащита и «Перспективный мониторинг» ориентированы на работу со своими клиентами и пока не видят перспектив (или не имеют ресурсов) в работе на широкую публику.

ПОЧЕМУ ТЕМА СОСОВ СТАЛА АКТИВНО РАЗВИВАТЬСЯ ИМЕННО СЕЙЧАС? ЭТО ПРОИСКИ ОТДЕЛЬНОЙ КОМПАНИИ, КОТОРАЯ ПРОДВИГАЕТ СВОИ УСЛУГИ? ИЛИ ЕСТЬ ДРУГИЕ ПРИЧИНЫ, ПРИВЕДШИЕ К ТАКОЙ АКТИВНОСТИ?



800

специалистов
приняли участие
в форуме в этом
году — на 300
делегатов больше,
чем в прошлом



Форум проводился при участии ФСБ России, ФСТЭК России, Банка России, организаторами выступили Закрытый клуб «SOC в России», Медиа Группа «Авангард»



Генеральным партнером выступила компания Solar Security. Официальные партнеры: Информзащита, Positive Technologies, Перспективный мониторинг, Лаборатория Касперского



SOC-Форум v.3.0 состоится

15.11.2017



Зато эта тема очень интересно свернула в сторону качества информации, обмениваемой в рамках информационного обмена, и качества подключающихся к обмену участников. По словам Игоря Ляпунова, во внешних фидах слишком много шлама и мусора и приходится очень активно их фильтровать (в отличие от данных той же ГосСОПКИ). А Евгений Климов задал риторический вопрос о том, как проверять подключающиеся к обмену компании? Не представляют ли они сами интересы злоумышленников, которые таким образом изучают то, что о них знают защитники информации? Этот непростой вопрос так и канул в Лету.

ЧЕГО Я НЕ УСЛЫШАЛ НА SOC-ФОРУМЕ?

Прошлый номер журнала, выпущенный как раз к SOC-Форуму, много материалов посвятил теме центров мониторинга ИБ, и я не буду подробно останавливаться на том, что рассказывали регуляторы на форуме и что было на его пяти потоках. Лучше напишу о том, чего я в презентациях не увидел. Лично для меня не хватило практики; и не важно с чьей стороны — заказчиков, интеграторов или поставщиков услуг SOC. Да, заказчиков было мало и причины этого я уже пытался анализировать у себя в блоге, но остальные-то, остальные! Нечего сказать или отсутствует желание делиться информацией с коллегами? Причин не знаю. Но в ито-

ге мы вновь вернулись к тому, от чего хотели отойти в прошлом году — к рассказам о том, что такое SOC и зачем он нужен, но не о том, как выстраивать те или иные процессы SOC и какие подводные камни могут быть на пути к тому или иному уровню зрелости центров мониторинга. Кстати, об уровнях зрелости не упоминал только ленивый, но вот к себе почему-то его никто не примерял, а если примерял, то «малость» завышал оценку.

Но вернемся к тому, чего я не услышал на SOC-Форуме. Так сложилось, что я имею некоторое представление о том, что рассказывают на западных, в частности, американских мероприятиях по SOC. Там есть ежегодный SOC Summit, там есть мероприятия по Threat Hunting, по Digital Forensics, по Incident Response. Поэтому, сравнение пока не в пользу нашего SOC-Форума. Ну да это понятно — бизнес-модель упомянутых западных мероприятий совсем иная. Там мероприятие платное для участников и поэтому они хотят видеть что-то конкретное и полезное, а не просто рассуждения на тему

«Что такое SOC?» или «Какой уровень зрелости должен быть у SOCа на втором году жизни?». Итак, вот мой список того, чего я не увидел на SOC-Форуме в этом году и что хотелось бы услышать в следующий раз:

♦ Больше докладов от заказчиков, которые делятся не только своими достижениями, но и своим негативным опытом, который тоже полезен. Как минимум, он позволяет не наступать на грабли последователям. А как максимум, показывает уровень зрелости компании, готовой делиться не только своими успехами. Очень мне понравился доклад от самого ЦБ об опыте работы внутреннего центра мониторинга. Нет, речь не о FinCERT, а о том, как ЦБ борется с угрозами внутри себя, в рамках своей платежной системы. Это вообще редкость, когда регулятор делится опытом собственной защиты. На моей памяти это вообще первый публичный случай. Мы эту тему обсуждали в программном комитете еще в прошлом году, и вот первый результат, который вышел не комом. У ФСБ тоже есть СОПКА (а не только ГосСОПКА) и было бы интересно (хотя я понимаю, что это малореально) послушать об их опыте самозащиты.

♦ Не хватало реальных кейсов поимки кого-либо или чего-либо. Большинство докладов фокусировалось на том, что такое SOC, какие функции он решает, какие процессы в нем есть и т.п. Но есть ли какая-то польза от него? Помог ли он решить те задачи, для которых его создавали. Даже если дистанцироваться от темы эффективности, которой был посвящен отдельный поток, было бы интересно посмотреть примеры обнаружения АРТ, поимки инсайдера и т.п. Такой доклад был только у JSOC и то, потому что у них, как у генеральных спонсоров, было целых три доклада. А если бы не было трех докладов? Выбрали бы рекламу себя или обмен опытом?

ОБ УРОВНЯХ ЗРЕЛОСТИ НЕ УПОМИНАЛ ТОЛЬКО ЛЕНИВЫЙ, НО ВОТ К СЕБЕ ПОЧЕМУ-ТО ЕГО НИКТО НЕ ПРИМЕРЯЛ, А ЕСЛИ ПРИМЕРЯЛ, ТО «МАЛОСТЬ» ЗАВЫШАЛ ОЦЕНКУ



♦ Не хватало реальных кейсов оценки эффективности деятельности SOC. Кроме доклада Газпромбанка и банка «Санкт-Петербург» по сути никто так и не привел метрик оценки своей эффективности даже вскользь. И возникает классический вопрос — так стоит ли овчинка выделки? Надо ли тратить немало ресурсов на создание того, что сложно оценить в конкретных показателях? Понятно, что тема эта непростая, но все-таки. Сюда же относится и демонстрация показателей TTD/TTC/TTR (Time-to-Detect/Time-to-Contain/Time-to-Response). Эти показатели звучали на SOC-Форуме только один раз — у меня в презентации в качестве примера метрик оценки эффективности SOC. У той же Информзащиты и JSOC в презентациях говорилось о времени реакции (это TTD, TTC или TTR?). При этом были указаны какие-то запредельные показатели в «15 минут» у Информзащиты и «10 минут» у JSOC (у них еще упоминались «30 минут» как время противодействия). Фантастические показатели, если честно. У того же Cyberbit в презентации были показаны более реальные значения — 80% инцидентов закрываются в течении 6 часов. И то, это «средняя температура по больнице». Правильнее было бы показывать диаграмму распределения времени обнаружения разных инцидентов. Например, в Cisco большая часть инцидентов детектируется (TTD) за 3–4 часа; на втором месте показатель

в 0–1 часа на обнаружение, затем идут 2–3 часа, 1–2 часа и т.д. С точки зрения реагирования (TTC) также время распределяется по шкале от 0–1 часа до 72 часа и более.

♦ Про финансовую оценку эффективности и говорить не приходится. Тема не звучала в принципе. Правда, справедливости ради, надо признать, что и на западных мероприятиях она мало звучит. Как и тема обоснования руководству необходимости SOC. Сложно пока многим компаниям показать связь бизнеса и своих активностей по информационной безопасности.

♦ Не хватало рассмотрения таких важнейших тем, как визуализация (об этом упомянул только «Эшелон», но на примере своего решения) и подготовка отчетов (об этом говорил НТЦ «Вулкан», но опять же на примере своего продукта). А хотелось бы услышать чуть больше советов о том, какие формы визуализации и для каких инцидентов подходят, какие отчеты и для каких целевых аудиторий нужны? От этого очень многое зависит в том, как будет воспринимать руководство построенный SOC.

♦ С технической точки зрения практически полностью отсутствовали рассказы о Threat Hunting, расследовании инцидентов, реагировании на них, приоритезации событий, применении современных методов анализа данных — машинном обучении (кроме доклада «Открытых технологий»), нейросетях

и т.п. А ведь именно эти сервисы/процессы отличают SOC от банального применения SIEM.

♦ Ну и конечно была упущена тема персонала для SOC, а точнее тех знаний и компетенций, которыми должен обладать специалист SOC (например, аналитик). Вкратце об этом говорил представитель моей альма-матер (МИРЭА), рассказав о том, как они готовят специалистов для ГосСОПКА. Но этого явно было недостаточно и не каждый готов пойти вновь на институтскую скамью, чтобы получать нужные знания.

В заключение хочу отметить, что тема мониторинга информационной безопасности сейчас находится на коне, и в условиях растущих числа и сложности атак ее важность будет только возрастать. Многие компании будут вынуждены задуматься о том, как объединить разрозненные средства защиты информации в единый центр сбора событий ИБ и реагирования на них. Поэтому у SOC-Форума очень хорошие перспективы собрать вокруг себя целое сообщество специалистов, которым интересны не только, и не столько, нормативные акты и рассказы о современных угрозах, сколько обсуждение реальных кейсов обнаружения нарушителей, компетенция которых растет зачастую быстрее специалистов по безопасности.



Андрей АКИНИН
генеральный директор
компании Вэб Контрол

НОВЫЙ МИР — НОВЫЕ ПОДХОДЫ?

ЧУДЕСА СЛУЧАЮТСЯ, НО ОРИЕНТИРОВАТЬСЯ НУЖНО
НА РЕАЛЬНОСТЬ: УСТОЙЧИВОСТЬ БИЗНЕСА И ЗАЩИТУ
КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ

Тема обеспечения информационной безопасности сейчас более чем актуальна, сказано много слов про различные средства и методы защиты информации. Еще больше в последнее время говорится о необходимости повышения профессионального уровня специалистов ИБ, создании SOC и подбора команд профессионалов, способных решать проблемы любой степени сложности. Очевидно, ландшафт ИТ стремительно эволюционирует, что требует изменения не только инструментов и методов, а зачастую подходов к Информационной безопасности в целом. Мы живем в постпревентивном мире — инциденты безопасности из потенциальной угрозы давно стали привычным фактором в бизнесе. Многие эксперты формируют новую парадигму безопасности информационной системы (далее ИС), которая выдвигает на первое место надежность и безопасность функционирования — функциональную безопасность ИС. В последнее время вместо защиты информации все чаще говорят о киберустойчивости, понимая под этим обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры в условиях постоянно присутствующего риска, а также в ходе кибератаки. Все более актуальной становится задача снижения ущерба в условиях принятия рисков безопасности взамен ранее при-

оритетной задачи устранения этих рисков. Стремление во чтобы то ни стало устранить риски приводит к снижению гибкости системы, что в свою очередь приводит к потере позиций в конкурентной среде.

Говоря об информационной безопасности, мы, как правило, говорим о защите собственно информации, защите информационных систем, защите физической инфраструктуры, разграничении доступа и контроле привилегий, но очень редко мы вспоминаем об устойчивости бизнеса и защите конечных пользователей. Вспоминая о конечных пользователях, многие эксперты ИБ непроизвольно «тянутся к пистолету». Основные темы — «как поймать нарушителя», «кого надо рассматривать как потенциальную угрозу», «как собрать доказательную базу для предъявления обвинений». Похожие вопросы возникают при взаимодействии с бизнесом — «как вынудить бизнес жить по нашим правилам», «как обосновать затраты на безопасность и откусить часть ИТ бюджета»? Давайте вместе подумаем, насколько такой подход оправдан и/или эффективен. Мне не хотелось бы выступать в роли «Капитана-очевидности», но попробуем начать сначала.

ИТ ИЗ ИНСТРУМЕНТА ОБЕСПЕЧЕНИЯ БИЗНЕСА ПРЕВРАЩАЕТСЯ В ЕГО ПРЕДМЕТ

Еще несколько лет назад информационные технологии расценивались как

средства облегчения документооборота и ускорения бизнес-процессов. ИТ-системы использовались прежде всего, как средства автоматизации бизнес-процессов внутри компаний. В таком ключе для обеспечения информационной безопасности достаточно было выстроить эффективный периметр безопасности, сегрегировать информационные потоки внутри компании и использование общедоступной информации из внешних сетей.

Но жизнь берет свое: интернет-технологии проникают в бизнес-процессы и становятся не только источником информации, но и средой/инструментом ведения бизнеса, клиентские приложения уходят в Интернет. Где провести водораздел? Как разделить информационные потоки? Где информация, а где приложения? Естественное желание человека, отвечающего в этой ситуации за безопасность, отключить всем доступ к Интернету, чтобы исключить потенциальную угрозу компрометации систем или хотя бы изолировать ее на специально выделенном для этого компьютере, огражденном от внутренней сети. В этих условиях и возникла необходимость изменения подходов к рискам и угрозам информационной безопасности.

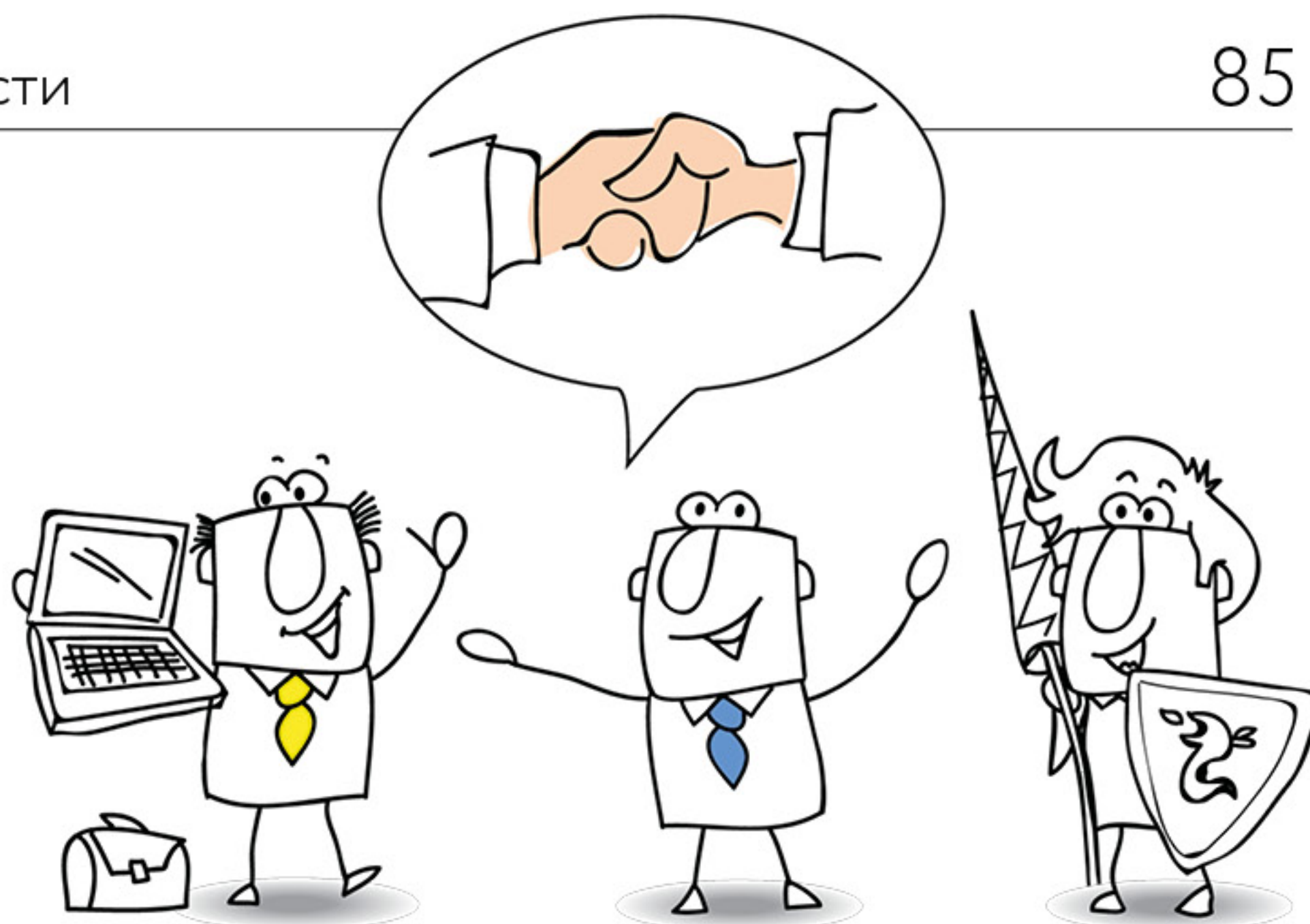
ЭВОЛЮЦИЯ БИЗНЕСА = ЭВОЛЮЦИЯ ПОДХОДОВ

В современном мире бизнес вышел в глобальную сеть и его уже не вер-

нешь назад за периметр безопасности. Все больше сотрудников коммерческих компаний, в том числе и финансово-кредитных организаций, становятся мобильными, работают за пределами офиса и используют Интернет для ведения бизнеса. В таких условиях практически невозможно исключить связанные с этим риски, поэтому приходится их принять, а проектирование информационных систем выполнять с учетом требований обеспечения их киберустойчивости.

Классическая модель защиты информации нацелена на поиск и обезвреживание нарушителя периметра безопасности. В условиях размывания и даже исчезновения периметра становится все сложнее найти точку применения инструментов безопасности. Конечные пользователи ИТ-систем и другие субъекты бизнес-коммуникаций оказываются на линии огня. В этих условиях многократно возрастает уязвимость ИТ системы. Кроме того, современный киберпреступник обладает огромными ресурсами, которым противостоят не хорошо развитая периметровая система информационной безопасности, а персональные средства защиты конечного пользователя в сочетании с «человеческим фактором». **Это не война, на ней нет фронтов. Это больше похоже на террористическую атаку.** Эта атака не всегда направлена на информацию, целью может стать вычислительная мощность или просто создание плацдарма для новой атаки. Сейчас уже не стоит вопрос, будет ли скомпрометирована сеть организации, вопрос звучит по-другому: что делать, когда это произойдет? Последние годы мы активно работаем с внутренними угрозами и опыт показывает, что многие компании уже смирились с наличием вирусов и элементов ботнета на компьютерах своих пользователей. Сейчас актуален вопрос, как снизить потенциальный ущерб при разумных затратах. Например, работа системы смены паролей администраторских и технологических учетных записей купирует угрозу компрометации привилегий, и чем чаще происходит эта смена, тем ниже риск прямого ущерба.

В эпоху Интернет, когда бизнес меняется со скоростью мысли, классические



ОЧЕВИДНО, ЧТО НЕВОЗМОЖНО СОЗДАТЬ НАДЕЖНУЮ ИТ-СИСТЕМУ БЕЗ ТЕСНОГО СОТРУДНИЧЕСТВА ИТ И ИБ

политики и правила безопасности становятся все менее и менее эффективными. То, что еще вчера можно было просто запретить без последствий, сегодня ведет к потере конкурентных преимуществ компании. В современном мире выигрывает тот, кто делает свой бизнес более удобным и простым для своих клиентов. В этих условиях классический подход «мистера Нельзя» перестает работать, потому что, если нельзя, но это позволяет зарабатывать деньги, то можно.

Так что же делать? Нужно изменить подход: думать, как сделать то, что приносит деньги бизнесу если не безопасным, то как минимум приемлемым. Пора позабыть про противодействие ИБ и ИТ, очевидно, что невозможно создать надежную ИТ-систему без обеспечения необходимых мер безопасности. ИТ-службы приняли это как данность, и **специалисту ИБ нужно помочь им сделать бизнес-процессы максимально безопасными, при этом не нарушая их привычный ход.**

Давайте искать друг в друге союзников. Кстати, большинство систем противодействия внутренним угрозам может быть полезно и для ИТ-специалистов. Информация, собираемая системами поведенческого анализа, может быть использована для анализа производительности и эффективности ИТ инфраструктуры, а записи систем регистрации действий пользовате-

лей помочь службе поддержки понять, что она делает не так. Таким образом возрастает значимость уровня информационной грамотности не только сотрудников ИТ и ИБ, но и рядовых пользователей ИС.

ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ

Учитывая смещение вектора угроз в сторону пользователя и устройств, с которыми он ежеминутно имеет дело, приходится менять подход к конечному пользователю с точки зрения ИБ. Вместе с поиском и наказанием нарушителя на первое место выходит **превращение конечного пользователя в союзника и активного участника в процессе обеспечения киберустойчивости компании.**

Как говорилось ранее, наравне с целенаправленными атаками, с которыми уже привыкли бороться, значительное беспокойство для бизнеса представляет безадресная веерная атака на различные элементы инфраструктуры и конечных пользователей. Современный киберпреступник во многих случаях начинает свою атаку задолго до того, как у него появилась цель и предмет атаки. Зачастую он работает впрок, проводя атаку «по площадям» с целью обнаружить «слабое место» и получить

ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ ЗНАЧИТЕЛЬНО СНИЖАЕТ КОЛИЧЕСТВО НЕСУЩЕСТВЕННЫХ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

плацдарм для будущей атаки. Этот тип атаки, как правило, незамысловат и достаточно просто отбивается автоматизированными средствами ИБ, если они работают и содержат актуальные базы угроз, но довольно часто этим «слабым местом» оказывается случайно не обновившийся антивирус или неработающие автоматизированные средства безопасности на компьютере пользователя, а также поведение самого человека.

Но злоумышленник может не использовать образовавшийся плацдарм сразу, а приберечь его до подходящего момента, и подобные «дыры», как правило, очень сложно обнаружить и, самое главное, абсолютно не разумно использовать для их поиска значительные ресурсы, потому что они могут никогда и не повлечь за собой никакого ущерба, и ресурсы будут израсходованы впустую.

Для борьбы с этим типом угроз необходимо прививать всем сотрудникам компании правила цифровой гигиены. Каждый сотрудник компании должен четко понимать и выполнять общие правила безопасного поведения при работе с информацией. К сожалению, при создании систем информационной безопасности вопрос осведомленности конечных пользователей стоит далеко не на первом месте. В то время, как в обычной жизни мы постоянно встречаемся с средствами информирования об опасности — «Не влезай, убьет!», «Осторожно, злая собака!», «Внимание, торговый зал снимает скрытая камера!» и прочие, в ИБ мы сидим в засаде и стараемся поймать нарушителя! Иначе как нам доказать свою необходимость и эффективность?!

Коллеги, как и в повседневной жизни, гораздо легче поймать нечаянного нарушителя, чем реального злоумышленника, причиняющего значительный ущерб. Повышение осведомленности конечных пользователей значительно снижает количество несущественных

инцидентов информационной безопасности, борьба с которыми может съесть значительную долю ресурсов систем информационной безопасности. Это так же позволяет высвободить ресурсы для борьбы с реальным ущербом. Что нужно сделать для этого?

- ◆ Разработать четкий и понятный свод правил информационной гигиены, как общих, так и персональных, связанных с функциональными ролями сотрудников;

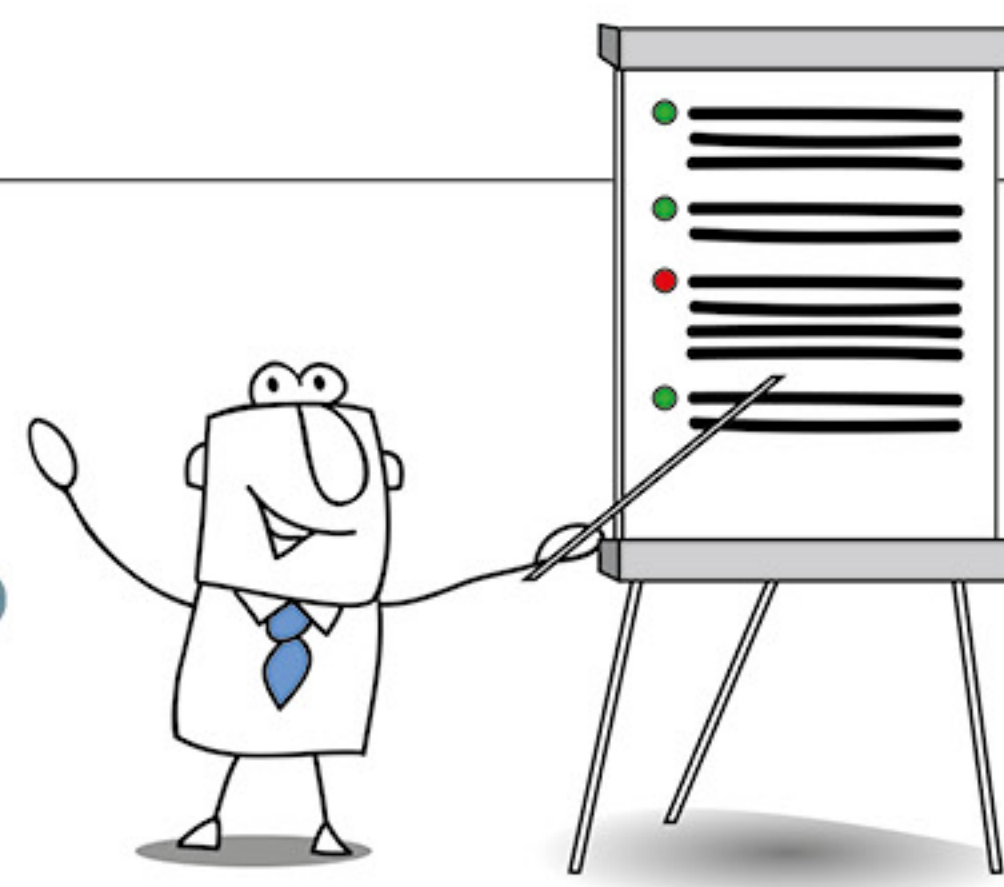
- ◆ Организовать обучение сотрудников этим правилам при приеме на работу и переводе на другую должность;

- ◆ Проводить регулярный инспекционный контроль знаний правил и следования этим правилам;

- ◆ Регулярно информировать сотрудников компании об актуальных угрозах ИБ и необходимых мерах осмотрительности в этих условиях.

Возможно, эти меры выглядят несколько архаично, но без союзников среди «простых граждан» терроризм не победить. Каждый сотрудник компании должен знать, что он должен и не должен делать, чтобы не стать мишенью злоумышленника как внешне, так и внутреннего. Это не только затруднит жизнь киберпреступникам, но и облегчит работу ИБ. Кроме этого, хорошо информированный сотрудник раньше обнаружит подозрительную активность и привлечет к ней внимание ИБ, повысив качество внутреннего контроля в организации. В такой ситуации нерадивый сотрудник трижды подумает прежде чем нарушить правила. Если его поведение будет выбиваться из общей поведенческой модели, это довольно скоро будет обнаружено системами поведенческого анализа, контролирующими внутреннюю безопасность организации.

Таким образом, необходимо формировать в компании профиль хорошего поведения. Как это сделать?



НЕ ПОЗВОЛИМ ХОРОШИМ ЛЮДЯМ ДЕЛАТЬ ПЛОХИЕ ВЕЩИ

Основной подход в обеспечении «хорошего поведения» сотрудников — это формирование безопасного профиля поведения, следуя которому выполнение функциональных обязанностей сотрудника будет максимально удобно, просто и безопасно. Можно выстроить всеобъемлющую систему запретов и ограничений, обеспечивающую максимальную безопасность, но, если это будет существенно мешать сотруднику исполнять свои обязанности, он будет пытаться ее обойти.

Эксперты в области безопасности очень много пишут и говорят о злоумышленниках и преступлениях, и это понятно. Борьба с плохими людьми — это то, за что нам платят деньги. Но давайте не будем забывать, что большинство людей все-таки хорошие, и они, как правило, приносят деньги компании. Наша задача, прежде всего, обеспечить их безопасность и функциональность.

В обычной жизни мы защищаем опасные участки перилами и оградами, развешиваем таблички, наконец, ставим охранников, чтобы люди не причинили вред себе и другим. То же самое нужно делать и в информационном пространстве, формируя для пользователей ИТ-систем оптимальные траектории цифрового поведения. В рамках данной статьи невозможно достаточно подробно раскрыть этот подход, остановлюсь на основных моментах.

Вводя какие-то ограничения, обусловленные требованиями безопасности, мы в той или иной степени наживаем себе врага. Потому, вводя какие-то ограничения, мы обязательно должны задуматься о возможных компенсационных мерах. Например, при введении требований к сложности и периодичности смены паролей, мы должны

подумать, как пользователь будет его придумывать и запоминать. Вводя ограничения на доступ к определенным Интернет-ресурсам, мы должны убедиться, что это не повлияет на доступ к остальным ресурсам. Правила и нормы поведения наиболее эффективны в том случае, если следование им является наиболее удобным или простым вариантом поведения. При создании безопасных ИТ-систем нужно не только создавать барьеры на пути «плохого» поведения, но и указывать на правильный путь. Это формирует ту оптимальную траекторию поведения, выбрав которую, пользователи будут находиться в большей безопасности с минимальными усилиями. Таким образом мы уберем хороших людей от плохих действий.

ДИФФЕРЕНЦИРОВАННЫЙ ПОДХОД К ПОЛЬЗОВАТЕЛЮ — ЗАЛОГ УСПЕХА

Однако не стоит забывать о том, что разные пользователи в организации требуют разного подхода с точки зрения обеспечения безопасности. Например, для контроля привилегированных пользователей недостаточно простой цифровой гигиены. Администраторы систем, как правило, могут обойти контрольные механизмы, то есть они постоянно находятся под искушением нарушить правила пусть даже и с благими намерениями. В этом случае необходимо выстраивать бизнес-процессы и инструменты контроля безопасности таким образом, чтобы их нарушение делалось более трудоемким, а еще лучше невозможным. До 45 % внутренних мошенничеств совершаются сотрудниками, которые наделены привилегией для совершения действий в обход контрольных мер. Прежде всего это проис-

ходит потому, что контрольные меры, как правило, затрудняют или замедляют действия пользователей, особенно в критической ситуации. Поэтому, внедряя контрольные системы, очень важно **обеспечить контролируемому пользователю минимальное влияние средств безопасности на его обычный бизнес-процесс**, а в идеале упростить его или ускорить.

Не всегда это получается, но если это удастся, то мы получаем кумулятивный эффект от внедрения мер безопасности. Мы не только делаем бизнес компании безопасней, но и получаем позитивное отношение сотрудников и руководства компании.

Другой причиной обхода привилегированными пользователями контрольных механизмов является сам факт возможности бесконтрольного использования этих привилегий. На первый взгляд звучит парадоксально, но по сути, давая пользователю эту привилегию, мы провоцируем его на нарушение. В идеале необходимо исключить

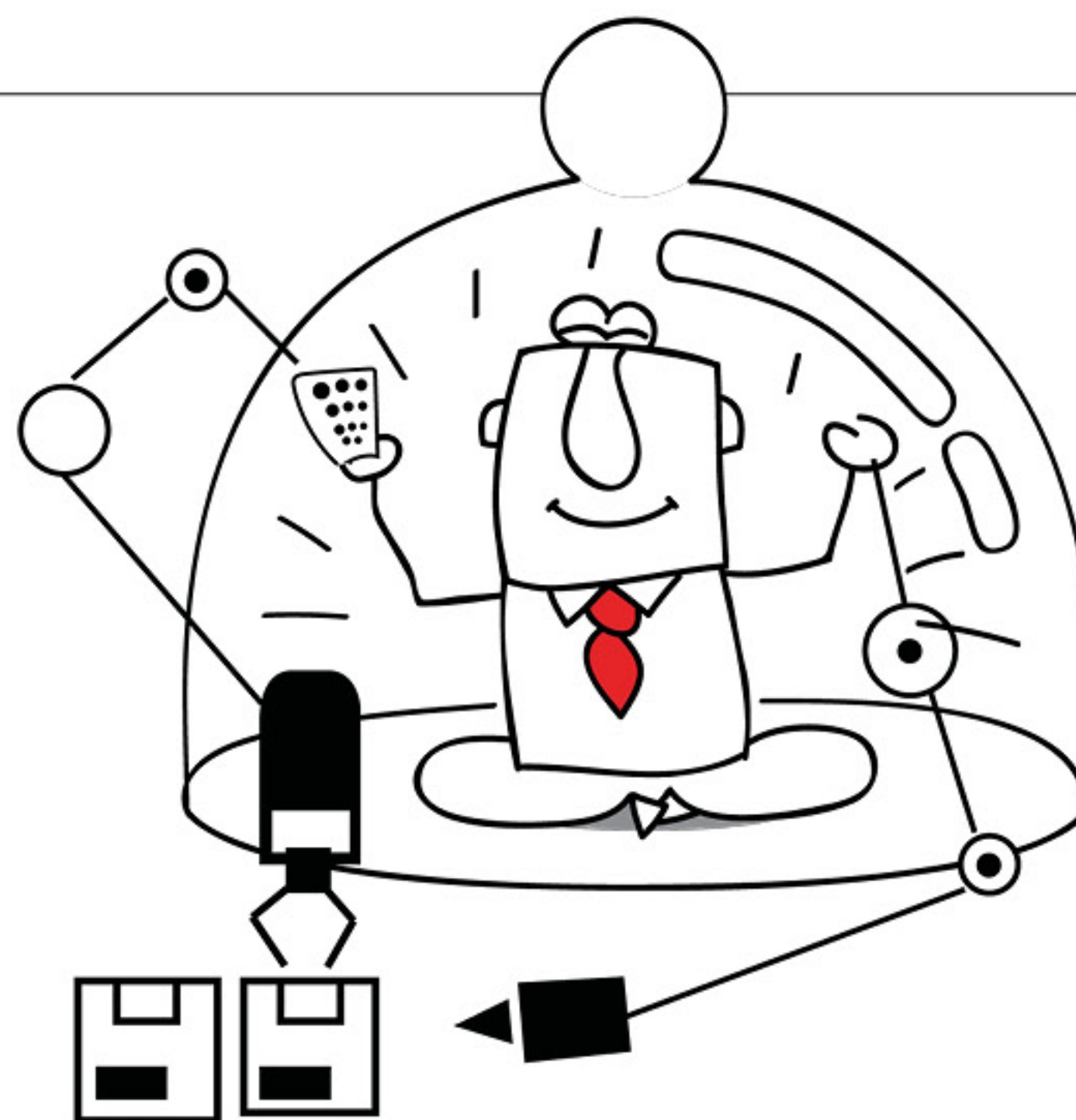
любой обход стандартных контрольных механизмов или он должен быть под особым контролем ответственного сотрудника ИБ.

Есть красивое решение этой дилеммы. Создание защищенной среды исполнения приложений, в которой пользователь может использовать положенные ему привилегии под контролем и без возможности компрометации учетных данных. Система авторизует пользователя для выполнения определенной привилегированной функции. После этого она выбирает в базе учетных данных соответствующую запись и запускает для пользователя сеанс администрирования с использованием необходимого для этого инструмента. Таким образом **пользователь никогда не получает привилегированных учетных данных и не может их использовать в обход защищенной среды**. То есть он использует привычные средства администрирования при исключении возможности их компрометации.

* * *

НЕОБХОДИМО СОЗДАНИЕ ЗАЩИЩЕННОЙ СРЕДЫ ИСПОЛНЕНИЯ ПРИЛОЖЕНИЙ, В КОТОРОЙ АДМИНИСТРАТОР МОЖЕТ ИСПОЛЬЗОВАТЬ ПОЛОЖЕННЫЕ ЕМУ ПРИВИЛЕГИИ ПОД КОНТРОЛЕМ И БЕЗ ВОЗМОЖНОСТИ КОМПРОМЕТАЦИИ УЧЕТНЫХ ДАННЫХ

Вы конечно скажете, что чудес не бывает, но мой опыт деятельности в этой области говорит о том, что это не чудо, а правильный выбор решения и схемы его внедрения. Ну и конечно же результат непосредственной вовлеченности в процесс внедрения всех заинтересованных сторон от контролируемого пользователя до владельца проекта.





«ЧТОБ БЫЛО В ТЕХ ЗЕМЛЯХ НЕ ЗНАТНО...»

ВЫШЛА В СВЕТ КНИГА,
ПОСВЯЩЕННАЯ ИСТОРИИ
КРИПТОГРАФИИ В РОССИИ

В Дипломатической академии МИД России при стечении множества именитых гостей — военных, дипломатов, историков и искусствоведов — состоялась презентация книги В.Г.Никонова и Б.В.Столпакова «Чтоб было в тех землях не знатно...».

Книга посвящена истории криптографии в России на самой ранней ее стадии — стадии освоения и внедрения тайнописи в повседневную практику работы Посольского приказа (предтечи Министерства иностранных дел) Московского государства в XVI — XVII вв.

Как единодушно признали гости презентации, книга получилась необыкновенной. Авторы — член-корреспондент Академии криптографии РФ, доктор технических наук, народный художник России Владимир Глебович Никонов и историк криптографии, кандидат физико-математических наук Борис Владимирович Столпаков — удивительным образом соединили под одной обложкой и научную монографию — жанр дотошный, кропотливый, совсем не развлекательный, и захватывающее, потрясающе интересное и безусловно полезное, чтение. Являясь представителями точных наук, исследователи со знанием дела и привлечением широкого массива исторических данных создали действительно глубокую и одновременно увлекательную книгу, которая, без сомнения, найдет своего читателя не только среди специалистов,

но и среди всех тех, кто интересуется отечественной историей.

Дело в том, что эта книга не только о криптографии. Тайнопись — вязь, литье, шифрование... в общем, криптография тут — как столбовая дорога, двигаясь по которой, вы непосредственно соприкасаетесь с разными сферами деятельности в Российском государстве XVI–XVII веков: дипломатией, математикой, историей, литературой, педагогикой...

Стоит особо отметить, что большую помощь в подготовке книги оказали Академия криптографии РФ, Дипломатическая академия МИД России, а издателем выступила Медиа Группа «Авангард».

В ходе прекрасно организованной презентации, на которой присутствовали многочисленные гости, выступили проректор Дипломатической академии Т.Н.Мозель, заведующий кафедрой Дипломатии и консульской службы С.Е.Иванов, генерал армии, доктор технических наук, действительный член Академии криптографии РФ, Российской академии инженерных наук и Международной академии связи В.Г.Матюхин, член Союза писателей России, кандидат искусствоведения Т.Б.Заболзаева, потомок А.С.Пушкина, кандидат физико-математических наук А.А.Кологривов и другие.



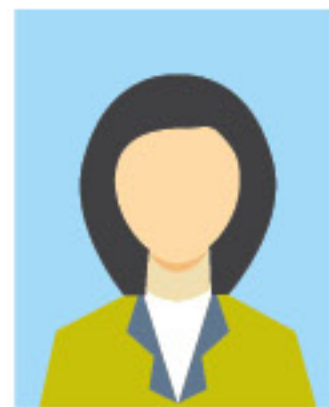
Авторы книги — Борис Столпаков и Владимир Никонов



КАДРОВАЯ СИТУАЦИЯ В ИБ 2016: РОССИЯ

АНОНС РЕЗУЛЬТАТОВ ПРОФИЛЬНОГО
СОЦИОЛОГИЧЕСКОГО ОПРОСА

*Отчет в полном объеме будет представлен
на IX Уральском форуме*



Александр БОДРИК
сертифицированный специалист
по управлению информационной
безопасностью корпоративных
и облачных ландшафтов, член
ISACA, ASIS, ACFE



На протяжении нескольких недель октября в рамках Facebook-группы «Вакансии ИБ» (CyberJobsRussia — 1500+ членов) и социальной сети А.Бодрика (2300+) был проведен опрос «Кадровая ситуация в ИБ».

Опрос был призван помочь понять кадровую ситуацию на едином рынке труда в России с точки зрения сотрудника и предоставить перспективы мобильности, компенсаций и стратегий соискателей для работодателей.

В опросе приняло участие 304 человека. Они ответили на 7 вопросов:

1. Кто Вы в индустрии информационной безопасности?
2. Какие опции предоставляет Вам работодатель в рамках компенсационного пакета?
3. Готовы ли Вы к релокации?
4. Каков размер Вашего фиксированного заработка (до вычета НДФЛ)?
5. В каком типе компании Вы работаете?
6. Ваш прогноз по размеру штата службы ИБ Вашей компании?
7. Ваша стратегия на рынке труда?

По каждому из вопросов были построены графики — как в целом, так и по четырем самым крупным группам респондентов (совокупно 78% всех респондентов):

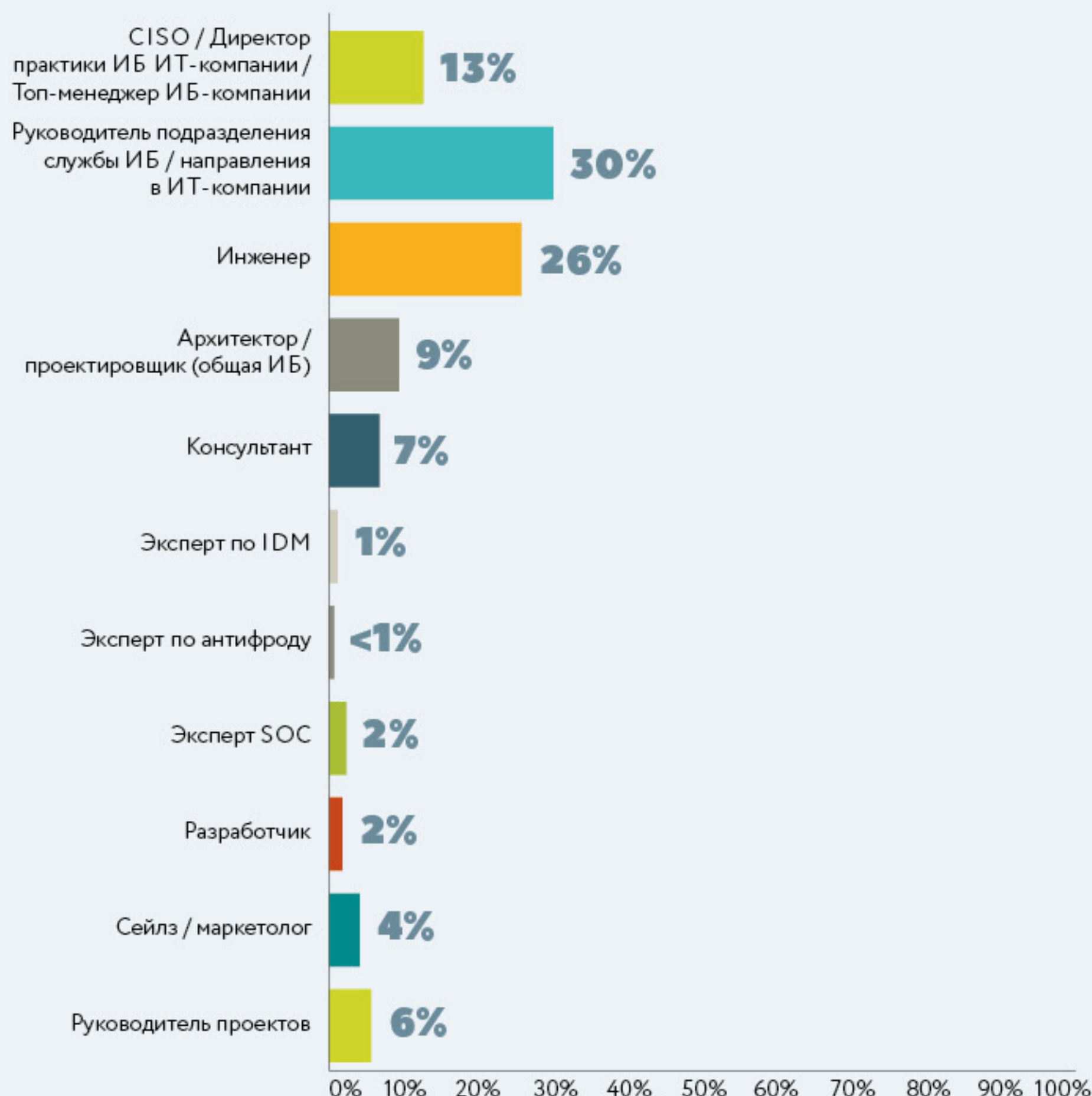
1. CISO / Директор практики ИБ ИТ-компаний / топ-менеджер ИБ-компаний (39 респондентов).
2. Руководитель подразделения службы ИБ / направления в ИТ-компаниях (90 респондентов).
3. Инженер (78 респондентов).
4. Архитектор / проектировщик (общая ИБ) (29 респондентов).

Кроме упомянутых категорий специалистов в опросе приняли участие консультанты по управлению информационной безопасностью, эксперты (IDM, SOC, антифрод), а также разработчики, руководители и специалисты коммерческого блока (маркетологи, менеджеры по продажам).

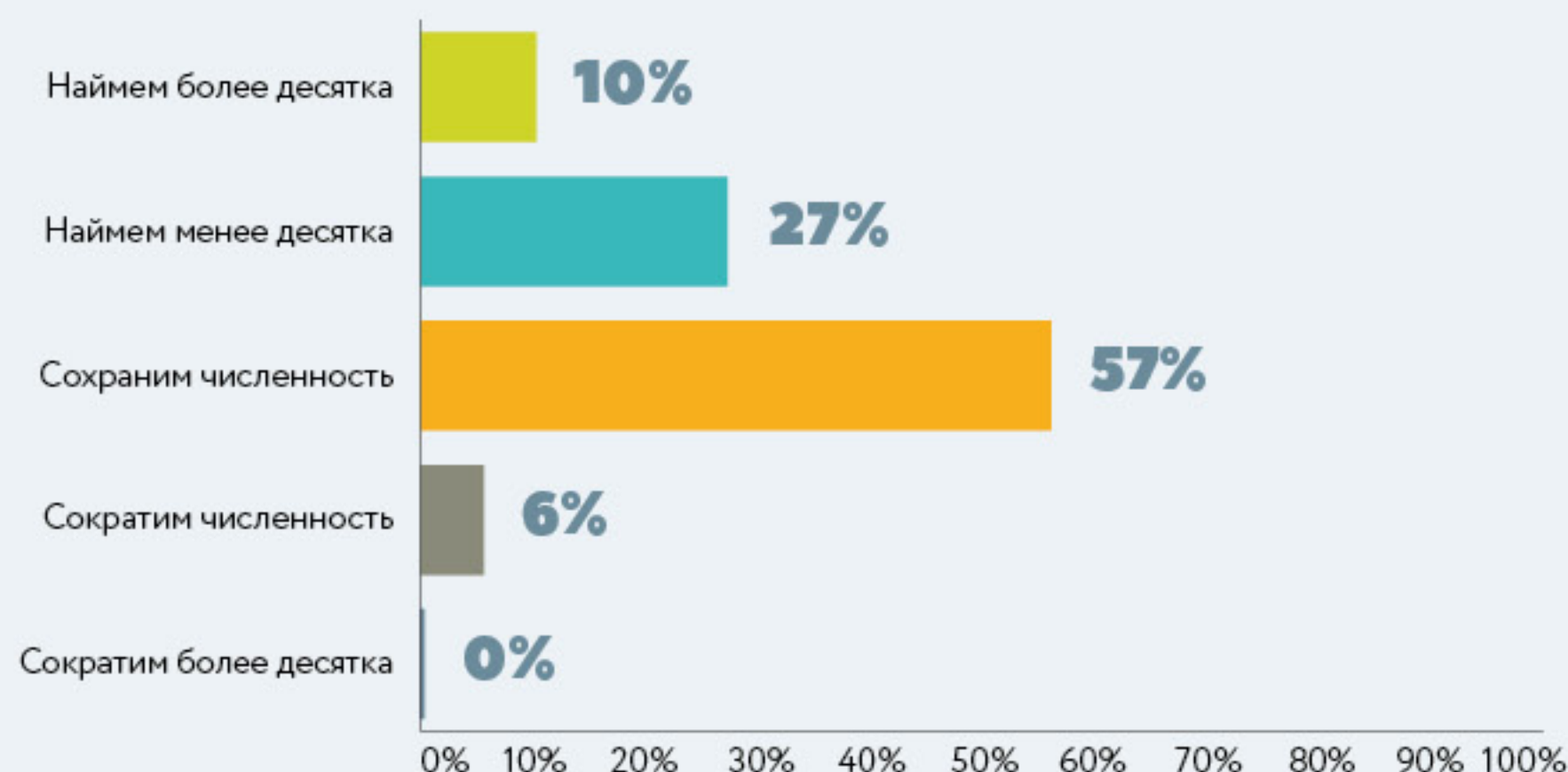
ПРЕДПРИЯТИЯ И СЛУЖБЫ ИБ: КОНТЕКСТ

Для понимания цифр по компенсациям, параметров мобильности и других необходимо знать, в какого рода ком-

РАСПРЕДЕЛЕНИЕ УЧАСТНИКОВ ОПРОСА ПО КАТЕГОРИЯМ



ПРОГНОЗ ПО РАЗМЕРУ ШТАТА СЛУЖБЫ ИБ ВАШЕЙ КОМПАНИИ



паниях работают респонденты. Ответы на этот вопрос показали более-менее равномерное распределение респондентов, ни по одному из пунктов не было набрано менее 10 и более 25 процентов:

♦ Клиент класса А (ТОП-100 РБК, банки ТОП-20, ТОП государственных структур).

♦ Клиент класса Б (есть в рейтингах, банки ТОП-50, государственные структуры, ТОП муниципальные структуры).

♦ Клиенты иных классов.

♦ ИТ-компания класса А (вендоры с капитализацией больше \$5 млрд, интеграторы с ИБ-выручкой от 1 млрд руб., крупные дистрибьюторы).

♦ ИТ-компания класса Б (вендоры с капитализацией больше \$500 млн, интеграторы с ИБ-выручкой от 300 млн руб., средние дистрибьюторы).

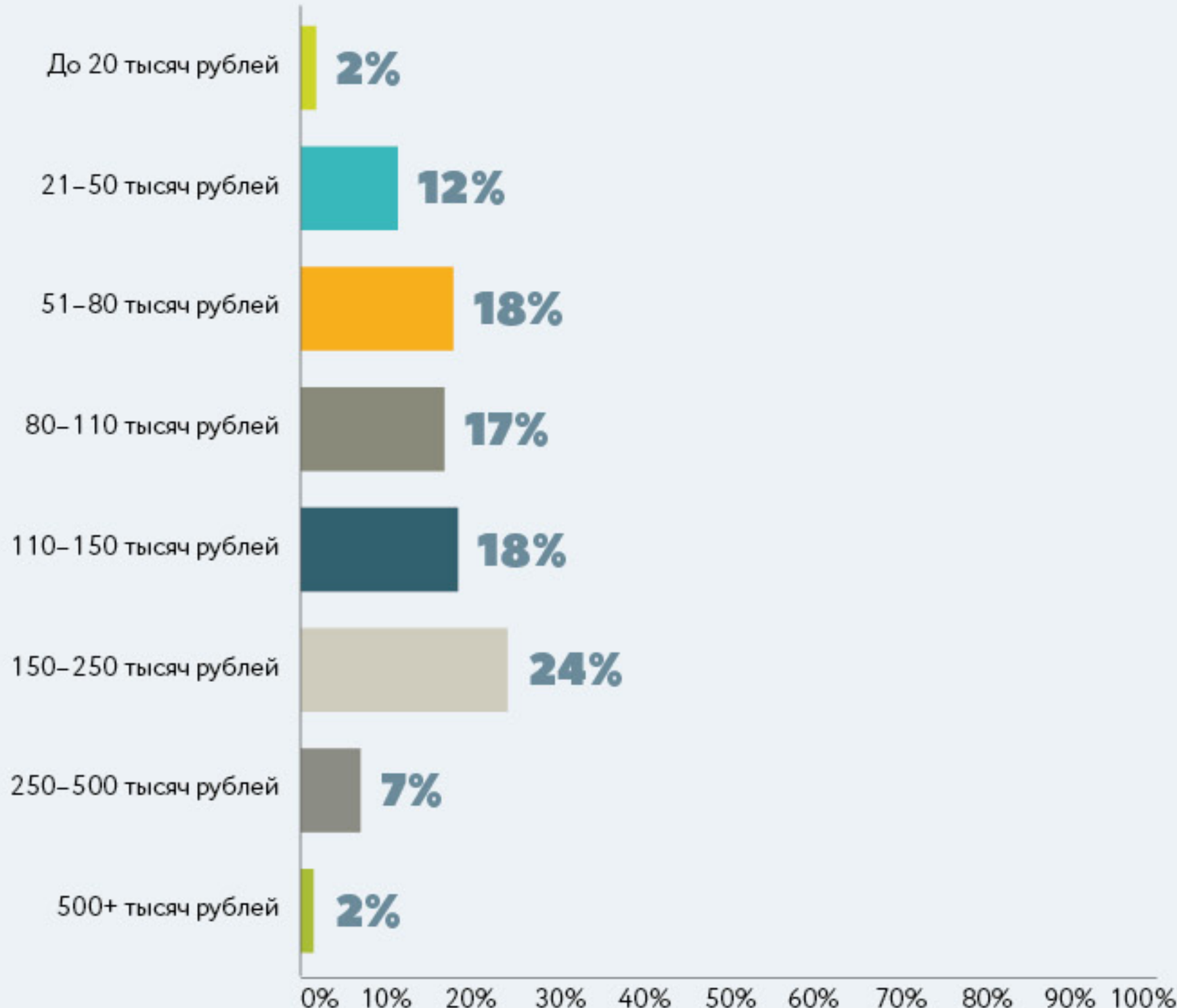
♦ ИТ-компания иных классов.

Так же критично понимание тренда спроса на специалистов — будут ли подразделения ИБ нанимать специалистов в ближайшее время.

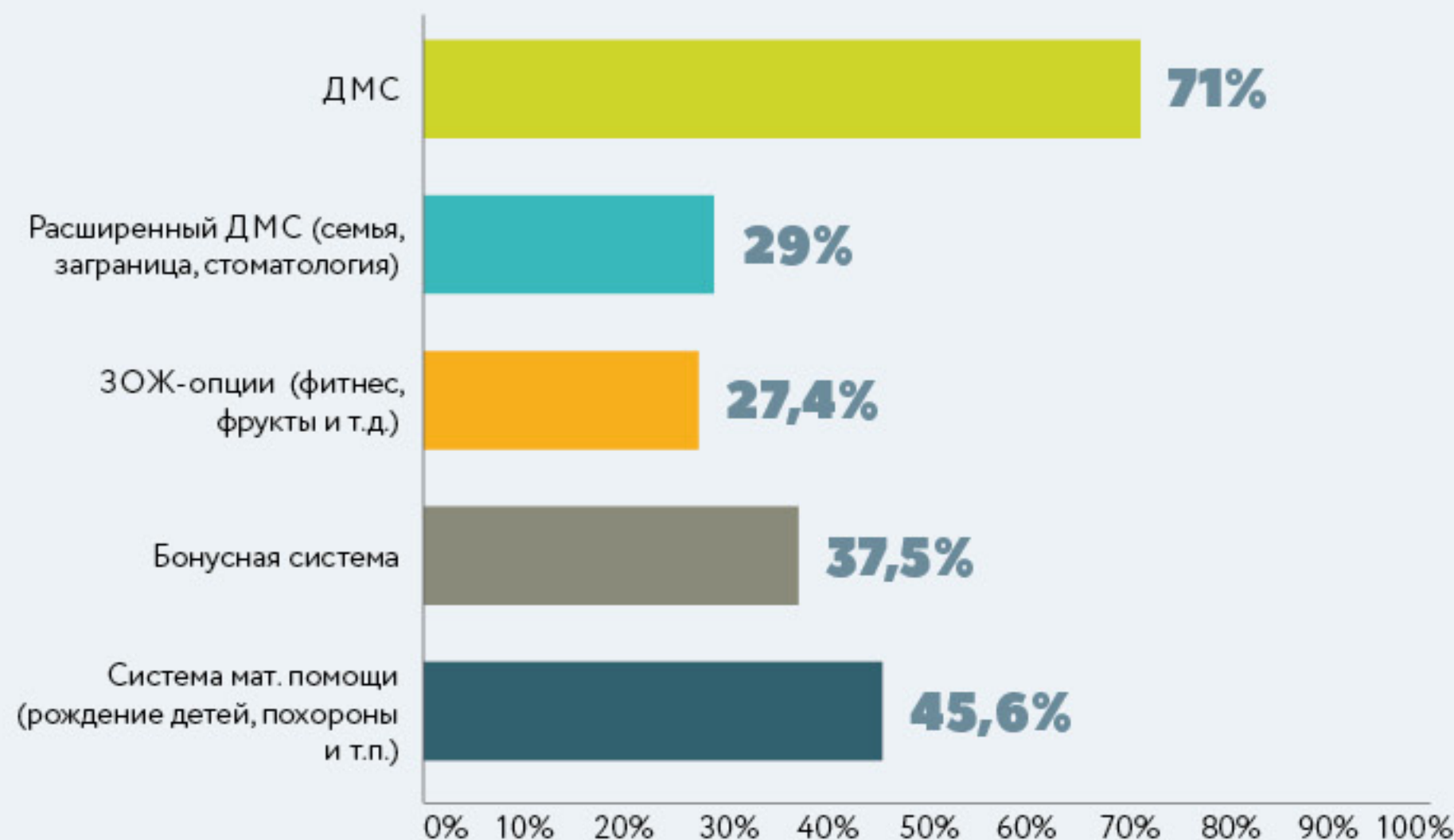
Ответ на вопрос о динамике спроса неоднозначный. С одной стороны, больше половины собирается сохранить размер штата. С другой — сокращения ожидаются небольшие, и более 30 респондентов указали, что наймут более десятка. Возможно, среди респондентов, ответивших положительно, есть представители одних и тех же организаций. С другой стороны, топовые службы ИБ страны насчитывают сотни и даже тысячи специалистов, и для них «найдем более 10» может трансформироваться в «найдем» 100, 200 или 300 специалистов только в одну организацию. С финансовой точки зрения это вполне реально (с учетом регионов это всего-то до 500 миллионов нагрузки на ФОТ в год, что для гигантов не принципиально), но найти столько качественных специалистов физически — проблема, а значит мы можем ожидать очередной виток кадровых войн, когда, как и в 2015–2016, тройка возмутителей спокойствия — Сбербанк, Solar Security, Лаборатория Касперского — изрядно попортили нервы руководителям подразделений ИБ. В 2017 такими «хулиганами» могут выступить активно нанимающие Сбербанк, Лаборатория Касперского, Информзащита, Ангара, Инфозащита, Сибинтек (аффилированная с Группой Роснефть структура). Особенно отмечу потенциал Ростелекома.

В августе 2016 Ростелеком нанял нового CIO, публично поставив ему задачу «создать внутренние центры компетенций ИТ». В корпоративной практике такая задача решается созданием внутреннего инсорсера, закрывающего 80–90% всех задач по поддержке внутренней ИТ-инфраструктуры. А информационная безопасность в инсорсинге обычно развивается именно внутри подразделений

КАКОВ РАЗМЕР ВАШЕГО ФИКСИРОВАННОГО ЗАРАБОТКА (ДО ВЫЧЕТА НДФЛ)?



КАКИЕ ОПЦИИ ПРЕДОСТАВЛЯЕТ ВАМ РАБОТОДАТЕЛЬ В РАМКАХ КОМПЕНСАЦИОННОГО ПАКЕТА?



поддержки инфраструктуры — проводится аудит организационной эффективности, выявляются пробелы в текущих компетенциях, незакрытые участки, после чего стартует активный набор сотрудников (например, так было в 2013–2014 в Росэнергоатоме), и ИБ выводится из поддержки инфраструктуры.

КОМПЕНСАЦИИ

Классическая дилемма «стакан наполовину полон или наполовину пуст» отражает ситуацию с материальной компенсацией (в первую очередь фиксированной заработной платой) практически во все времена. Этот актуальный вопрос был включен и в наш опрос.

Парадоксально, но больше половины специалистов по кибербезопасности / информационной безопасности заявили компенсацию от 110 тысяч рублей. Вероятно, стоит сделать поправку на большую распространенность сетей, через которые проводился опрос (Twitter, LinkedIn, Facebook), в двух столицах, а также на круги, в которых вращается организатор опроса (консультанты по управлению ИБ, узкоспециализированные эксперты и инженеры, CISO). Однако тенденция налицо — зарплаты в ИБ в разы больше средних по стране и по столице (Москва — 57 тысяч рублей), а почти 9% специалистов имеют приличные и по мировым меркам компенсации (от 250 тысяч рублей или порядка \$ 50 000 в год).

Но не зарплатой единой. Многие специалисты воспринимают дополнительные опции (ЗОЖ, матпомощь по особым случаям) как свидетельство заботы организации о персонале. Посмотрим, отвечают ли им взаимностью сами организации.

И среди таких опций безусловным лидером стал ДМС, второе место заняла распространённая в нефтегазовой и энергетической отраслях система материальной помощи (по случаю профессиональных дней, отпусков, рождению детей, болезней и т.п.). Расширенные ДМС и направленные на здоровье сотрудников (фитнес, фрукты и т.п.) опции пока еще редкость, но даже обычная бонусная система встречается пока только в 38% компаний.

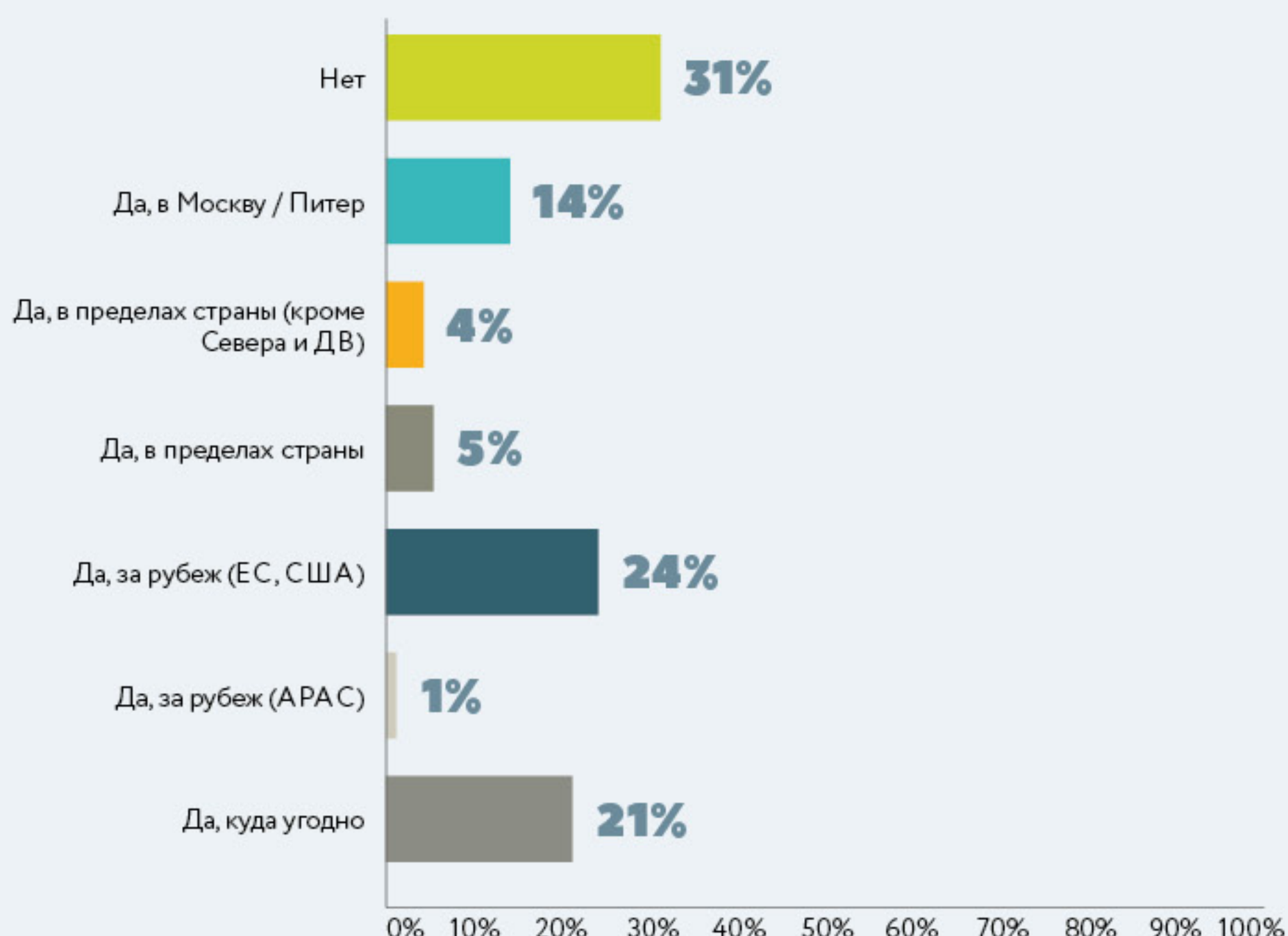
КАДРОВЫЕ СТРАТЕГИИ ПРОФЕССИОНАЛОВ

Статистика может быть занимательной, но лучше, чтобы она была полезной. Поэтому наш кадровый опрос не смог обойтись без направленного на выяснения настроений и стратегий профессионалов блока.

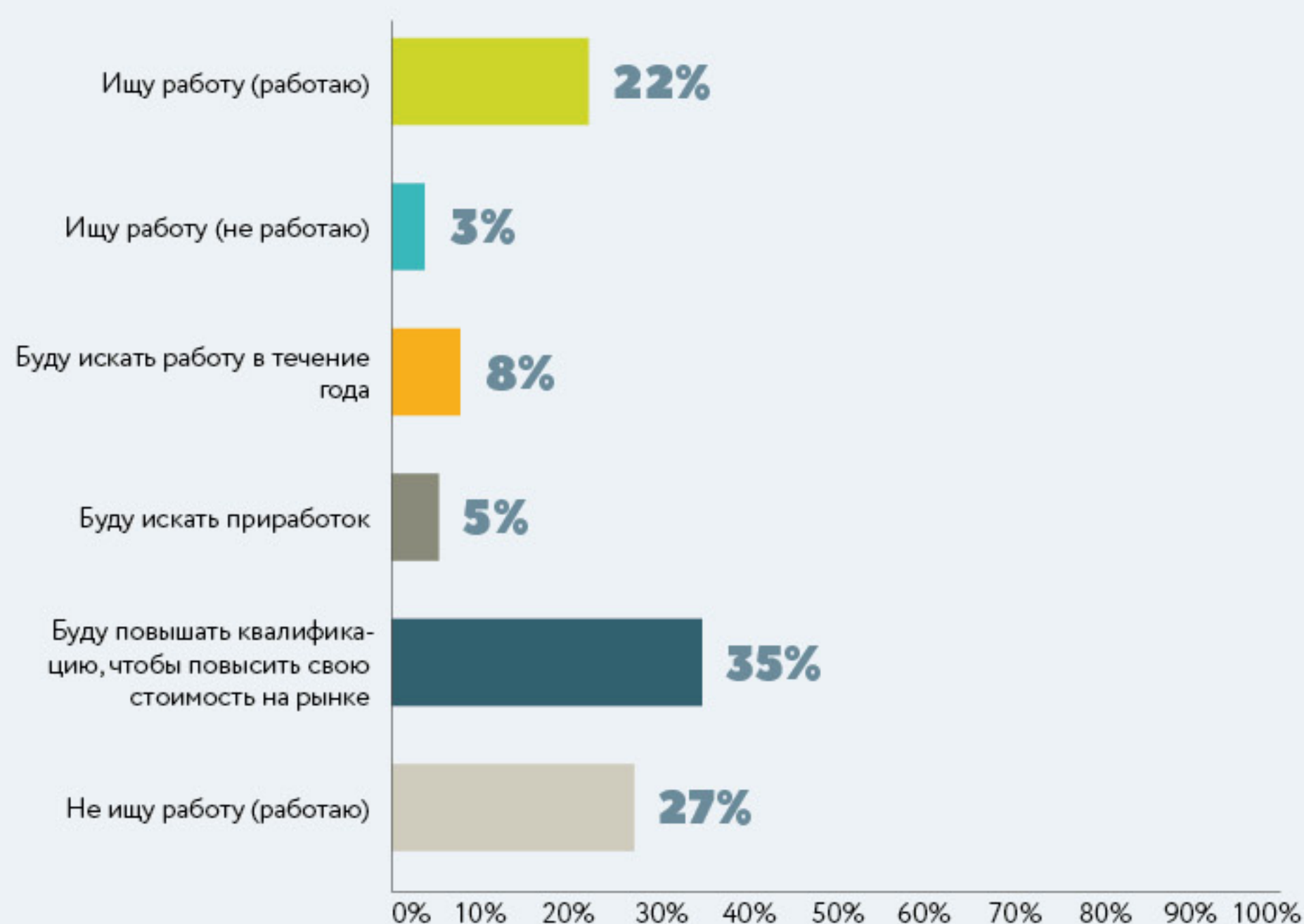
Ответ на вопрос о готовности к релокации потрясает. 7 из 10 профессионалов готовы переехать, 2 из 10 готовы мчаться без оглядки куда угодно (вероятно — лишь бы были интересные задачи и достойная оплата).

Такая высокая готовность к жизненным переменам должна как-то выражаться и в текущих планах действий. Итак, какие планы у профессионалов по информационной безопасности?

ГОТОВЫ ЛИ ВЫ К РЕЛОКАЦИИ?



ВАША СТРАТЕГИЯ НА РЫНКЕ ТРУДА?



ОТВЕТ НА ВОПРОС О ГОТОВНОСТИ К РЕЛОКАЦИИ ПОТРЕСАЕТ. 7 ИЗ 10 ПРОФЕССИОНАЛОВ ГОТОВЫ ПЕРЕЕХАТЬ, 2 ИЗ 10 ГОТОВЫ МЧАТЬСЯ БЕЗ ОГЛЯДКИ КУДА УГОДНО

Ключевой план — «что-то делать», ведь только немногим меньше 30% не собираются ничего предпринимать. Третью будет повышать квалификацию, больше пятой части сменит работу, и лишь 3 процента не работает — безработица в кибербезопасности как минимум в 2 раза меньше, чем официальная в стране.

КЛЮЧЕВЫЕ ВЫВОДЫ

Подводя итоги, сформулируем 3 ключевых вывода:

1. Рынок труда в России по-настоящему единый. Очевидно, что постоянные релокации сдерживают финансовый аспект и информационная асимметрия на кадровом рынке, но даже они по мере роста востребованности профессионалов отходят в прошлое.

2. 73 процента опрошенных ищут пути для повышения своей стоимости на кадровом рынке и / или увеличения

дохода. Это делает работодателей уязвимыми к хедхантингу со стороны западных и крупнейших федеральных корпораций, что обладают несравненно большими финансовыми ресурсами.

3. 46 процентов опрошенных готовы уехать за рубеж. Очевидно, что отток сдерживают слабое владение английским и глобальная конкуренция за рабочие места с Китаем, Индией, Украиной и Беларусью.

КЛЮЧЕВЫЕ РЕКОМЕНДАЦИИ

Увы, выводы получились пессимистичными. Однако, существует ряд простых и экономически эффективных шагов, призванных сгладить возможные кадровые риски:

1. Закрыть ненужные вакансии по информационной безопасности. Открытие вакансий «впрок» или без четко определенной бизнес-необходимости

«надувает» спрос на кадровом рынке и подогревает инфляцию компенсаций.

2. Консолидировать компетенции. Консолидация компетенций в центрах оказания услуг не только повышает производительность (по оценкам консультантов минимум на 20–30%), но и позволяет создать профессионально интересную среду обмена мнениями и практиками, из которой профессионалам будет сложнее уйти.

3. Обратит внимание на молодых и очень опытных кандидатов. На кадровом рынке в целом такие кандидаты имеют дисконт от 20%. Однако, далеко не всякий молодой кандидат «летун», а очень опытный мечтает о пенсии. Внимание к нестандартным кандидатам может окупиться сторицей как в плане сдерживания роста ФОТ, так и, что более важно, в плане роста производительности.



Андрей ЯНКИН

руководитель отдела консалтинга
Центра информационной безопасности
компании «Инфосистемы Джет»

Автором была проделана важная работа по анализу рынка труда в области ИБ, позволяющая работодателю более взвешенно подходить к вопросам найма и аутсорсинга. Однако при использовании результатов стоит учитывать следующий нюанс — состав опрошенных. В него не были включены технические специалисты, вчерашние студенты, зато присутствовало много

высококвалифицированных (хорошо оплачиваемых) профессионалов.

Индустрия ИБ в России стремительно расширяется, не смотря на любые кризисные явления, что приводит к кадровому голоду. Люди с крайне посредственными знаниями и низкой мотивацией, имеющие некоторый опыт в ИБ, легко могут трудоустроиться. Штаты многих организаций хронически не укомплектованы. Все это приводит к существенному снижению качества обеспечения ИБ в нашей стране.

Отдельной проблемой является найм узких специалистов в регионах. Так, один из наших заказчиков жаловался, что не имеет возможности построить SOC в Калининграде, потому что укомплектовать штат местными кадрами просто невозможно, а релокация аналитиков слишком накладна.

Найти технических специалистов, которые не просто указывают компетенции в резюме, а реально что-то знают и хотят развиваться, очень непросто. Чтобы нанять грамотного проектиров-

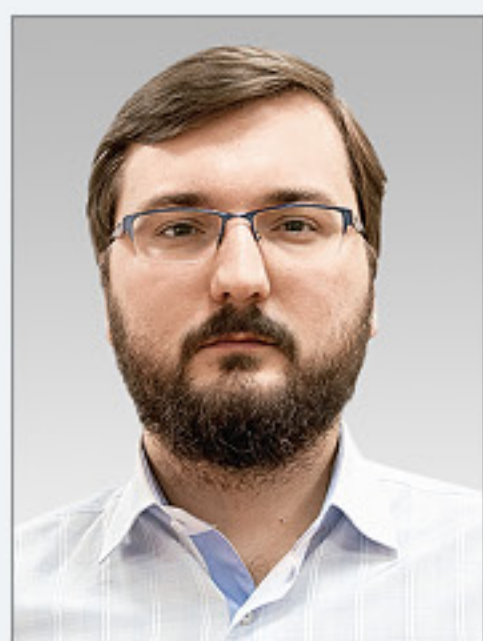
щика или внедренца по таким тематикам, как защита БД, WAF или SIEM, нам приходится проводить до 40 собеседований. Отдельная история — это найм пентестеров. Этот рынок в России настолько невелик, что его штормит от любых движений крупных игроков. В один момент на рынке может вообще не быть предложений, а уже через месяц специалисты будут томиться без единого собеседования.

Осложняет ситуацию и то, что многие специалисты по ИБ предпочитают продолжать свою карьеру за рубежом. Огромное число моих коллег покинуло страну, и это талантливейшие и высокопрофессиональные в своих областях люди. Уезжают лучшие.

С другой стороны, сегодня время возможностей. Молодой и способный специалист уже в 25 лет может возглавить крупный проект, стать руководителем подразделения и высокоцениться на рынке. В более консервативных отраслях добиться такого намного сложнее.

BIS-КОММЕНТАРИЙ

BIS-КОММЕНТАРИЙ



Сергей АНТИПОВ
старший аудитор отдела
безопасности банковских систем
ЗАО НИП «Информзащита»

Всего несколько лет назад в отрасли информационной безопасности наблюдалась ситуация, схожая с ситуацией в отрасли HR в начале нулевых — сегмент узкий, все друг друга знают, грамотных специалистов готовит небольшое число вузов. В настоящее время наблюдается непрерывное интенсивное расширение потребностей бизнеса, поставщиков услуг и представителей госсектора в квалифицированных кадрах и качественных услугах по безопасности. Все новые вузы открывают кафедры и факультеты подготовки специалистов в сфере ИБ. Рост, впрочем, нелинейный — каждая новая технология в области ИТ порождает новые уязвимости и векторы атак и, как следствие, требует новых — иногда принципиально новых — мер обеспечения информационной безопасности.

Чтобы избежать сингулярности, следует обратить внимание на фундамент — в любой области жизнедеятельности общества им являются кадры. Кроме руководящего состава и технических специалистов (архитекторов, инженеров, консультантов, аудиторов), принявших участие в опросе, проанализированном в статье, не менее важны для успеха проектов по информационной безопасности знания

и компетенции руководителей проектов и аккаунт-менеджеров. Важна связь бизнеса с вузами, готовящими специалистов по информационной безопасности. К примеру, в «Информзащите» практически все сотрудники, участвующие в пресейлах и проектах, имеют высшее профильное образование, многие сотрудники обладают сертификатами соответствующих областей ИБ. Также у нас есть программа стажировок для студентов и будущих выпускников, в настоящее время в компании проходят стажировки и пишут дипломы несколько студентов московских вузов.

Интересно посмотреть географическую статистику ИБ: сейчас специалистов по ИБ помимо Москвы (МГУ, МГТУ, МИФИ, МИЭТ, ВШЭ) и Санкт-Петербурга (СПБПУ, ГУМРФ им. С. О. Макарова) готовят и Казань (КФУ), и Ростов (ЮФУ), и Урал (УрФУ). Релокация в наше время в принципе не вызывает особых проблем у людей, а уж в рамках достойной карьеры тем более. Например, в Ростове-на-Дону есть несколько сильных игроков рынка разработки мобильных приложений и игр. Если компания готова обеспечить адекватные условия труда, почему бы не поехать: там тепло и девушки красивые.

Стабильно высокие зарплаты на рынке привлекают всё большее количество людей. К тому же, ИБ неуклонно спускается с высот «где-то там в большом дата-центре Гугла» на

уровень каждого дома (мобильная коммерция, оплата подписки Apple Music и удалённый запуск кофеварки со смартфона). И если мы росли на фильме «Хакеры», то современные подрастающие кадры уже видят утечки персональных данных у крупных государственных компаний, DDoS-атаки с помощью систем видеонаблюдения и личные фотографии голливудских знаменитостей в открытом доступе. Тема информационной безопасности уже стала неотъемлемой частью нашей жизни, и карьера в этой области уже рассматривается многими выпускниками школ наряду с другими профессиями.

Перед участниками рынка информационной безопасности стоит два очень важных вопроса: подготовка квалифицированных кадров и их удержание. Вузам полезно шире вовлекать в процесс обучения профессионалов со стороны бизнеса, а компаниям — быть открытыми к найму потенциальных специалистов и обеспечению их роста внутри компании. В «Информзащите» любой студент, обучающийся по специальности информационной безопасности, может пройти стажировку и написать диплом, а успешно прошедшим практику и зарекомендовавшим себя компания предлагает работу. Большинство специалистов компании в течение года проходят различные виды обучения и сертификации, включая международные.

**ТЕМА ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ УЖЕ СТАЛА
НЕОТЪЕМЛЕМОЙ ЧАСТЬЮ НАШЕЙ
ЖИЗНИ, И КАРЬЕРА В ЭТОЙ ОБЛАСТИ
РАССМАТРИВАЕТСЯ МНОГИМИ
ВЫПУСКНИКАМИ ШКОЛ НАРЯДУ
С ДРУГИМИ ПРОФЕССИЯМИ**

КУДА ПОЙТИ УЧИТЬСЯ ЗА ГРАНИЦЕЙ?



Марина БРОДСКАЯ
обозреватель
BIS Journal

ОБЗОР ЗАРУБЕЖНЫХ ВУЗОВ, ГОТОВЯЩИХ СПЕЦИАЛИСТОВ В СФЕРЕ ИБ

В обзоре «Абитуриенту-2017 про Абитуриента-2016¹» на портале BIS JOB мы представили довольно подробный обзор отечественных вузов, готовящих специалистов в области ИБ. После чего редакция получила коллективный читательский запрос на аналогичный обзор зарубежных вузов.

СИТУАЦИЯ С КАДРАМИ

Сначала еще раз о ситуации с кадрами. Популярный российский рекрутинговый сайт предлагает множество вакансий по направлению «информационная безопасность». Средняя зарплата самого востребованного специалиста отдела ИБ, в обязанности которого входит подготовка и доработка корпоративной документации в соответствии с требованиями законодательства и регуляторов, — 60–80 тыс. руб. Начальник IT-отдела, что-то понимающий в ИБ, — от 150 тыс. руб. Сотрудник отдела ИБ, который на практике занимается анализом и предотвращением кибератак, — от 60 тыс. руб. до 300 тыс.

Беглый анализ требований к кандидатам показывает, что работодатели по-прежнему занимаются преимущественно бумажной защитой своих сетей или хотят закрыть бреши в защите силами IT-специалистов с базовыми знаниями в области защиты информации.

В США на сайтах по поиску работы ИБ-вакансий намного больше, и требования к ним выше. Специалист среднего звена должен обладать знаниями о способах защиты компьютерных сетей, методах шифрования, управлении рисками и анализе уязвимостей, уметь прогнозировать и предотвращать инциденты. Помимо сертификатов, подтверждающих опыт работы с различными системами, кандидат должен иметь степень бакалавра и опыт работы более 10 лет или степень магистра и опыт работы от 6 лет. Такой сотрудник может претендовать на зарплату от \$ 90 тыс. в год и выше. Выпускник колледжа или не получивший диплом претендент на место ассистента, уже проработавшие некоторое время в аналогичных должностях, могут претендовать на среднюю зарплату от \$ 55 тыс. в год.

Иная ситуация в Австралии, где местные университеты не готовят нужного числа специалистов в сфере кибербезопасности. По оценкам экспертов, Австралия сегодня обеспечена такими специалистами на одну десятую от реальных потребностей. И этот дефицит стремительно увеличивается на фоне растущего числа киберугроз. Для частичного решения этой проблемы Университет Нового Южного Уэльса совместно с Commonwealth Bank создали специальную инженерную кибер-лабораторию, готовящую новых специалистов. Лаборатория обошлась в \$ 1,6 млн, не считая приглашения на работу пре-

подавателей мирового уровня и грантов талантливым выпускникам для продолжения исследований в области ИБ в докторантуре.

РЕЙТИНГ TIMES HIGHER EDUCATION

Так в какой университет стоит поступить, чтобы получить образование в сфере ИБ, обеспечивающее достойную зарплату?

По данным рейтинга, составленного журналом Times Higher Education², в 100 лучших учебных заведениях 2016–2017 гг., в которых изучают компьютерные дисциплины, в т.ч. и информационную безопасность, вошли университеты США, Европы, Китая, Южной Кореи, Австралии, Японии. В их числе есть и два российских университета: МГУ (43 место) и Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (56 место).

Пятерку лучших возглавила Швейцарская высшая техническая школа Цюриха. Направление IT в ней было выделено в отдельный департамент еще в 1981 г. и сегодня там работают 30 профессоров из 10 стран, 50 старших научных сотрудников, около 200 докторантов и научных сотрудников. В числе партнеров Школы — IBM, Microsoft, Google, SAP, Disney..., и их совместные

1 <http://bisjob.ib-bank.ru/publikaciya/93>

2 <https://www.timeshighereducation.com/student/best-universities/best-universities-computer-science-degrees>



Швейцарская высшая
техническая школа Цюриха



Калифорнийский Технологический университет



Оксфордский университет



Массачусетский Технологический институт



Технологический институт Джорджии

научно-исследовательские проекты во многом определяют будущее человечества, в том числе и в сфере ИБ.

Второй в рейтинге — Калифорнийский Технологический университет в Пасадене, известный как лидер в области математики и компьютерных технологий. Среди достижений университета — минимальное число студентов на одного преподавателя (3:1), это самый низкий показатель для учебных заведений высшей школы. Сотрудники и студенты университета вместе с Intel принимали активное участие в разработке первого асинхронного микропро-

цессора и создании суперкомпьютера Delta Touchstone.

Третье место у Университета Оксфорда. Лаборатория компьютерных технологий — одно из самых молодых его направлений. Лекции рассчитаны на подготовленных слушателей, получающих постдипломное образование. Повышение квалификации идет по трем направлениям (просто компьютерные технологии, математика и информатика, компьютерные технологии и философия).

Четвертым стал Массачусетский Технологический институт. Девизом кафедры электротехники и информатики

там считают заявление «Наши студенты изменяют мир». И действительно, выпускники MIT работают преимущественно в самых передовых компаниях, таких как Google и Microsoft.

Замыкает пятерку Технологический институт Джорджии. Школа компьютерных технологий была основана там в 1970 г., ее сотрудники и студенты получили признание за выдающиеся достижения в области искусственного интеллекта, исследования систем и теоретической информатики. Выпускники института получают среднюю стартовую зарплату в размере \$ 70–120 тыс.

Место	Университет	Страна
1	ETH Zurich — Швейцарский федеральный технологический институт Цюриха	Швейцария
2	Калифорнийский технологический институт	Соединенные Штаты
3	Оксфордский университет	Великобритания
4	Массачусетский технологический институт	Соединенные Штаты
5	Технологический институт Джорджии	Соединенные Штаты
6	Университет Карнеги Меллон	Соединенные Штаты
7	Имперский колледж Лондон	Великобритания
8	Федеральная политехническая школа Лозанны (EPFL)	Швейцария
9	Технический университет Мюнхена	Германия
10	Национальный университет Сингапура	Сингапур
11	Cornell University	Соединенные Штаты
12	University College London	Великобритания
13	Университет штата Вашингтон	Соединенные Штаты
= 14	Гонконгский университет науки и технологии	Гонконг
= 14	Nanyang технологический университет (NTU Singapore)	Сингапур
16	Эдинбургский университет	Великобритания
17	Университет Торонто	Канада
18	Университет штата Иллинойс в Урбана-Шампейн	Соединенные Штаты
19	Университет штата Мэриленд, Колледж-Парк	Соединенные Штаты
20	Колумбийский университет	Соединенные Штаты

Таблица 1. Рейтинг университетов Times Higher Education 2016–2017 гг. (в области компьютерных технологий)

РЕЙТИНГ DIGITAL GUARDIAN

В отличие от Times Higher Education, сайт Digital Guardian³ составил рейтинг лучших образовательных и научно-исследовательских программ в области кибербезопасности. По мнению автора рейтинга, в быстроменяющемся мире информационных технологий важно не только получить образование в сфере ИБ, но и поучаствовать в практических исследованиях. На фоне глобальной нехватки кадров такая возможность повысить квалификацию в процессе учебы может оказаться решающей для успешной карьеры.

82 программы⁴, которые привлекли внимание обозревателя Digital Guardian, охватывают все направления информационной безопасности и смежных с ней специальностей. Список

университетов (в основном из США и Великобритании) представлен в алфавитном порядке, авторы исследования постарались собрать максимум информации не только о курсах, программах и исследованиях по ИБ, но и по условиям проживания в учебном заведении и затратах на образование. Во многом список совпадает с рейтингом Times Higher Education, однако акцент сделан именно на программы по информационной безопасности и перспективы выпускников найти высокооплачиваемую работу по специальности.

ЧТО НУЖНО, ЧТОБЫ ПОСТУПИТЬ?

Для поступления в большинство университетов США и Европы иностранные студенты должны иметь законченное среднее образование и сдать тест на владение языком, на котором ведется преподавание курса ИБ. Многие

университеты организуют подготовительные курсы для гарантированного зачисления иностранцев в бакалавриат и магистратуру, в большинстве случаев время обучения и прочитанные курсы засчитываются в основную учебную программу. Прослушав 1–2 года основной программы, иностранные студенты могут оформить OPT-стажировку (optional practical training), которая дает возможность работать вне колледжа до 545 дней и позже поменять ее на рабочую визу на 3 года.

По оценкам посреднических компаний, предоставляющих российским абитуриентам помощь при поступлении в иностранные университеты, по IT-направлению за границу едут учиться всего 1,5% от всех выезжающих на учебу. Сколько абитуриентов поступают в иностранные вузы самостоятельно, и, главное, возвращается на родину, статистика умалчивает.

³ <https://digitalguardian.com/>

⁴ <https://digitalguardian.com/blog/cybersecurity-higher-education-top-cybersecurity-colleges-and-degrees>

ЧТО ЖДЕТ МОЛОДОГО СПЕЦИАЛИСТА?

ОБЗОР РЕЙТИНГОВ
ПО ТРУДОУСТРОЙСТВУ ВЫПУСКНИКОВ

Абитуриент мечтает поступить в вуз, студент — сдать сессию и отдохнуть, а выпускник вуза — найти работу с хорошей зарплатой. Большую роль в трудоустройстве молодого специалиста играет то, в каком вузе он учился.

МИРОВЫЕ РЕЙТИНГИ

В новый «Рейтинг по трудоустройству выпускников вузов» британской компании Quasquarelli Symonds¹ вошли сразу семь российских университетов. МГУ и МГИМО находятся в нем в промежутке 101–150 (без указания точных номеров позиций). Тем не менее по конкретному показателю «Успешность выпускников» МГУ обозначен как третий в мире. А МГИМО вообще лидирует по показателю «Трудоустройство в первые 12 месяцев после окончания вуза», получив максимальное число баллов — 100. Также 100 баллов — по показателю «Организация взаимодействия работодателей со студентами» — получил НИТУ «МИСиС», определенный в общем рейтинге вместе с МФТИ и НИУ «Высшая школа экономики» в группу 201+.

Отметим, что в группе 151–200 упоминаются Санкт-Петербургский государственный университет и РЭУ им. Г.В. Плеханова.

В бесспорных лидерах по трудоустройству выпускников — вузы США: Стэнфордский университет и Массачусетский технологический институт.



¹ <http://www.topuniversities.com/university-rankings/employability-rankings/2017>

По показателю «Успешность выпускников» в рейтинге Quasquarelli Symonds МГУ обозначен как третий в мире

В десятку лучших также вошли Университет Цинхуа (КНР, 3 место), Сиднейский университет (Австралия, 4), Кембриджский университет (Великобритания, 5), Политехническая школа ParisTech (Франция, 6), Колумбийский университет (США, 7), Оксфордский университет (Великобритания, 8), Калифорнийский университет Беркли (США, 9) и Принстонский университет (США, 10).

ОТЕЧЕСТВЕННЫЕ РЕЙТИНГИ

Отечественные рейтинги в первую очередь единодушно ставят МГУ, СПбГУ, МФТИ, НИУ ВШЭ и МГТУ им. Баумана. А направление «информационная безопасность» (10.00.00), которое с некоторых пор ввели во многих вузах, замыкает двадцатку лучших специальностей.

По данным одного из интернет-рейтингов, специальность «компьютерная безопасность» (10.05.01) представлена в 30 вузах, «информационная безопасность автоматизированных систем» (10.05.03) — в 42, «информационная безопасность телекоммуникационных систем» (10.05.02) — в 21, «информационно-аналитические системы безопасности» (10.05.04) — в 4. Бакалавриат по направлению «информационная безопасность» (10.03.01) открыт в 113 вузах, а «безопасность информационных технологий в правоохранительной сфере» преподают в 13

НАПРАВЛЕНИЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» (10.00.00), КОТОРОЕ С НЕКОТОРЫХ ПОР ВВЕЛИ ВО МНОГИХ ВУЗАХ, ЗАМЫКАЕТ ДВАДЦАТКУ ЛУЧШИХ СПЕЦИАЛЬНОСТЕЙ

вузах. Специальность «Противодействие иностранным разведкам» можно получить в одном вузе — ИКСИ Академии ФСБ РФ.

НА ФОРУМАХ

Многочисленные комментаторы на интернет-форумах, посвященных ИБ, в ходе многостраничных дискуссий о том, учиться на «безопасника» или пойти на простого программиста и не мучиться, часто сходятся в одном: качество образования молодого безопасника, как правило, невысокое. В погоне за рейтингами вузы открывают новые специальности, но не имеют кадров и материально-технической базы для обучения на должном уровне. Конечно, со временем ситуация улучшается: закупаются компьютерные лаборатории, появляются опытные преподаватели, вуз налаживает сотрудничество с антивирусными компаниями, разработчиками ПО и интеграторами.

Меняется на форумах и мнение IT-специалистов о направлении ИБ. Еще шесть-восемь лет назад комментаторы

говорили о безопасниках как о системных администраторах, отвечающих за установку антивирусов на компьютеры сотрудников и следящих за безопасностью компьютерных систем в IT-подразделении (чаще в «бумажной» форме), или как о людях из спецслужб, противодействующих хакерским атакам на сверхсекретные объекты. Редко кто давал подробный отчет о том, чем придется заниматься молодому ИБ-специалисту и какими знаниями надо владеть, чтобы стать высоким профессионалом. Карьерные и финансовые перспективы описывались смутно, чаще комментаторы-безопасники рассказывали об успехах бывших сокурсников в других сферах, далеких от ИБ.

Три-четыре года назад мнение форумчан изменилось кардинально: безопасники, выросшие из молодых специалистов, теперь делятся с подрастающим поколением опытом и учебы, и работы в сфере ИБ. Все комментаторы сходятся на том, что помимо знаний, которые дают преподаватели, необходимы самообразование и практический интерес к профессии. И что на старших курсах, за несколько месяцев практики под руководством опытных спецов они получили громадный опыт по защите информации в соответствии с требованиями регуляторов и спецслужб.

Многие на конкретных примерах рассказывают об успешных карьерах своих сокурсников в сфере ИБ. Форумчане призывают будущих коллег как можно раньше устроиться на работу по специальности и получить практические знания и навыки. Но многие по-прежнему отмечают, что есть немало случаев, когда компании экономят на ИБ и занимаются бумажной безопасностью. Есть и такие, кто заманивает молодых специалистов на работу, посылит только опытному дорогостоящему безопаснику, и платят как новичку.





В Москве состоялся юбилейный XX Пленум Федерального учебно-методического объединения в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность». На нем обсуждались вопросы модернизации государственных образовательных стандартов в области информационной безопасности в соответствии с новыми принципами обеспечения информационной безопасности. Предметом серьезной полемики стало проектирование актуализированных ФГОС ВО 3++ и других образовательных программ по направлениям ИБ. В рамках пленума состоялась научная конференция «Интеллектуальные системы в информационном противоборстве». Кроме представителей вузов в пленуме приняли участие ответственные лица и специалисты из Государственной Думы РФ, Совета Федерации РФ, ФСБ, Минобороны, МВД, Минкомсвязи, ЦБ РФ, Росфинмониторинга, Сбербанка, Росатома, субъектов РФ.

Открывая пленум, председатель ФУМО ВО ИБ Андрей Борисович Пичкур сообщил, что в зале собрались представители 115 вузов, то есть «наше УМО является одним из самых крупных в Российской Федерации». А также рассказал, что 20 лет назад было

принято парадоксальное на первый взгляд решение: сугубо гражданское УМО возглавил военный вуз — Институт криптографии, связи и информатики Академии ФСБ, и это решение оказалось правильным и дальновидным. «Сегодня, объединяя усилия Института и множества гражданских вузов по всей стране, мы высоко несем знамя, которое подняли 20 лет назад. В то время информационная безопасность была «терра инкогнита», а сегодня — это полностью сформированная образовательная область. Единственное, чего мы можем теперь пожелать, — это готовить больше специалистов по информационной безопасности, чтобы удовлетворять потребности нашей страны», — сказал А. Б. Пичкур.

Заместитель директора Департамента Минобрнауки РФ Сергей Александрович Пилипенко очертил ситуацию с подготовкой кадров с позиций министерства. Статистика такова: специалистов в сфере ИБ готовят 138 вузов,

по соответствующему направлению в них обучаются 25,5 тыс. человек. Из них 5 тыс. — по программам магистратуры. 77,6 % всех студентов обучаются за счет средств бюджета при среднем балле ЕГЭ 71,6 (средний по стране — 66,6) и среднем конкурсе на поступление 10,9 чел./место (средний по стране — 8,6 чел./место). Это высокие показатели, они подтверждают востребованность специальностей в сфере ИБ. О том же говорит ежегодное заметное увеличение цифр приема первокурсников.

Подробно рассказав о законодательных аспектах обсуждаемой сферы, С. А. Пилипенко сообщил, что область образования «Искусство и культура» уже практически на 100 % решила задачу актуализации образовательных стандартов, их ФГОС уже находится на согласовании в НСПК, после чего будет представлен на общественное обсуждение и далее рекомендован к внедрению. И напомнил, что ФЗ-122 предписы-

СПЕЦИАЛИСТОВ В СФЕРЕ ИБ ГОТОВЯТ 138 ВУЗОВ, ПО СООТВЕТСТВУЮЩЕМУ НАПРАВЛЕНИЮ В НИХ ОБУЧАЮТСЯ 25,5 ТЫС. ЧЕЛОВЕК. ИЗ НИХ 5 ТЫС. — ПО ПРОГРАММАМ МАГИСТРАТУРЫ



вает актуализировать все федеральные государственные образовательные стандарты с учетом профессиональных стандартов до 1 июня 2017 года, а к 1 сентября 2017 года разработать примерные основные образовательные программы, с тем чтобы вузы были готовы разработать основные профессиональные образовательные программы к 1 сентября 2018 года.

Последнее напоминание вызвало едкий вопрос из зала: «Мы понимаем, что до 1 июня нужно провести актуализацию стандартов, а к 1 сентября подготовить примерную программу... А в Министерстве понимают, что все образовательные организации в июне проводят итоговые аттестации, а на июль-август уходят в отпуск?»

Услышав, что ФГОС 3+ уже утвержден, переаккредитации на него не потребуются, так как речь идет не о разработке новых стандартов, а о коррекции уже сформированных, взволновавший-ся было зал понял: запас времени есть, руки развязаны, всю дальнейшую работу можно сделать не спеша, — и успокоился. А.Б. Пичкур подытожил вспыхнувшую дискуссию так: «Вывод простой: реализация ФГОС 3+ и 3++ — это внутреннее дело вузов УМО в рамках предложенных сроков, и не будем больше мучить Министерство».

Представитель Совета Безопасности РФ Алексей Андреевич Петров рассказал о работе над проектом доктрины информационной безопасности страны. Совершенствованию системы

подготовки кадров в ней уделено особое внимание. Во-первых, предполагается развитие материально-технического обеспечения образовательных программ в области ИБ. Основой такого развития должно стать создание комплексов учебно-тренировочных средств, которые объединятся в единый национальный полигон. Во-вторых, планируется сформировать механизм оценки состояния кадрового обеспечения, который позволит комплексно оценивать, насколько количество выделенных бюджетных мест в вузах соответствует текущим потребностям. В-третьих, требуется дальнейшее совершенствование контроля качества образования. Как указано в Послании Президента Федеральному Собранию (от 04.12.2014 г.), пора перестать гнаться за количеством и сосредоточиться на качестве подготовки кадров. В-четвертых, необходимо повысить престиж и привлекательность специальностей в области информационной безопасности. В упомянутом Послании Президента Федеральному Собранию отмечена важность дополнительного внешкольного образования детей и необходимость найти наиболее приемлемую организационную форму дополнительной подготовки молодежи.

Заместитель председателя ФУМО ВО ИБ Евгений Борисович Белов наряду с другими важными вопросами поднял фундаментальный вопрос статуса и смысла деятельности ФУМО. «Если мы хотим перейти на западную систему, где нет стандартов, а вместо нее общественная аккредитация, то давайте отменим стандарты, нельзя быть наполовину в положении. Надо или рожать, или не рожать. Или возвращаемся к нашим стандартам, но в другом, современном облике. И не надо бояться такого выбора: сообщество в состоянии определить базовые компетенции и сформулировать их», — заявил Е.Б. Белов.

Ставя вопрос так резко, Е.Б. Белов призывал решить скорее тактические, чем стратегические задачи. Весь ход XX пленума показал, что корабль ФУМО отлично держится на плаву и, не сбиваясь, идет своим курсом к общей цели — готовить специалистов в области ИБ, не отставая от времени.

Представитель Минобрнауки РФ также назвал Топ-10 вузов в сфере ИБ:

1. Московский технологический университет;
2. Московский государственный технический университет имени Н.Э. Баумана;
3. Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики;
4. Национальный исследовательский ядерный университет «МИФИ»;
5. Национальный исследовательский университет «МЭИ»;
6. Северо-Кавказский федеральный университет;
7. Санкт-Петербургский политехнический университет Петра Великого;
8. Томский государственный университет систем управления и радиоэлектроники;
9. Самарский национальный исследовательский университет имени академика С.П. Королева;
10. Уфимский государственный авиационный технический университет.

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



kaspersky.ru/corporate

ОНИ КОВАЛИ ПОБЕДУ

О ВЫДАЮЩЕМСЯ СОВЕТСКОМ
КРИПТОАНАЛИТИКЕ С. С. ТОЛСТОМ

Окончание. Начало в № 4/2016 г.

Наиболее информативными были линии связи Токио — Берлин, Токио — Рим, Токио — Москва, Токио — Стокгольм, Хельсинки, Стамбул и др.

Материалы дешифрованных японских телеграмм позволяли органам госбезопасности отслеживать возможность угрозы японского нападения на СССР, которая не снималась с повестки дня вплоть до середины 1943 г. — до разгрома гитлеровских войск на Курской дуге, а также успешно вести борьбу с японской агентурой, своевременно предупреждать диверсионно-

террористические акции, которые предпринимались японской стороной на железнодорожных и оборонных сооружениях в Приморье, Забайкалье и Сибири.

Информация органов госбезопасности по японской линии высоко оценивалась ГРУ и Генеральным штабом Красной Армии и позволяла последнему своевременно принимать решения, связанные с переброской частей Красной Армии с Дальнего Востока на советско-германский фронт. Для примера приведём ряд дешифрованных японских телеграмм:

**ДЕШИФРОВКА ТЕЛЕГРАММЫ
НАЧАЛЬНИКА БЮРО
ЕВРОПЕЙСКО-АМЕРИКАНСКИХ
ДЕЛ ЯПОНСКОГО МИД
СИГЭНОРИ ТОГО ЯПОНСКОМУ
ПОСЛУ В БЕРЛИНЕ**

27 июня 1942 г.

Государственная тайна.

Лично.

Признаю, что первоочередной задачей Империи на данном отрезке времени является успешное завершение войны с Англией и США. Для выполнения этой задачи требуется усилить наши операции против Англии и США, создавая вместе с тем стабильную обстановку на юге, укрепляя наши позиции в Китае. В связи с вышеизложенным остаётся неизменным направление нашей политики, о котором императорское правительство известило германскую сторону 2 июля прошлого года.

При данных обстоятельствах необходимо сохранить существующее положение на севере. Разумеется, мы всегда готовы дать решительный отпор, ежели, паче чаяния, он нарушит спокойствие. Однако теперь, когда перед нами ряд неразрешённых проблем, признано необходимым воздержаться от ослабления нажима на Англию и США и посылки войск на север, чем был бы заново расширен фронт войны.



Геннадий ЕМЕЛЬЯНОВ
член-корреспондент
Академии КRYPTOграфии РФ



Дмитрий ЛАРИН
кандидат технических наук



Американский линкор «Аризона» горит в гавани Перл-Харбора после атаки японской авиации

Прошу учесть вышесказанное и дать германской стороне следующий ответ:

Империя поздравляет Германию с её решительными победами в войне с Советским Союзом. Императорское правительство с глубоким пониманием приняло недавно выраженные взгляды и пожелания германской стороны в связи с успешным ходом германо-советской войны, вместе с тем оно хочет высказать следующую точку зрения.

Со времени вступления Японии в войну с Англией и США в декабре прошлого года наши военные операции создали серьёзную угрозу для Австралии и США на Тихом и Индийском океанах. Мы верим, что германская сторона признает эффект этих операций в деле победы Японии, Германии и Италии в их общей войне.

С другой стороны, Япония вынуждена тратить большие усилия также на ликвидацию сил Чунцина (*город в Китае, в котором тогда находилось китайское правительство во главе с Чан Кайши — авт.*), в настоящее время являющихся опорой Америки и Англии в Восточной Азии. В самом деле, в последнее время постепенно усиливается тенденция превращения китайского материка в непосредственный опорный пункт США и Англии в борьбе против Японии.

В дальнейшем Япония намерена ещё более сосредоточить свои усилия на операциях по подавлению Англии и целиком устремиться к завершению совместной войны трёх стран. Но, несмотря на крупные боевые успехи, до настоящего момента сопротивление американцев по-прежнему упорно, а следовательно, необходимо ещё более напрячь усилия в дальнейших операциях. Мало того, Японии надо ещё большее напряжение сил для того, чтобы сделать невозможным использование ресурсов юга противником, а вместе с тем захватить и самой использовать ресурсы. Сейчас Япония как раз приступила к этому.

Обобщая сказанное, переход Японии в этих условиях к активным мероприятиям против Советского Союза излишне распылит бы силы Японии и отнюдь не повлек бы за собой благоприятной с точки зрения общего положения обстановки. И не только эта великая опас-



Японский бомбардировщик Mitsubishi Ki-21 бомбит китайский город Чунцин

ность, что ослабит давление Японии на США и Англию в Восточной Азии и усилит их боеспособность в Европе, а вместе с тем откроет для США выгодную арену для борьбы с Японией, что также неизбежно имело бы неблагоприятные последствия. Мы убеждены, что с точки зрения руководства войной трёх стран нельзя сознательно становиться на путь такой политики. Разумеется, Япония полностью подготовлена в отношении севера. Благодаря этому она и до сих пор, сколько возможно сковывала Советский Союз на Востоке и в дальнейшем рассчитывает делать это.

Надеемся, что германская сторона поймёт политику Империи, которая с начала войны заключалась в том, чтобы сосредоточить все наши усилия на важнейших направлениях, победу на которых мы признали особо важной в интересах успеха трёх стран — Японии, Германии и Италии в общей войне. Что касается северного направления, то в данной обстановке мы стремимся сохранить там спокойствие, твёрдо проводя вместе с тем политику сговора советского влияния в Восточной Азии и расширения операций против Англии и США.

Выражаем надежду, что германская сторона полностью согласится с тем, что такая политика с точки зрения об-

щей ситуации даст наибольший эффект в деле успешного ведения общей для Японии, Германии и Италии войны.

Данная телеграмма утверждена на совместном совещании правительства и Верховной ставки.

Того. ЦА ФСБ России. [Органы, 1995, том 3, книга 1], [Черевко, 2010].

**ДЕШИФРОВКА ТЕЛЕГРАММЫ
№ 190 ПОСЛА ЯПОНИИ
В БЕРЛИНЕ Х.ОСИМЫ В МИД
ЯПОНИИ О ЕГО ПРЕДСТОЯЩЕЙ
ВСТРЕЧЕ С И.РИББЕНТРОПОМ
ДЛЯ ОБСУЖДЕНИЯ ПОЗИЦИИ
ЯПОНИИ В ОТНОШЕНИИ
СОВЕТСКОГО СОЮЗА**

12 февраля 1943 г.

Лично главе учреждения.

В ближайшее время я собираюсь встретиться с министром иностранных дел Риббентропом. Как Вам известно, во время последней встречи в центре внимания стояла проблема о Советском Союзе. Совершенно ясно, Германия желает, чтобы Япония, если, конечно, она располагает свободными силами, вступила в войну против Советского Союза. Естественно, следует ожидать, что сейчас, когда положение на Восточном фронте продолжает для Германии ухудшаться, этот вопрос будет предметом разговора и во время предстоящей



Японские связисты прокладывают полевую кабельную линию в Китае

встречи. Разумеется, такой вопрос должен быть нами решен самостоятельно в зависимости от нынешней обстановки в Восточной Азии и от государственной мощи империи, однако я считаю необходимым дать германской стороне объяснение, которое бы сделало для Германии достаточно ясной нашу позицию. В связи с этим прошу Вас телеграфировать Ваши соображения.

Осима. ЦА ФСБ России [Органы, 1995, том 4, книга 1], [Черевко, 2010].

**ДЕШИФРОВКА ТЕЛЕГРАММЫ
№ 817 ЯПОНСКОГО ВОЕННОГО
АТТАШЕ В БЕРЛИНЕ
ПОМОЩНИКУ НАЧАЛЬНИКА
ГЕНШТАБА ЯПОНСКОЙ АРМИИ
С ДАННЫМИ О ВОЕННОМ
ПОТЕНЦИАЛЕ ГЕРМАНИИ**

17 февраля 1943 г.

Тотальная мобилизация, которая проводится Германией в настоящее время, по-видимому, даст около 4 млн человек. Ниже сообщаю контингенты мобилизации:

а) лица, оставшиеся от прошлого призыва, и лица, прошедшие вторичную проверку годности, — 500 тыс.;

б) лица, ранее признаваемые негодными, — 700 тыс.;

в) обслуживающий персонал войск противовоздушной обороны, как в самой Германии, так и за границей (молодежь 1926–1927 гг. рождения, подлежащая призыву в ближайшее время, и личный состав частей, где мужчин можно заменить женщинами) — 1800 тыс.;

г) лица, предназначавшиеся для тыловых частей, — 1 млн. Кроме того, подлежат очередному призыву в этом году около 600 тыс. человек.

Военный атташе. ЦА ФСБ России [Органы, 1995, том 4, книга 1].

**ДЕШИФРОВКА ТЕЛЕГРАММЫ
№ 244 ГЕНЕРАЛЬНОГО
ШТАБА ЯПОНСКОЙ АРМИИ
ЯПОНСКИМ ВОЕННЫМ АТТАШЕ
В СТОКГОЛЬМЕ, ХЕЛЬСИНКИ
И СТАМБУЛЕ О СБОРЕ
ИНФОРМАЦИИ ОТНОСИТЕЛЬНО
ДИСЛОКАЦИИ СТРАТЕГИЧЕСКИХ
СИЛ СОВЕТСКИХ ВОЙСК
НА СОВЕТСКО-ГЕРМАНСКОМ
ФРОНТЕ, ДАЛЬНЕМ ВОСТОКЕ
И НА ТУРЕЦКО-ИРАНСКОЙ
ГРАНИЦЕ**

19 февраля 1943 г.

Если у Вас имеются сведения относительно расположения Советской Армии, прошу сообщить их (не позднее марта месяца) по нижеследующим пунктам:

1. Число стратегических единиц на советско-германском фронте. Номера этих соединений, дислокация и номера частей, входящих в их состав. Фамилии командующих. Причём в отношении авиации сообщить тип самолетов в авиадивизии.

2. Какие соединения советских войск находятся на турецко-иранской границе, их расположение и номера. То же в отношении Дальнего Востока.

Пом. начальника генерального штаба. ЦА ФСБ России [Органы, 1995, том 4, книга 1].

**ИЗ ДЕШИФРОВКИ ТЕЛЕГРАММЫ
МИД ЯПОНИИ № 122
ПОСЛУ ЯПОНИИ В БЕРЛИНЕ
О ПОЛИТИКЕ ЯПОНИИ
В ОТНОШЕНИИ СССР**

24 февраля 1943 г.

Мы прекрасно понимаем, что в нынешних условиях германская сторона в душе желает и надеется, чтобы Япония начала войну против Советского Союза. Однако императорское правительство твердо придерживается линии политики в отношении советского правительства, изложенной в моей телеграмме от прошлого года за № 588. Примите это к сведению и, когда увидите с рейхсканцлером Гитлером и министром иностранных дел Риббентропом, дайте им детальные объяснения.

О подробностях по данному вопросу в телеграмме достаточно исчерпывающе изложить трудно, поэтому я поручу группе связистов, выезжающей из Токио в начале марта, дать вам все соответствующие пояснения...

Тани (Тани Масакжи — японский дипломат, в 1941–1943 гг. — директор правительственного комитета информации, в 1942–1943 гг. — министр иностранных дел Японии, в 1943–1945 гг. — посол Японии при нанкинском правительстве в Китае). ЦА ФСБ России [Органы, 1995, том 4, книга 1].

**ДЕШИФРОВКА ШИФРТЕЛЕГРАММЫ
№ 16 МИНИСТРА ИНОСТРАННЫХ
ДЕЛ ЯПОНИИ МАМОРУ
СИГЭМИЦУ ЯПОНСКОМУ ПОСЛУ
В МОСКВЕ С ИНСТРУКЦИЯМИ
О ПОЗИЦИИ ЯПОНИИ НА
ПЕРЕГОВОРАХ С СССР ПО
УРЕГУЛИРОВАНИЮ РЯДА
СПОРНЫХ ВОПРОСОВ**

28 июня 1943 г.

Японское правительство стремится поддержать нормальные отношения между Японией и Советским Союзом и побуждать Советский Союз строго придерживаться пакта о нейтралитете. Вместе с тем оно намерено по возможности всегда иметь точное представление об отношениях между СССР и США и отношениях между СССР и Германией, чтобы следить таким образом за международной обстановкой. В этих целях японское правительство желает активно разрешить ряд спор-

ных вопросов между Японией и СССР, в частности на определенных условиях компенсации передать советской стороне нефтяные и каменноугольные концессии на Северном Сахалине.

Примите меры к тому, чтобы данные переговоры не вызвали охлаждения между Японией и Германией.

Сигэмицу [Органы, 1995, том 4, книга 1].

**ДЕШИФРОВКА ТЕЛЕГРАММЫ
ЯПОНСКОГО ВОЕННОГО
АТТАШЕ В БЕРЛИНЕ № 365
ПОМОЩНИКУ НАЧАЛЬНИКА
ГЕНШТАБА ЯПОНСКОЙ
АРМИИ О ЧИСЛЕННОСТИ
И ДИСЛОКАЦИИ ВОЙСК
ГЕРМАНИИ, АНГЛИИ И США
В РАЙОНЕ СРЕДИЗЕМНОГО
МОРЕЯ И НА БАЛКАНСКОМ
ПОЛУОСТРОВЕ**

29 сентября 1943 г.

Информация о численности войск Германии, Англии и Америки с южной части Средиземного моря на 20 сентября.

1. В районе Средиземного моря: германских войск — 89–93 дивизии (из них в Северной Италии — 10–13 дивизий); англо-американских войск — 30 дивизий (из них больше половины находятся на острове Сицилия).

2. На балканском полуострове: германских войск — 22 дивизии (из них в Греции — 8 дивизий, в Югославии — 11 дивизий, в Болгарии — 2 дивизии, в Румынии — 1 дивизия).

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

**ИЗ ШИФРТЕЛЕГРАММЫ
ГЕНШТАБА ЯПОНСКОЙ
АРМИИ № 212 ВОЕННОМУ
АТТАШЕ В СТОКГОЛЬМЕ
С ИНФОРМАЦИЕЙ
О ГЕРМАНСКОЙ АРМИИ**

21 марта 1944 г.

Информация о германской армии, составленная на основании сведений, полученных от японских военных атташе в Европе.

1. В конце прошлого года общая численность германских войск составляла 9800 тысяч человек, в том числе: в сухопутной армии — 8100 тысяч человек, в авиации — 1500 тысяч человек, во флоте — 210 тысяч человек.

2. Помимо существующих в сухопутной армии 320 полевых дивизий, весной или летом нынешнего года намечено сформировать еще 40 дивизий.

Распределение дивизий, включая 10 вновь сформированных: Восточный фронт (включая Финляндию) — 200 дивизий (в том числе автобронетанковых — 25 дивизий, танков — 40000); Норвегия — 13 дивизий; Дания — 5 дивизий; Бельгия, Голландия и Франция — 50 дивизий (из них 9 вновь сформированных); Италия — 27 дивизий; Балканы — 24 дивизии.

3. Количество дивизий по родам войск, не считая вновь сформированных: полевых и пехотных дивизий — 225; бронетанковых дивизий — 45, в том числе 12 дивизий СС; мотомеханизированных дивизий — 20; горно-егерских дивизий — 10; кавале-

рийских — 2; пехотных дивизий при авиации — 18. Всего: 320 дивизий.

4. Авиация состоит из 7 воздушных эскадр и отдельных воздушных соединений. Самолетов первой линии — 8000. Распределение и численность авиации: восточный фронт — 1-я, 4-я, 6-я воздушные эскадры (3500 самолетов); Норвегия — 5-я воздушная эскадра (500 самолетов); Дания, Бельгия, Голландия, Франция — 3-я воздушная эскадра (1200 самолетов); Италия — 2-я воздушная эскадра (800 самолетов); Балканы — отдельное воздушное соединение (500 самолетов); в самой Германии — отдельная воздушная эскадра (1500 самолетов).

Пом. начальника генштаба. ЦА ФСБ России [Органы, 1995, том 5, книга 1].

**ИЗ ШИФРТЕЛЕГРАММЫ № 982
ПОСЛА ЯПОНИИ В БЕРЛИНЕ
ХИРОСИ ОСИМА В МИД ЯПОНИИ
О ВОЕННОМ ПРОИЗВОДСТВЕ
ГЕРМАНИИ**

10 августа 1944 г.

Лично главе учреждения.

Ниже сообщаю суммарную информацию о военном производстве, данную мне министром вооружения Шпеером:

а) месячная продукция винтовочных патронов 500–600 млн;

б) пулеметов новой системы 20000, старой системы 5000;

в) легких гаубиц калибра 10,5 см — 1000 (в свое время от рейхсканцлера было указание, чтобы добиться 300);

г) тяжелых гаубиц калибра 15 см — 300;

д) штурмовая артиллерия. Ставилась цель, чтобы она могла преследовать танки, обладая большей скоростью, чем они. Стали производить более легкую артиллерию, весом в 15 тонн вместо 25. В феврале будущего года производство легких орудий в месяц достигнет тысячи единиц. Как только мы сможем перейти к массовому выпуску, производство орудий типа «РАК» будет прекращено и будет производиться только штурмовая артиллерия;

е) зенитная артиллерия производится трех типов: калибром в 8,8 см, 10,5 см и 12,6 см... В дальнейшем наиболее распространенным орудием будет тип калибром в 8,8 см;



Линия сборки истребителей Хейнкель He-162 на подземном заводе в Тартуне, Германия

ж) для германской промышленности большое затруднение представляет тот факт, что ей приходится иметь дело с тремя видами орудий: легкими гаубицами в 10,5 см, противозенитными пушками в 8,8 см и противотанковыми в 7,5 см. Сильная сторона нашего противника — Советского Союза в том, что все его орудия одинакового калибра в 7,6 см;

з) противозенитные пулеметы имеются двух видов... Так как боевые качества первого слабы, его должен вытеснить второй...

Как я вам уже докладывал, производство самолетов в Германии резко увеличилось. Полагаю, что в ближайшем будущем мы сможем иметь больше истребителей и штурмовиков, чем Англия и США вместе взятые.

Шпеер продолжал дальше:

«Меди, марганца и молибдена у нас имеется достаточно. Этого количества нам вполне хватит. Мы имеем запасы хрома на 2 года. Так как понемногу мы

будем получать его с Балкан, то отсутствие экспорта из Турции изменений не внесёт. Мы будем экономно расходовать запасы.

Вольфрама тоже хватит на год-два. Имеются запасы превосходного никеля. Хром и никель очень важные элементы, и, если их в Германии не станет, военная промышленность окажется поставленной в затруднительное положение. Я намечаю широкое внедрение заменителей...

О самолётах-снарядах «V-1» (в основном говорил Мильх). Каждый день по объектам противника самолётов-снарядов типа «V-1» выпускается от 150 до 200 штук. У самолётов-снарядов удобная форма и большая скорость, поэтому противозенитная артиллерия их сбить не может...

Шпеер сказал: «В феврале нынешнего года я (Шпеер) принял авиапромышленность под ведение министерства вооружений. Как раз в то время из-за бомбардировок производство

истребителей и бомбардировщиков, в увеличении производства которых германская сторона была особо заинтересована, упало до 1150 в месяц. После этого удалось быстро поднять производство, и в июле оно достигло уже 4500, а к концу этого года намечено выпускать от 6500 до 7000...

Подземные авиазаводы занимают площадь минимум в 800000 кв. метров, вскоре она будет увеличена до 1000000 кв. метров. Тогда только одна подземная авиапромышленность в месяц будет давать до 1000 самолетов. К концу года подземную площадь намечено расширить до 3000000 кв. метров.

Осилью. ЦА ФСБ России [Органы, 1995, том 5, книга 2].

Обратим внимание, что в двух последних телеграммах содержатся весьма подробная информация о состоянии немецкой армии и оборонной промышленности. Анализ перехваченных



К 120-ЛЕТИЮ ГЕОРГИЯ ЖУКОВА

*Хорошая работа шифровальщиков
помогла выиграть не одно сражение*
Георгий Жуков

В мае 1939 г. в районе реки Халхин-Гол японские войска вторглись на территорию Монголии, имевшей договор с СССР об оказании военной помощи.

В отражении нападения принимала участие группа советских криптографов. Сразу по прибытии они приступили к дешифрованию кода японской Квантунской армии. Были достигнуты определенные успехи в дешифровании, когда в первых же боях был захвачен образец кода. Японцы продолжали использовать этот код вплоть до окончания боевых действий, и наши дешифровальщики получали ценные сведения. Эта информация ежедневно докладывалась командующему советскими войсками будущему маршалу Советского Союза Г. К. Жукову.

Перед решающим наступлением, Жуков разработал план оперативно-тактического обмана противника, включающий программу дезинформации.

«Мы знали, что противник ведет радиоразведку и подслушивает телефонные разговоры, и разработали в целях дезинформации целую программу радио и телефонных сообщений. Переговоры велись только о строительстве обороны и подготовке ее к осенне-зимней кампании. Радиообман строился главным образом на коде, легко поддающемся расшифровке» [Жуков Г. К. Воспоминания и размышления. М. Воениздат 1971].

В результате японцы поверили в то, что советские войска укрепляют свою оборону и наступать не собираются, и просчитались. Советскому командованию информация о том, что японцы «клюнули» на дезинформацию, стала известна благодаря дешифрованию перехваченной японской радиограммы.

Дмитрий ЛАРИН
кандидат технических наук

и дешифрованных нашими спецслужбами японских радиogramм свидетельствует, что советским криптоаналитикам удавалось прочитывать их содержание и своевременно докладывать эту информацию советскому руководству.

Вышеупомянутый Указ о награждении советских дешифровальщиков свидетельствует о том, что успехи С. С. Толстого в криптоанализе были очень весомы. Во время Отечественной войны С. С. Толстой был ещё раз награжден орденом Ленина, орденами Красного Знамени и Трудового Красного Знамени и орденом Знак Почёта. Уже одно то, что даже непосредственные начальники С. С. Толстого не имели стольких наград, говорит о важности дешифрованной ими информации для Верховного командования. Закончил войну С. С. Толстой полковником, заместителем начальника отделения 5 Управления НКГБ СССР. В качестве почётного гостя вместе с дочерью Ольгой он был приглашен на исторический Парад Победы.

Сергей Семёнович активно участвовал в обучении криптографов на курсах и в Специальной школе. Нельзя не отметить и тот факт, что С. С. Толстой в соавторстве с Б. А. Аронским, С. Г. Андреевым и А. И. Копытцевым (последние двое упомянутым Указом выше были отмечены орденами Трудового Красного Знамени) в 1939–40 годах написали один из первых советских учебников криптографии [Энциклопедия, 2004]. К сожалению, Сергей Семёнович не дожил до победы над Японией, он умер 23 июля 1945 года от обширного кровоизлияния в мозг прямо на рабочем месте. Видимо, сказалось громадное нервное напряжение четырёх военных лет, ведь в июле для одного из ведущих наших дешифровальщиков война была еще в самом разгаре. Бывшие сослуживцы и помощники рассказывали, что он был одержим работой, о его характере и аналитических способностях сложены легенды [Кузьмин, 1998], [Соболева, 2002], [Энциклопедия, 2004, с. 735]. Подробнее о работе С. С. Толстого и его коллег можно прочитать в главе 5 книги [Бутырский, 2012].



От имени СССР генерал-лейтенант Кузьма Деревянко подписывает акт о капитуляции Японии на борту линкора «Миссури», 2 сентября 1945 года

ЛИТЕРАТУРА

- [Анин, 1996] Анин Б. А., Петрович А. И. Радиошпионаж. М.: «Международные отношения», 1996.
- [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.
- [Забелин, 2008] Забелин А. Центр японского шпионажа в Скандинавии // Независимое военное обозрение № 6, 2008, с. 7.
- [Кошкин, 1989] Кошкин А. А. Крах стратегии «спелой хурмы». Военная политика Японии в отношении СССР 1931–1945 гг. М.: «Мысль», 1989.
- [Кузьмин, 1998] Кузьмин Л. А. Не забывать своих героев // Защита информации. Конфидент № 1, 1998, с. 83–85.
- [Ландер, 2007] Ландер И. И. Негласные войны. История специальных служб 1919–1945. Одесса, «Друк» 2007. <http://www.lander.odessa.ua>
- [Органы, 1995] Органы государственной безопасности СССР в Великой Отечественной войне 1941–1945. Сборник документов. М.: «Русь» 1995.
- [Соболева, 2002] Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.
- [Сыромятников, 2001] Сыромятников Б. А было ли нападение внезапным? // Сигары Шееле для «Барона Дризена» М.: «Издательский дом Гелеос», 2001, с. 17–34.
- [Черевко, 2010] Черевко К. Е. Военные тайны XX века — Серп и молот против самурайского меча. М.: Российская Академия наук. Институт российской истории // www.modernlib.ru, www.fb2book.com. 21.11.2010.
- [Энциклопедия, 2004] Энциклопедия секретных служб России. М.: Астрель, 2004.
- [en.wikipedia] <http://en.wikipedia.org>
- [Kahn, 1967] Kahn D. The codebreakers. N- Y: Macmillan Publ. Co., 1967.
- [topcatalog] www.topcatalog.com.ua/news/322245.html
- [vif2ne] <http://vif2ne.ru/forum/0/archive/1788/178855.htm>



Александр БОДРИК
сертифицированный специалист
по управлению информационной
безопасностью корпоративных
и облачных ландшафтов, член
ISACA, ASIS, ACFE

ПАУТИНА РИСКОВ ТРЕТЬИХ СТОРОН

КАК ДЕРЖАТЬ ЕЕ ПОД КОНТРОЛЕМ

В 2012 году, участвуя от Службы ИБ в Программе по автоматизации АЗК глобальной нефтегазовой Группы, я не представлял, в какую паутину рисков попадает подключающееся к любой третьей стороне предприятие.

В это время на АЗК активно продвигалась карта ХХХ с начислением бонусных баллов от оператора системы ло-

яльности ХХV, а значит компрометация сети оператора создавала новый вектор атаки на сеть Группы.

Произведем простой расчет. Допустим, вероятность взлома сети АЗК составляет 50%. Аналогично, вероятность взлома ХХV — 50%. Итого вероятность взлома АЗК со стороны ХХV $\text{вероятность взлома АЗК} = 50\% \times 50\% = 25\%$.

Итоговый риск — 75%, т.е. уровень риска АЗК вырос на 50% только из-за подключения оператора. Вспоминая популярную фразу «Существуют три вида лжи: ложь, наглая ложь и статистика», можно отмахнуться даже от таких простых расчетов, но тяжело забыть взлом розничной сети Таргет в 2013. Тогда утекло 130 миллионов клиентских записей, и уволился гене-

ральный директор сети. А ведь похитивший данные вирус пришел со стороны обслуживавшей POS третьей стороны.

Но самая проблемная часть связанного с третьими сторонами риска (далее — third party risk или TPR) — это его плохая управляемость. Пока мы совершенствуем процессы и внедряем технологии защиты внутри организации у партнеров происходит непонятно что. Многие ли службы ИБ включили в требования к партнерам необходимость соответствовать стандартам ИБ организации в данный момент времени?

В 2015 году из интервью представителя интегратора ХХЗ я узнал о заключенном еще в 2005 году долгосрочном аутсорсинговом контракте между ХХЗ и вышеупомянутым оператором. В первом приближении стоило бы к нашему TPR добавить половину (12,5%), допуская что у ХХЗ с ИБ не лучше, чем у других участников цепочки. Т.е. из-за подключения 1-го партнера наш риск вырос с 50% до 87,5%. А в том же интервью ХХЗ рассказали о поддержке телекома, банка и других...

И тут цепочка превращается в паутину. Один раз организовав подключение всего лишь одного партнера, организация теряет прозрачность своего профиля риска ИБ. Ведь ни ХХЗ, ни какой другой из ТОП-10 интеграторов не раскрывают публично свои практики ИБ (в отличие от западных вендоров Google, Microsoft, Amazon).

ИДЕНТИФИКАЦИЯ РИСКОВ. ВНЕДРЕНИЕ ТОЧЕК КОНТРОЛЯ

Увы, не только ХХЗ подключается к современной организации. Это были и ИТ-аутсорсеры/вендоры, и информационные сервисы для руководства (Reuters+), и многие другие инициативы, отследить которые отдельная непростая задача.

В идеале оптимален гибридный подход — «и сверху, и снизу»: «сверху» делать требования по ИБ приложением любого договора организации (как есть NDA), а «снизу» делать невозможным добавление любых сетевых маршрутов или пользователей в системы организации без согласования с ИБ.

И ТУТ ЦЕПОЧКА ПРЕВРАЩАЕТСЯ В ПАУТИНУ. ОДИН РАЗ ОРГАНИЗОВАВ ПОДКЛЮЧЕНИЕ ВСЕГО ЛИШЬ ОДНОГО ПАРТНЕРА, ОРГАНИЗАЦИЯ ТЕРЯЕТ ПРОЗРАЧНОСТЬ СВОЕГО ПРОФИЛЯ РИСКА ИБ

Таким образом мы защитимся от случаев «хотели как лучше, а получилось как всегда», когда бизнес просто не понимает рисков, которые приносит его потенциальная сделка. Рисков, влияющих на P&L как отдельного бизнес-юнита, так и P&L организации.

УЧЕТ РИСКОВ

Каждый партнер может подключаться не только в одном месте и одним способом, а значит, для понимания профиля риска и поиска причин инцидентов ИБ, необходим учет подключений. Для начала это может быть простая таблица, содержащая минимальную информацию — название организации партнера, ответственные от ИБ, бизнеса и ИТ-инфраструктуры, если принято решение типизировать партнера, то его тип, дата последнего прохождения партнером аудита безопасности и ссылка на профиль риска партнера, ранее заполненного офицером ИБ.

Можно использовать свободное и промышленное ПО от западных или российских производителей. В частности, существует квадрат Gartner «IT Risk Management», в других странах управление TPR уже внедрено в крупнейших организациях — JPMorgan, Citigroup, Pepsi и NEC.

АУДИТ ТЕКУЩИХ РИСКОВ

Наладив процесс идентификации будущих TPR, разумно обратить внимание на существующие. Ведь организация уже имеет консультантов, СП, аутсорсеров и др., профиль риска которых влияет на профиль риска организации. Все их подключения необходимо определить и вести их учет — для дальнейшего управления TPR.

Для аудита могут быть полезны технические системы управления рисками сети, которые покажут какие подклю-

чения извне имеет сеть и «подсветят» те подключения, использование которых может привести к эксплуатации реальных уязвимостей организации. Наиболее продвинутые из них позволяют моделировать новые подключения и анализировать состояние сети в прошлом, интегрируясь с сетевыми устройствами, сканерами уязвимостей и CMDB.

Необходимо обратить внимание и на контракты с консультантами, сидящими в офисе организации, и пользователями, имеющими право удаленного доступа.

УПРАВЛЕНИЕ РИСКАМИ — СНИЖЕНИЕ РИСКОВ

Различающийся профиль рисков связанных сторон приводит к необходимости в первую очередь снижать риски. Ведь инцидент безопасности может произойти не у самой организации, а у ее связанной стороны, и эти убытки организация не всегда сможет покрыть. Кроме примера с Таргет приведу и другие.

В сфере нефтегаза. На АЗК нефтегазовой группы через партнера пробрался вирус. Вирус распространился по сети и добрался в головную компанию холдинга, а через нее в газотранспортный дивизион холдинга. В итоге вирус изменил режим работы газоперекачивающего агрегата, вследствие чего поломалась турбина агрегата, стоимость замены — \$4 млн. Дело было в зимний пик поставок газа, и страна-потребитель предъявила холдингу иск на \$10 млн неустойки. Ни одна АЗК в принципе не стоит \$14 млн.

Финансовая индустрия. Каждую неделю банки видят, как через взломанные клиент-банк контрагента перемещаются деньги для затруднения

возврата. Каждый такой случай несет юридические и финансовые риски для взломанного «прокси» контрагента.

Если все же бизнес готов принять «все риски» и «безотлагательно», то необходимо зафиксировать это письменно (неплохая форма есть в стандарте ISO 13569), и тогда в будущем будет понятно — это безопасность перестраховывалась или бизнес недостаточно ответственно относился к создаваемым им рискам. Иногда после предъявления такой формы риск-аппетит бизнеса стремительно падает. Особенно если бизнес-модель уже устоялась (консервативные индустрии — ТЭК, ГМК и т.п.).

КОНТРОЛЬ РИСКОВ

Контроль связанных рисков подразумевает соблюдение трех принципов:

- ◆ «чтобы было не хуже, чем у нас»;
- ◆ «соответствие требованиям в текущий момент времени»;
- ◆ «переносимость требований на партнеров партнера».

Аналогично не помешают выборочные проверки физической безопасности активов партнера.

Интересной альтернативой тщательному контролю выполнения требований будет прописанная в контракте финансовая ответственность за инциденты ИБ. Понятно, что партнер в этом случае должен иметь заведомо лучшие практики ИБ и стабильное финансовое положение. Например, это может быть один из ИТ-гигантов. Хотя после четырех лет, проведенных в переговорах с самыми разными организациями, я обнаружил что в Группе была, вероятно, лучшая служба ИБ среди нефтегазовых компаний России, ее PaaS-инфраструктура от одного из ИТ-гигантов в швейцарском ЦОДе подвергалась аудитам безопасности службой ИБ ИТ-гиганта в разы чаще, чем внутренняя сеть Группы.

ОПТИМИЗАЦИЯ РИСКОВ — КАПИТАЛИЗАЦИЯ РИСКОВ

Понятно, что попытка реализовать, например, службой ИБ Сбербанка принципы контроля рисков могут встретить ожесточенное сопротивление партнеров. Ведь как ООО «Ромашка» может выделить на безопасность сопостави-

ИНТЕРЕСНОЙ АЛЬТЕРНАТИВОЙ ТЩАТЕЛЬНОМУ КОНТРОЛЮ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ БУДЕТ ПРОПИСАННАЯ В КОНТРАКТЕ ФИНАНСОВАЯ ОТВЕТСТВЕННОСТЬ ЗА ИНЦИДЕНТЫ ИБ

мые с гигантами средства? Эффект масштаба обычно позволяет крупным компаниям достигать уровня безопасности, недостижимого для «малышей».

В таких случаях в дело вступает «капитализация» рисков, когда бизнес вместо того, чтобы постоянно платить за повышенный уровень безопасности в партнере (выбирать более дорогих партнеров (OPEX), один раз платит за внедрение технических точек контроля (CAPEX).

Техническими точками контроля могут быть NAC, secure remote access, PIM, IPS, 2FA, adaptive access.

Внедрение технических точек контроля позволяет закрыть возможные векторы атаки — снизить уязвимость сети организации перед внешним подключением и таким образом снизить необходимость в применении 100 % требований ИБ организации к партнерам.

МОНИТОРИНГ РИСКОВ

Новые технологии и бизнес-тренды меняют не только профиль риска организации, но и профили риска ее партнеров. Необходим мониторинг TPR, чтобы понимать насколько TPR влияет на профиль рисков организации, насколько служба ИБ операционно эффективна.

Для мониторинга TPR необходимо контролировать 3 основных домена:

- ◆ Эффективность процесса управления связанными рисками организации.
- ◆ Профиль риска партнера.
- ◆ Профиль связанных рисков организации.

Примеры метрик для измерения эффективности процесса управления связанными рисками:

- ◆ Процент подключений партнеров, прошедших оценку ИБ среди всех партнеров.

- ◆ Медианное время подготовки профиля риска офицером безопасности.

Примеры метрик для профиля риска партнера:

- ◆ Количество инцидентов ИБ за последний год.
- ◆ Дата последнего аудита ИБ партнера организацией.
- ◆ Количество найденных несоответствий.
- ◆ Процент устраненных в оговоренный период несоответствий.
- ◆ Количество принятых рисков для этого партнера.

Примеры метрик для профиля связанных рисков организации:

- ◆ Медианное значение количества невыполненных требований (принятых рисков) на одного партнера.
- ◆ Среднее отклонение количества инцидентов ИБ по партнерам.
- ◆ Количество инцидентов ИБ, вызванных соединением с партнером.
- ◆ Процент контрактов с партнерами включающих требования по ИБ.

Для запуска мониторинга выстраиваем коммуникации. В частности, определяем контактные лица по ИБ в целом, управления инцидентами и устранения несоответствий со стороны организации и партнера, а также резервные КЛ (болезни, отпуска и т.п.).

Кроме контактных лиц необходимо определить правила классификации и обработки инцидентов ИБ, формы и периодичность отчетности партнера (например, уровень обновлений, отчетность антивирусной системы в периметре сервисов для клиента).

ИНФОРМИРОВАНИЕ О РИСКАХ (RISK INTELLIGENCE)

Эффективное управление TPR возможно на основе достоверной информации, и традиционным первым шагом будет предварительный аудит партнера перед



подписанием договора. Такой аудит необходим при прямом сетевом подключении, предоставлении доступа к чувствительной информации или другом серьезном изменении. Проводить его желательно с использованием ранее разработанных критерий типизации партнеров с точки зрения ИБ.

Аудит должен быть направлен на оценку способности службы ИБ партнера грамотно и эффективно управлять профилем риска партнера. Име-

ет ли служба ИБ партнера поддержку бизнеса? Какие угрозы она считает актуальными и как с ними борется?

У крупных компаний на Западе принято заказывать тест на проникновение партнера. Для снижения сопротивления бизнеса желательно забюджетировать пентест на стадии формирования бюджета проекта.

Предостерегу от слепого доверия наличию сертификации по риск-ориентированным стандартам ИБ (27001 и др.),

что само по себе не гарантирует мер безопасности. В моей практике сертификат, выданный одной из ТОП-30 компаний страны, охватывал несколько ПК SOC партнера, тогда как предлагались услуги call-center.

По итогам аудита безопасности важно не только понять профиль риска партнера, но и установить рабочие отношения — расширить профессиональную сеть контактов для двухстороннего обмена информацией об угрозах. Партнеры обычно работают в других секторах экономики, у них другой «сектор обзора» и от них можно получить информацию об угрозах, от которых организация еще не пострадала.

Для стимулирования партнера к совершенствованию системы ИБ рационально предусмотреть в договоре штрафы за нарушения требований ИБ организации (естественно, как и right to audit). На практике штрафы редко применяются, но само их наличие облегчит коммуникацию с партнером и мотивирует его менеджмент.

ЗАКЛЮЧЕНИЕ

Разумная и эффективная система управления TPR позволяет не только снизить влияние TPR на профиль риска организации, но и снизить профиль риска национальной экономики. Ведь упомянутый в начале рассказа оператор имеет соединения с десятками компаний, каждая из которых может пострадать от небрежностей руководства оператора при построении системы ИБ.

Аналогичная ответственность лежит и на тех организациях, которые сами создают много подключений к сетям других партнеров. Укрепляя собственную безопасность, они укрепляют собственный бренд, защищают рыночную долю, не допуская таких инцидентов как взлом Таргет или утечки Сноудена, получившего доступ к чувствительным данным, работая в консультанте Booz Allen Hamilton. Учитывая высокий потенциал ущерба от внутренних нарушителей и целый ряд кейсов злоупотребления полномочиями, не хотелось бы добавлять к внутренним нарушителям организации еще и внутренних нарушителей партнеров.

ПОСЛЕДНИЙ ДЕНЬ ПОМПЕИ

ПОЧЕМУ К 2025 ГОДУ
ПОПУЛЯЦИЯ ИБ-ИНЖЕНЕРОВ
СОКРАТИТСЯ В РАЗЫ

Александр БОДРИК

сертифицированный специалист
по управлению информационной
безопасностью корпоративных
и облачных ландшафтов, член
ISACA, ASIS, ACFE

Сегодня ИБ-инженером быть хорошо — значительный спрос, понятно что нужно делать, чтобы быть востребованным и зарабатывать больше. Но такая «красивая жизнь» продлится не долго, так как против ИБ-инженеров играют 5 больших факторов.

2 РАЗВИТИЕ РЕШЕНИЙ

Заказчики-пионеры IDM в 2007–2011 гг. использовали Oracle и IBM, внедрение которых требовало больших команд (вплоть до десятков человек на инфраструктурах в сотни тысяч юзеров). Более современные решения позволяют реализовывать проекты силами 2–3 человек, предоставляя намного больше «из коробки»

5 КОНСОЛИДАЦИЯ ИТ-ЛАНДШАФТА

За последние годы крупные вендоры (Cisco, VMware, IBM, Microsoft, Dell) совершили не один десяток поглощений ИБ-компаний. ИБ-технологии проникают в ИТ-среду, становятся ее характеристикой. Сравните ИБ-возможности винсерверов года эдак 2003-го и нынешнего — небо и земля. А ведь управлять этими технологиями будут в первую очередь ИТ-инженеры

1 ОБЛАКА

Бизнес (хоть и с запозданием относительно прогнозов) уходит в «облака», которые в свою очередь консолидируют мировую ИТ-инфраструктуру. А где консолидация, там повышение эффективности и снижение потребности в инженерах в пересчете на объект обслуживания

3 МАШИННОЕ ОБУЧЕНИЕ

Один из ТОП-5 банков обходится 1 full-time сотрудником для решения задачи антифрода. 99,99 % всех проблем устраняются с помощью нейронных сетей и другой «вуду-магии»

4 ДИДЖИТАЛИЗАЦИЯ БИЗНЕСА

Работающий на цифровой скорости бизнес требует работающей на той же скорости ИБ. Придется отказаться от «человеческого фактора» по максимуму, иначе ИБ выбросят за борт реальных бизнес-процессов и оставят починять антивирусы

Кстати, подобная тема касается и пентестеров, ИБ-архитекторов и всех «технических» людей. Эпоха «дикого Запада» подходит к концу, и револьвер будет деклассирован законом — повышением осведомленности пользователей, управлением third party risk, управлением взаимоотношениями с бизнесом (бизнес-партнеры), интегрированным управлением методологией и сервисами ИБ (через SLA тех же «облаков»). Ростки изменений уже взошли, например, в США, где соотношение револьвер/закон совсем не такое, как в России.

ЛОНДОН — МОСКВА:



ГДЕ ДЕНЬГИ?

Операции между российскими и британскими банками, завязанные на валютном контроле и информационной безопасности, издавна дело многосложное, противоречивое. Расскажу о личном опыте рядового клиента, а опыт, по словам любимого А. С. Пушкина, — «...сын ошибок трудных». Надеюсь, читателю будет интересно.

Обо всем по порядку. Лондонская фирма начислила мне гонорар за выполненную творческую работу. Чтобы его получить, я скорёхонько открыл текущий счет в фунтах стерлингах в одном из крупнейших столичных коммерческих банков (его название опускаю из этических соображений). Направил

в Лондон реквизиты счета по e-mail, и, для душевного спокойствия, продублировал их по факсу. Ответ пришел незамедлительно: «Деньги Вам перевели». По семейным обстоятельствам, они были тогда нам очень нужны.

Выждал два дня, обычно занимающие перевод денег из-за рубежа, и, лущезарно улыбаясь, пришел в банк получить свою рублевую наличность. Увы, деньги не пришли.

Два месяца я ходил за ними в отделение банка, как на работу! Для сотрудников отделения стал добрым знакомым — они угощали меня кофе и конфетами. Британский банк клялся-божился, что деньги перевел, — прислал по e-mail подтверждение. В конце концов, банк

известил, что из России деньги к нему вернулись. Я смог их получить лишь через несколько месяцев, уже на месте.

Я добросовестно попытался выяснить: на каком, собственно, основании российский банк не принял от британского банка мои трудовые деньги? Все условия валютного контроля были строго соблюдены. Реквизиты счета проверены-перепроверены. Мной руководил даже не меркантильный, а, скорее, исследовательский интерес.

Но все усилия оказались втуне — лоб уперся в железобетонную бюрократическую стену молчания. Наши банки охраняют подобные секреты с усердием дракона, стерегущего вход в пещеру с сокровищами. Я так и не уразумел:

к чему вся эта детская секретность? причем здесь информационная банковская безопасность?

Не стоило бы «поднимать пургу», как сейчас модно говорить, из-за единичного случая. Но дело в том, что с такими же проблемами столкнулись все мои друзья и знакомые, связанные с российско-британскими банковскими операциями. Они не смогли получить творческие гонорары, пенсионные деньги, оплатить учебу детей и т.д. и т.п. А это уже дело серьезное

Налицо, согласно постулату старой доброй марксистской философии, «истина факта». Поэтому из единичного случая, можно сделать обобщения. А именно: в настоящее время российская и британская банковские системы элементарно не состыковываются, как не скрещиваются между собой столь похожие кролик и заяц. Справедливо отметил А. С. Пушкин: «В одну телегу впрячь не можно / Коня и трепетную лань» («Полтава», 1829 г.).

Достаточно отметить, что ведение личного банковского счета в Соеди-

ненном Королевстве принципиально отличается от существующего в нашей стране. Регистрируются четырехзначный «sort code» (порядковый номер филиала) и, собственно, номер счета. Без «sort code» британская банковская система немыслима. Это первое, о чем спрашивают клиента, основа информационной безопасности британских банков. Номер счета стоит на втором месте.

Не указав «sort code» счета получателя, и пенса не переведешь, тем более, в далекую, неведомую Россию. Попытаться растолковать сотрудникам британских банков, что на планете по имени Земля есть государства, а в них банки, не ведающие четырехзначного «sort code», дело безнадежное. Это выше их разумения.

Россияне и англичане пытаются решить подобные проблемы, пользуясь международными платежными системами, главным образом, «Western Union». Но они, увы, обеспечивают денежные переводы лишь между физическими лицами, да и берут за операции людоедский процент. Часто граждане незатейливо пересылают на-

личность в конвертах через родственников и друзей, как во времена шекспировских ростовщиков. Вот так и живем в XXI веке от Рождества Христова.

Главный вывод из сказанного: 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.

Я рассказал о сложностях участия в международном банковском общении простых трудовых россиян и англичан. Надеюсь, рассказ прозвучал познавательно. О том же, как решают банковские проблемы перекачки в Соединенное Королевство наворованных у народа денег наши бесчисленные казнокрады от Камчатки до Калининграда и «русская мафия», пусть расскажет другой автор. Я подобной информацией не располагаю.



ГОРОСКОП-2017



КОЗЕРОГ

Козерогу для достижения успеха нужно будет немало потрудиться! Звезды призывают Вас быть предельно осторожным, категорически избегать всего, что хоть как-то связано с риском.



ВОДОЛЕЙ

Этот год будет для Вас особенно плодотворным в творческом плане: возникнет множество идей и возможностей их реализовать. Но именно Вам необходимо избегать соблазна нарушить закон или общепринятые нормы – последствия таких нарушений могут быть непредсказуемыми.



РЫБЫ

Год пройдет под девизом «Дом и семья», появится возможность благоустроить жилье так, как Вы давно хотели. Если Рыбы надеются весь год спокойно плыть по течению, уповая на отлаженность своего бизнеса и надежность карьерного положения, то увы, это едва ли получится.



ОВЕН

Сфера деловых интересов может радикально перемениться: придется заняться каким-то новым направлением в бизнесе или повыситься в должности, что принесет много вопросов и стрессовых ситуаций. Ваша щедрость вернется Вам в трехкратном размере.



ТЕЛЕЦ

Тельцам год подарит поистине волшебный профессиональный успех. Прекрасное самочувствие положительно скажется на моральном самоощущении: Вы будете успешны в работе, а также чувственны и несравненны в отношениях с противоположным полом. У Вас появятся силы на физические упражнения. Не упустите момент и уделите время занятиям спортом.



БЛИЗНЕЦЫ

Личная жизнь может стать приоритетней работы и карьеры. Многим семьям предстоит преодолеть проблемы с детьми, требующих не только финансовых затрат, но и душевных сил.



РАК

Проверяйте любую поступающую информацию, особенно ту, которая кажется вам особенно неприятной. Будьте разборчивы в отношениях, доверяйте только тем, кто уже не раз помогал вам в трудные моменты. На особенно лёгкие успехи лучше не рассчитывать.



ЛЕВ

Вас ждет благоприятный и удачный год, будет возможность многому научиться, получить ценный опыт. Постарайтесь найти баланс между работой и личной жизнью, чтобы ничем не пришлось жертвовать.



ДЕВА

Год связан с переоценкой ценностей и изменением привычек. Найдутся новые способы решения старых проблем и жизнь заиграет более яркими красками. Вас ждет пополнение в семье.



ВЕСЫ

Насыщенный плодотворный год, который сложится тем лучше, чем решительнее вы будете действовать. Возможно, Ваша вторая половинка давно ждет предложения руки и сердца, не тормозите!



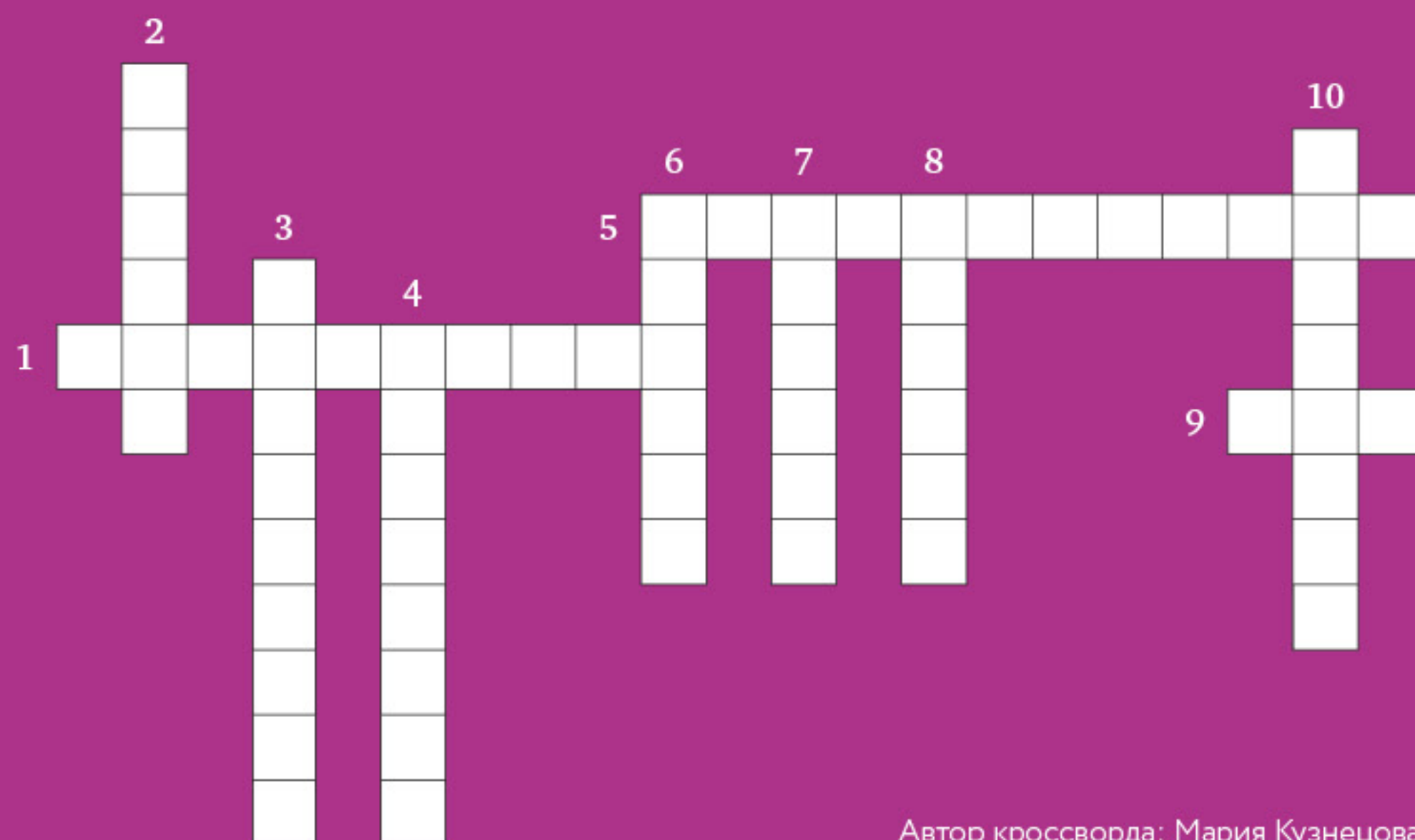
СКОРПИОН

Первые месяцы года могут показаться. Скорпионам излишне нервным и нестабильным временем на работе. Вторая половина года будет гораздо более удачной и приятной в карьерном и профессиональном плане. Следует быть очень осторожными в общении: любое неосторожное слово может привести к острому конфликту и близкие люди могут предать вас в сложной ситуации.



СТРЕЛЕЦ

Год беспокойный и интересный. Он даст вам возможность проявить себя и блеснуть талантами. Будьте внимательны к своему спутнику жизни, возможен развод. Старайтесь разумно расходовать силы и не забывайте отдыхать.



Автор кроссворда: Мария Кузнецова

КРОССВОРД

ПО ГОРИЗОНТАЛИ:

1. Искажение веб-страниц.
5. Свойство системы противостоять внешним или внутренним дестабилизирующим факторам.
9. Ошибка в компьютерной программе, которая изначально была допущена при ее разработке.

ПО ВЕРТИКАЛИ:

2. Программа, предназначенная для сокрытия в системе определенных объектов, либо активности.
3. Программа или аппаратное устройство, предназначенные для перехвата клавиатурного ввода.
4. Вид сетевой атаки, также называемый «пассивное прослушивание сети».
6. Вредоносная программа, которая осуществляет модификацию загрузочного сектора MBR.
7. Данный термин используется в смысле минимизации уязвимости средств и ресурсов.
8. Конфиденциальная информация аутентификации, обычно состоящая из строки знаков.
10. Более чем однократное использование компонента при различном выполнении операций.

БЛОГЕРЫ УЛЫБАЮТСЯ

ПРО ШТИРЛИЦА

Штирлиц послал ring. Сайт не ответил. Штирлиц послал ring по IP-адресу. Сайт не ответил. Штирлиц поехал в офис компании и толкнул ногой дверь. Дверь не открылась. Штирлиц разбежался и бросился на нее всем телом. С тем же успехом. «Файервол», — догадался Штирлиц.

ПРО АУДИТ

Проверяющий никак не мог определиться: аудит банков — это профессия или форма ведения бизнеса.

АССОЦИАЦИИ

- Одна пропущенная уязвимость, и ты — отец.
- Собака! Лайкает, а в «друзья» не пускает.
- Подидосил — и бросил.
- Аттач аттачивали, аттачивали, да недоаттачивали.
- Из резюме. Сфера деятельности: ИБ-безопасность. Уровень: Бог.

УСТАВ ИБ

Настоящий специалист по ИБ:

- всегда прав, либо рад, что не прав;
- не интересуется в DLP-системе зарплатой других сотрудников;
- знает, что канал утечки информации зависит не столько от пропускной способности канала, сколько от числа перекуров сотрудников;
- уверен, что запросы и комментарии делаются без прочтения нормативных документов, которые обсуждаются.

P. S. Просим читателей присылать недостающие пункты «Устава ИБ» для дальнейшей их публикации.

Из блога Валерия Естехина
<https://estekhin.blogspot.ru>



**Мы показываем
безопасность**
tv.ib-bank.ru



Медиа Группа «Авангард» представляет первое российское специализированное интернет-телевидение о событиях мира информационной безопасности. BIS TV всегда в центре событий, рассказывая зрителям об актуальных темах отрасли и предоставляя слово авторитетным специалистам.

BIS TV — это репортажи с ключевых мероприятий отрасли, эксклюзивные интервью о темах ИБ, практические советы и мнения экспертов, а также спецпроекты с ведущими разработчиками решений для защиты информации.

Поделитесь своим мнением, обсудите важные для вас вопросы и продемонстрируйте самые яркие моменты ваших мероприятий — в эфире BIS TV. Вас увидят и услышат сотни профессионалов в области ИБ.

BIS TV зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, номер свидетельства о регистрации ЭЛ № ФС 77 - 61377 от 10 апреля 2015 г.



АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Книжное
издательство

ib-bank.ru