BIS JOURNAL

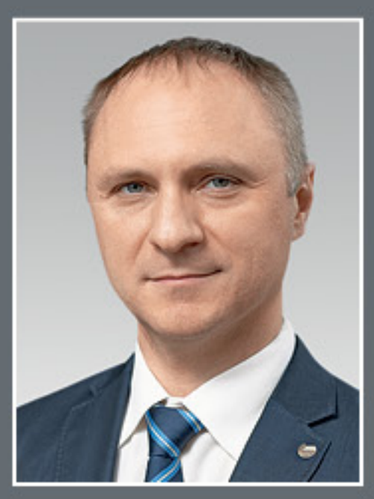
№4 (31)
2018

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ

БИОМЕТРИЯ В БАНКАХ. ЗОЛОТОЙ КЛЮЧ

16> Иван БЕРОВ
Ростелеком
ЕБС набирает высоту

29> Артем СЫЧЕВ
Банк России
167-ФЗ и 382-П: ликвидация главной бреши



36> Сергей ЛЕБЕДЬ
Сбербанк
Кибербезопасники всех стран, объединяйтесь!

49> Федор ДЗЕРЖИНСКИЙ
ТехноСофт
Банк, его аутсорсер и их работники

88> Валентин ПАНОВ
Ассоциация удостоверяющих центров
Региональные УЦ: быть или не быть?

САМАЯ МАСШТАБНАЯ КОНФЕРЕНЦИЯ В ОТРАСЛИ

SOC ФОРУМ

#SOCFORUM

ПРАКТИКА ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ
И ПОСТРОЕНИЯ ЦЕНТРОВ МОНИТОРИНГА ИБ

27–28 ноября 2018 года, г. Москва,
Конгресс-парк гостиницы
«Рэдиссон Ройал Москва»

Регистрация:
SOC-FORUM.IB-BANK.RU

Игорь НЕКРАСОВ
главный редактор
BIS Journal

По сути, история цивилизации — это перманентная флуктуация знаковых систем и технологий, словно ручейки и речки питающих море. Нынче очередной такой неожиданно большой водоем называется виртуальной реальностью. Что будет дальше — неведомо. Переплыть бы это.

Но есть проблема. Билет на пароход и другие плавсредства. Вернее, форма этого билета. Она должна быть простой, понятной и удобной для всех — проверяющих и, безусловно, предъявляющих, коих собственно миллионы и миллиарды.

Какой?

Чем масштабнее задача, тем проще должен быть велосипед. И такой примитивный велосипед, даже не велосипед, а еще проще — колесо, нашлось. Прикатилось прямиком из глубины веков.

Записав на глиняной табличке в 650 году н.э. мысль о том, что «скрепление договора отпечатком пальца есть метод для установления подлинности документа и исключения его подделки», китайский ученый Цзя Гунъянь всего лишь зафиксировал давно сложившуюся в Китае практику биометрической идентификации личности. В порядке вещей считал такую практику и пророк Мухаммед, приложив примерно в то же самое время ладонь к знаменитой ныне охранной грамоте христианского монастыря на Синае. А еще за две тысячи лет до этого точно так же считали древние ассирийцы, вавилоняне, финикийцы и египтяне. Свидетельства этому свободно лежат в археологических музеях.

А вот документы, регулирующие первые практики биометрической идентификации, растворились во времени. То же самое, надо полагать, произойдет и с Единой биометрической системой. Но сегодня она, признаем, — тренд, актуальнейшая из задач и одновременно куча проблем.

И потому именно она стала «Темой номера» этого выпуска BIS Journal.

Остановили, так сказать, мгновение истории для сиюминутной надобности.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ
Емельянов Г.В. — член-корреспондент Академии криптографии РФ, действительный государственный советник РФ 3 класса
Сычев А.М. — Первый заместитель директора Департамента информационной безопасности Банка России, кандидат технических наук, доцент
Шипилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

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

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

РЕДАКЦИЯ ЖУРНАЛА
Главный редактор: **Некрасов И.В.**
Шеф-редактор: **Былевский П.Г.**
Директор по развитию: **Минаков А.В.**
Арт-директор: **Мельников Н.С.**
Обозреватели, корреспонденты: **Бендин С.В., Северный В.П., Хвастунова О.Н., Бродская М.А., к.т.н.**
Иллюстрация на 1-й обложке: **Ларичкина О.А.**
Фото в номере: **фотобанк DepositPhotos, Салаватова Я.М., Мясоедов О.В., wikipedia.org**
Менеджер по распространению: **Кузнецова М.Д.**
Цветокорректор: **Науменко М.Б.**
Корректор: **Бальтерманц Л.Ф.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ
ООО «Медиа Группа „Авангард"»
Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д.21 (м. «Достоевская»)
Координаты: 55.779380, 37.611150
Тел./факс: +7 499 271-70-85
Интернет-версия: journal.ib-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 (Роскомнадзором). Свидетельство ПИ № ФС77–55062 от 14 августа 2013 г.
Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность банков».

Перепечатка и воспроизведение иными способами без разрешения редакции запрещаются.
При использовании материалов ссылка на журнал обязательна.
Мнение редакции может не совпадать с мнением авторов.
Присланные материалы не рецензируются и не возвращаются.

Подписан в печать 15.10.2018. Тираж 7000 экз.
Заказ № 166/8. Цена договорная.
Отпечатан в «Типографии на Угрешской»
115088 РФ, Москва, ул. Угрешская, д.2, стр.2.
Тел.+7 495 720-62-28

16+

© BIS Journal, 2018

НОВОСТИ

5 **В мире, криминал, в России**

ТЕМА НОМЕРА

10 **Биометрия в банках**
Максим Осокин (BIS Journal)
Биометрия в двух актах. Третий — через год

12 **Биометрия в банках**
Анатолий Аксаков (Государственная Дума РФ)
Дорого и сложно, но можно и нужно

16 **Биометрия в банках**
Иван Беров (ПАО «Ростелеком»)
ЕБС набирает высоту

20 **Биометрия в банках**
Артем Харченко (Тинькофф Банк)
Новые акценты — новые задачи

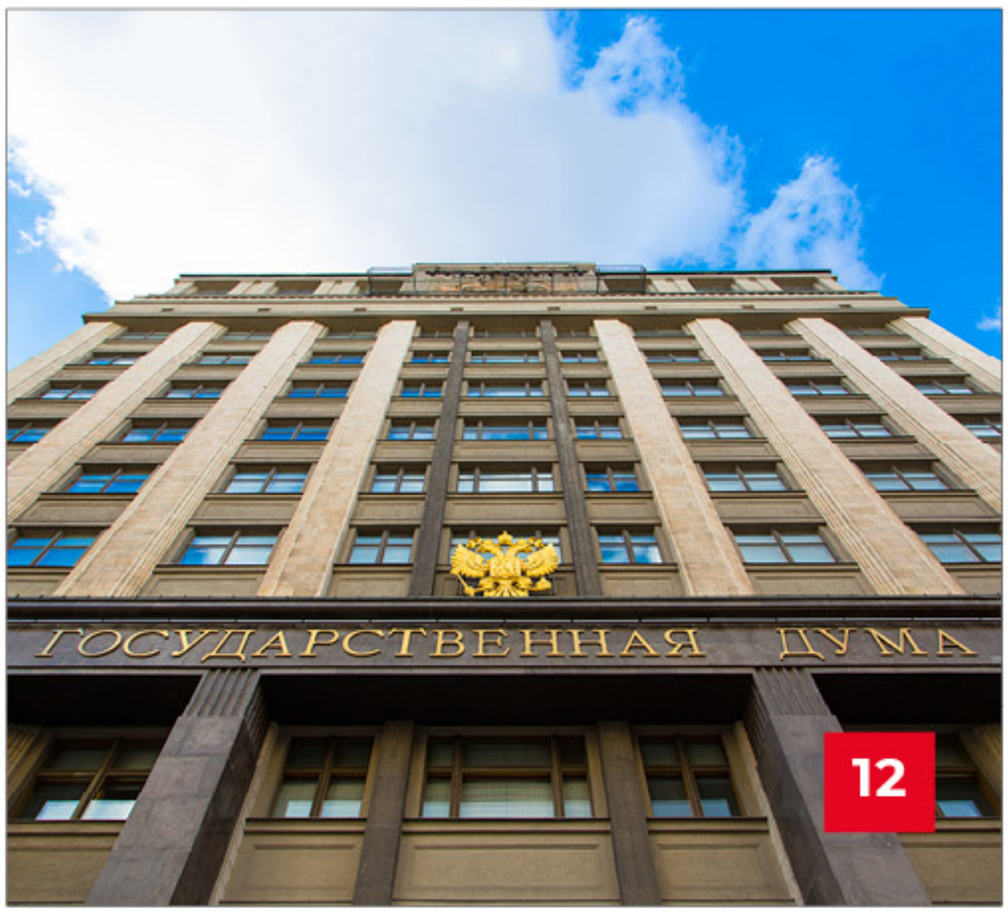
23 **Биометрия в банках**
Мирослава Бондаренко, Сергей Тихонов (РАНХиГС)
Биометрия в аутентификации

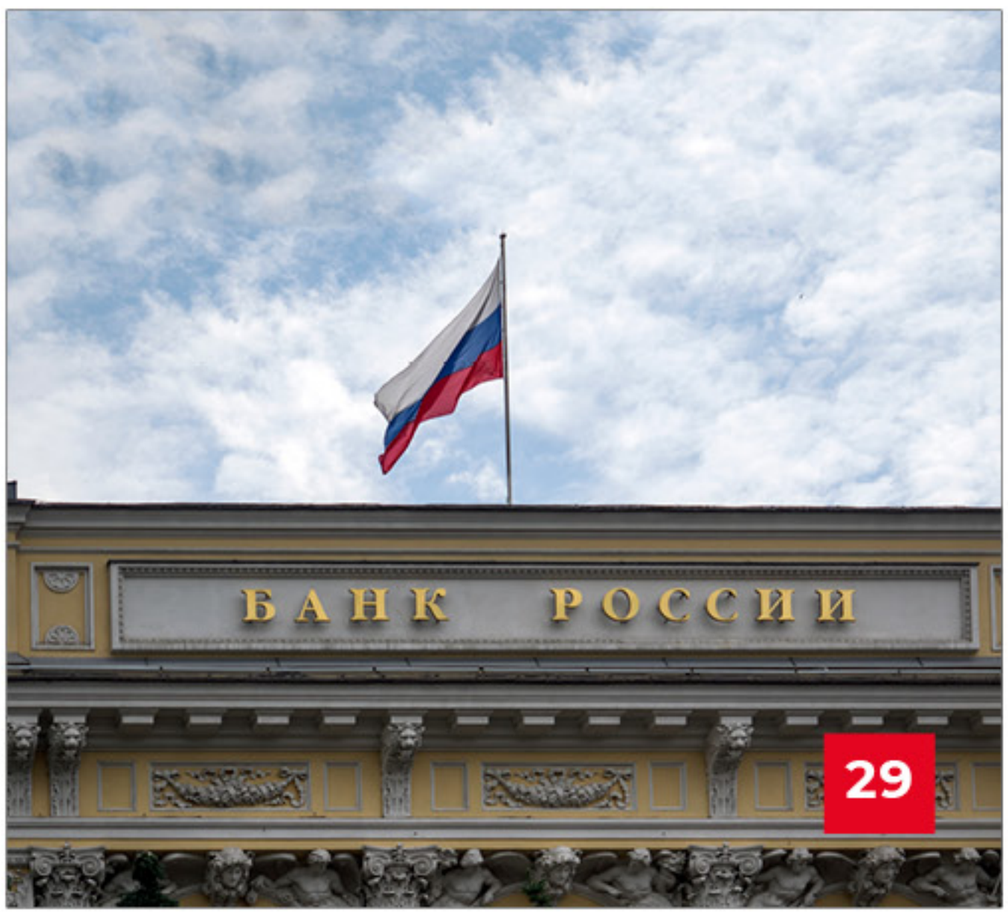
РЕГУЛЯТОРЫ

26 **Антитеррор**
Василий Пискарев (Государственная Дума РФ)
Безопасность требует ответственности

29 **Нормативно-правовая база**
Артем Сычев (Банк России)
Антифрод: нормативные новации

33 **Банк России**
Артем Калашников (Банк России)
ФинЦЕРТ и банки: обмен стал проще





БАНКИ

36 **Интервью**
Сергей Лебедь (Сбербанк)
Кибербезопасники всех стран, объединяйтесь!

40 **Мобильные операторы**
Иван Янсон (Сбербанк)
Право на ЕИСПСА

44 **Мобильные операторы**
Виктор Минин, Александр Першин (АРСИБ)
Остановить цунами

49 **Аутсорсинг**
Федор Дзержинский (ТехноСофт)
Банк, его аутсорсер, их работники и разработка банковского ПО

УГРОЗЫ И РЕШЕНИЯ

58 **СКЗИ**
Александр Веселов (С-Терра СиЭсПи)
СКЗИ в виртуальной среде

60 **Нормативная база**
Антон Свинцицкий (ДиалогНаука)
Безопасность финансов

63 **Jet CSIRT**
Алексей Мальнев (Инфосистемы Джет)
История одного сервиса

66 **Anti-APT**
Алексей Данилин (Positive Technologies)
Как обнаружить целевую атаку на банк?

68 **Стратегия развития**
Андрей Акинин (Вэб Контрол)
Не омологация продукта, а создание новых ценностей!

70 **SIEM**
Александр Дорофеев, Алексей Титов (Эшелон Технологии)
Салют, КОМРАД!

73 **КИИ**
Олег Иванов, Роман Косичкин (ЦИБИТ)
«Безопасность КИИ — не только техника»

ИНФРАСТРУКТУРА

76 Деловые мероприятия
Только наличные!

78 Деловые мероприятия
Марк Новодачный (BIS Journal)
ЦОД-2018

79 Деловые мероприятия
Николай Кольский (BIS Journal)
Дистанционный банкинг 2018

80 Деловые мероприятия
Корней Реут (BIS Journal)
BIS Summit 2018

84 Деловые мероприятия
Николай Кольский (BIS Journal)
«Штабные знают шире!»

86 Деловые мероприятия
PKI-Форум Россия

88 PKI
Валентин Панов (Ассоциация удостоверяющих центров)
Региональные удостоверяющие центры. Быть или не быть?

92 Фоторепортаж
Визит мэра

96 Обзор
София Симонова (BIS Journal)
AI, ML и ИБ

ОБРАЗОВАНИЕ И КАРЬЕРА

100 SOCи России
Александр Бодрик (ANGARA Professional Assistance)
Кадровые стратегии для SOC

103 Обзор
Анна Катанкина (BIS Journal)
Академии для гиков

105 Обзор
Марина Бродская (BIS Journal)
«На первой сессии у нас «слились» 60 % курса»

108 Молодой специалист
Валерия Мещерякова (BIS Journal)
Как я начал(а) трудовую жизнь...

СУБЪЕКТЫ

112 Корифеи
Сергей Булаев, Сергей Голованов, Дмитрий Ларин (историк криптографии)
Инженер, изобретатель, историк

114 История
Дмитрий Ларин (историк криптографии)
XV век. Время замены

119 История
Борис Столпаков (историк криптографии)
Время роста

124 Мысли вслух
Александр Бодрик (ISACA Moscow)
Уроки управления стратегическими проектами

126 BIS TV
Играют все!

128 Драматургия
Рустэм Хайретдинов (Инфовотч)
Трое и пипец

ХАКЕРЫ ВЗЯЛИ ПОД КОНТРОЛЬ БРАЗИЛЬСКИЕ БАНКИ

Хакеры модифицировали настройки DNS более 100 тыс. маршрутизаторов, тем самым перенаправив пользователей на фишинговые страницы. Порядка 88% этих маршрутизаторов находятся в Бразилии, а перенаправление осуществляется только при попытке пользователя зайти на страницы электронного банкинга бразильских финансовых организаций.

Вредоносная кампания продолжается уже как минимум с середины августа. Злоумышленники сканируют пространство бразильских IP-адресов в поисках маршрутизаторов со слабыми паролями или вообще без паролей и в настройках меняют легитимный DNS интернет-провайдера на свой собственный. Все проходящие через скомпрометированные маршрутизаторы DNS-запросы перенаправляются на DNS-серверы злоумышленников, которые отправляют некорректные данные для 52 сайтов.

В основном эти сайты представляют собой страницы бразильских банков и хостинговых сервисов. При попытке зайти на них пользователи попадают на фишинговые страницы, предназначенные для похищения их учётных данных.

АНГЛИЯ СОЗДАЁТ КИБЕРВОЙСКА

Идея создания кибервойск для противостояния угрозам со стороны России принадлежит Министерству обороны и Центру правительственной связи Великобритании, которые отвечают за ведение радиоэлектронной разведки и обеспечение защиты информации органов правительства и армии.

В состав новой структуры войдут сотрудники центра правительственной связи, военные и контрактники. По мнению экспертов, инициатива по созданию кибервойск обойдётся в 330 млн долларов.

Бывший глава Объединённого командования Вооружёнными силами Великобритании генерал Ричард Бэррон выразил мнение, что наращивание киберзможностей имеет первостепенное значение для страны в условиях, когда другие государства уже наступают.

реклама

news
все новости и блоги
представляет

НАЦИОНАЛЬНАЯ ПРЕМИЯ
ФИНАНСОВЫЙ ОЛИМП 2018

Вершина успеха!
ФИНАНСОВЫЙ ОЛИМП

01.09 – 18.11.2018 Прием заявок на участие
01.10 – 20.11.2018 Экспертный совет
27.11.2018 Международный мультимедийный пресс-центр «Россия сегодня»
Панельная дискуссия
Фуршет в честь лауреатов

Оргкомитет премии
olymp@finolymp.ru / 8 (495) 989-58-59

ГЕНПРОКУРАТУРА КОНСТАТИРОВАЛА РОСТ УЩЕРБА

В январе-августе 2018 года ущерб от преступлений в сфере компьютерной информации в России вырос почти на 44% и составил 400 млрд рублей. Об этом сообщила заместитель начальника управления взаимодействия со средствами массовой информации Генпрокуратуры РФ Татьяна Захарова.

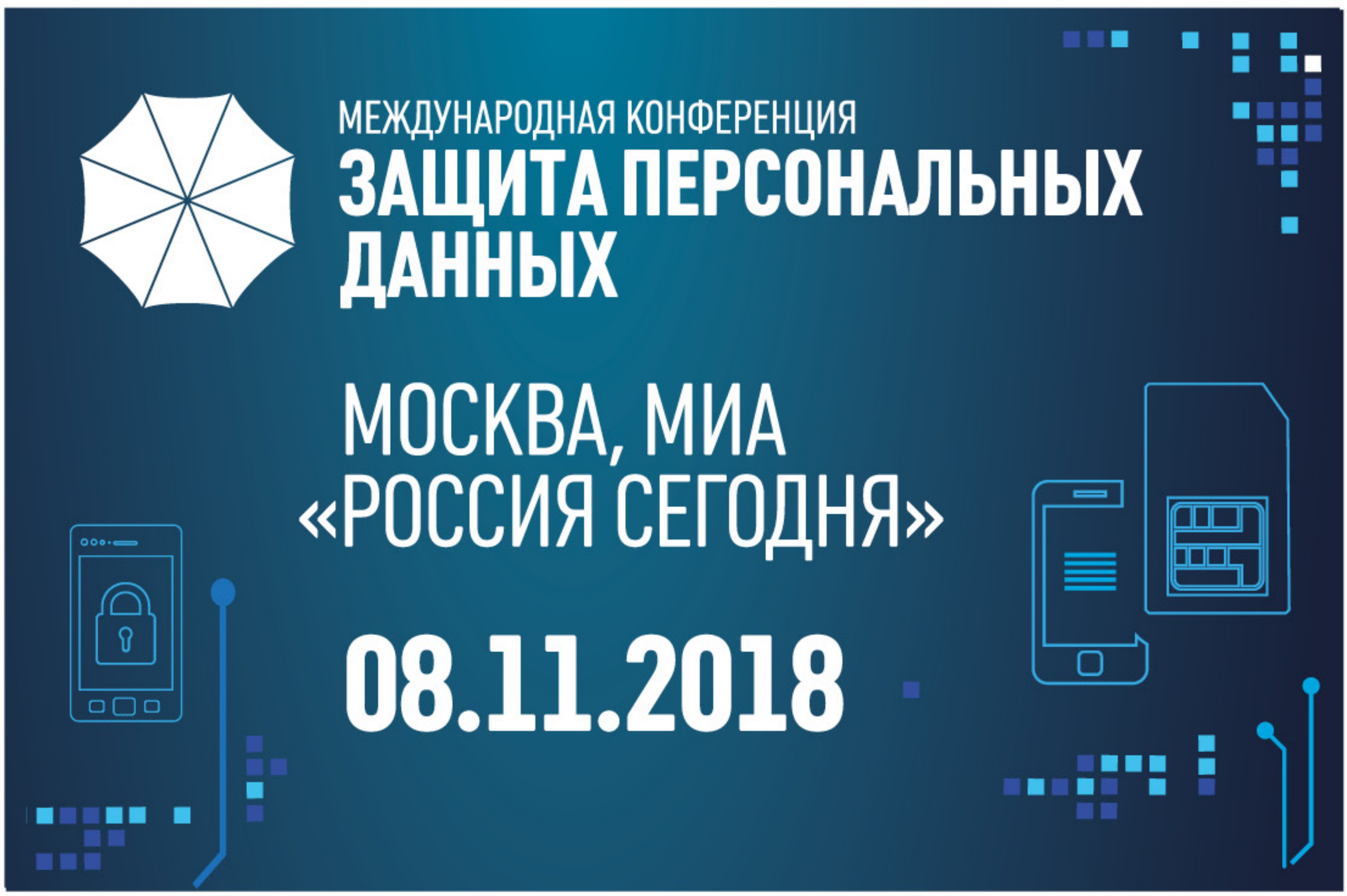
«В период с января по август 2018 года правоохранительными органами РФ зарегистрировано 107 980 преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Предварительно расследовано 28 329 такого рода преступлений. Ущерб от них составил почти 400 миллиардов рублей, что на 43,6% больше аналогичного показателя прошлого года», — заявила Захарова.

ГРУППИРОВКА COBALT ВЗЯЛАСЬ ЗА СТАРОЕ

Хакеры группировки Cobalt вывели из АО Банк «Жилфинанс» около $100 тыс. через шлюзы платёжных систем.

Подобная атака не только не характерна для этой группировки, её не использовали много лет. Причиной тому является сложность вывода крупных сумм через шлюзы платёжных систем. Платёжные системы и банки устанавливают лимиты на общий объём переводов в течение дня, на максимальный размер перевода и на количество однотипных переводов.

Хакеры из группировки Cobalt решили эту проблему, взломав автоматизированную банковскую систему, что позволило им увеличить лимиты. В итоге деньги были переведены на карты и обналичены. Доступ к банковской системе хакеры получили с помощью фишингового письма. Аналогичным способом были заражены ещё три кредитные организации. Их с «Жилфинансом» объединяют низкий уровень информационной безопасности, отсутствие российских антивирусов, лицензионного программного обеспечения и обновлений.



JETCSIRT

Центр мониторинга и реагирования на инциденты ИБ

МОНИТОРИНГ инцидентов информационной безопасности

РЕАГИРОВАНИЕ на инциденты информационной безопасности

ЭКСПЛУАТАЦИЯ средств защиты информации

JET CSIRT — ЭТО:

- Больше чем SOC.
  Экспертный аутсорсинг полного цикла
- Две модели подключения к Jet CSIRT.
  SIEM и СЗИ в инфраструктуре заказчика или в нашем защищенном облаке
- Работа с широким спектром SIEM и СЗИ
- Гибкий выбор состава услуги
- Быстрое развертывание и масштабирование

Инфосистемы Джет

+ 7 495 411 76 01
csirt@jet.su
www.jet.su

БУДЕМ ЖИТЬ ПО БАЗЕЛЮ III

Банк России обяжет банки оценивать операционные риски и подсчитывать ущерб по новому порядку. Эти требования содержатся в опубликованном на сайте регулятора проекте положения «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

Документ разработан после решения Базельского комитета по банковскому надзору, который в конце 2017 года уточнил подход к оценке операционного риска для расчёта норматива достаточности капитала в рамках стандарта Basel III.

Новый подход будет внедрен с 2022 года, однако банки должны предоставить информацию о потерях от «событий операционного риска» за последние пять лет. Также нужно привести свои системы в соответствии с новым положением к концу 2019 г.

АРМИЯ-2018

В Москве состоялся форум-выставка «Армия-2018». В этом году на нем уделялось много внимания информационной безопасности.

Первые три дня выставки были «закрытыми», и именно в это время проводились самые интересные события деловой программы для специалистов. Круглые столы и конференции охватывали самые разные аспекты «военной» темы: от обсуждения исторических деталей ВОВ до «Психологической обороны» (совместная конференция с МГУ), где внимание сосредоточилось на информационных войнах. На стендах появились новые участники — такие компании как ДиалогНаука и Позитив Технолоджиз.

Круглые столы также не обошли стороной тему ИБ: «Мы всегда защищаемся от того, что уже произошло, а стоит действовать по-другому, увеличивать темпы изменяемости системы. Проще говоря — нужно стать как хамелеон. Кроме того, очевидно, что сегодня нападают не на информацию, а на процессы управления. Отсюда еще одна проблема сферы ИБ — обучение специалистов. Нужно возвращать в университет теорию управления! Все эти и ряд других вопросов по ИБ и обсуждался на форуме на круглых столах», — рассказал профессор СПИИ РАН Борис Соколов.

Новости подготовили Анна Воробьева и Валерия Мещерякова

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АКАДЕМИЯ

КОД ИБ. АКАДЕМИЯ

500+ ВИДЕО, ПРЕЗЕНТАЦИЙ И ТЕКСТОВЫХ КОНСПЕКТОВ ПО РАЗНЫМ АСПЕКТАМ ИБ

ACADEMY.CODEIB.RU

Кибербезопасность крупного бизнеса

KASPERSKY lab

Kaspersky® Anti Targeted Attack Platform

Комплексное решение для защиты от целевых атак и сложных угроз

- Блокирование сложных угроз и снижение риска целевых атак
- Постоянный мониторинг на уровне сети и рабочих мест
- Выявление аномалий в поведении объектов IT-инфраструктуры
- Экспертное сопровождение и помощь в расследовании компьютерных инцидентов
- Оценка потенциальных рисков IT-безопасности в текущей инфраструктуре

www.kaspersky.ru/enterprise

#ИстиннаяБезопасность

© АО «Лаборатория Касперского», 2018. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей

ДиалогНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

БИОМЕТРИЯ В ДВУХ АКТАХ. ТРЕТИЙ — ЧЕРЕЗ ГОД

РЕПОРТАЖ ИЗ ОФИСА БАНКА ВТБ

Максим ОСОКИН
внештатный корреспондент BIS Journal

Я много слышал и читал про биометрию и её использование. Видел и ролик в «тюбике» с участием спонсора из «Что? Где? Когда?», видел и карикатуру «А теперь три раза скажите: хочу снять сто рублей!». Но видеть и слышать — это одно, а попробовать технологию в действии на себе — совсем другое. Это, как говорят в Одессе, две большие разницы.

АКТ ПЕРВЫЙ

Сказано — сделано. Для проведения эксперимента выбрал дополнительный офис банка ВТБ (ПАО) на Китай-городе. Расположение удобное, погода шепчет, публика ещё не отошла после ЧМ-2018.

Захожу. Слева автомат электронной очереди. Экран ностальгически напоминает о былом сложносочинённым логотипом: «ВТБ Банк Москвы». На талоне — та же картина: над номером Q305 гордо заявлено — «ВТБ Банк Москвы» (логотип ВТБ тоже старый, не «Адидас»). Становится ясным, что именно этот «документ» был взят за основу при подготовке летних санкционных списков от Госдепа США. Как иначе объяснить включение в них несуществующего уже более двух лет Банка Москвы?

Но я отвлёкся: тому, кто захочет сдать свою ~~кровь~~ биометрию, подскажу: выбирайте в автомате электронной очереди услугу «SMS и интернет услуги». Я с первого раза не догадался. Помогли работники допофиса. За это им, разумеется, спасибо!

Подошла моя очередь. Первый вопрос операционистки был: «Что вас интересует?». Я ответил. «Хотите сдать биометрию? Серьёзно? Почему? Откуда узнали?». Я сказал что-то наподобие «слышал по радио, видел ролик в Ютьюбе, да и вообще интересуюсь технологиями». После секундной заминки приступили к делу. Последовал первый вопрос: зарегистрирован ли я на Портале госуслуг? Я ответил, что нет. Проверили мой паспорт, посмотрели в компьютер. После чего поинтересовались, а есть ли у меня с собой СНИЛС. К сожалению, зелёной карточки у меня с собой не было, и номер я не помнил (как, впрочем, не помню и сейчас). Мне было предложено самостоятельно зарегистрироваться на Портале и после этого прийти к ним вновь — тогда, дескать, всё и сделаем.

Я поблагодарил всех участниц процесса за проявленную готовность помочь (подтянулись ещё работницы допофиса) и попрощался.

Вышел на улицу. Погода продолжала шептать (правда, как-то неразборчиво)…

АКТ ВТОРОЙ

Итак, прошло несколько дней. Я зарегистрировался на Портале госуслуг. Даже установил на смартфон соответствующее мобильное приложение. Справедливости ради должен отметить, что приложение попало в ряд немногих, не вызывающих стойкого раздражения с первых минут своего использования. Но сейчас не об этом…

Как в своё время выразился поэт, «и вновь я посетил…» офис банка. На этот раз я уверенно обращался с автоматом электронной очереди. И это было очень даже кстати, т.к. на этот раз все помещение допофиса было заполнено уверенными мужчинами. Нет, я не о клиентах, которые пришли сдать свои биометрические данные, я — о работниках банка. На этот раз все — мужчины. Случайность это или нет, но про себя этот факт я отметил.

Вскоре меня пригласили. На этот раз никто не удивился тому, что я решился на «сдачу биометрии». Работник банка деловито взял мой паспорт, уточнил насчёт регистрации на Портале госуслуг.

Как мы себе представляем новые технологии? Что-то такое технически-фантастическое, тумблеры-индикаторы и т.п. А тут — всё просто! На столе операциониста на небольшой подставке на резиновых растяжках закреплён микрофон. Рядом со столом на фотоштативе закреплена веб-камера. Названий того и другого я не увидел. По виду — ничего фантастического. Причём камера закреплена с лёгким перекосом по горизонтали. Исправить это затяжкой крепления не получается. Ну да ладно…

Начали с соблюдения формальностей — согласие гражданина на обработку биометрических данных. Здесь всё понятно и малоинтересно. Моё согласие получили Министерство цифрового развития, связи и массовых коммуникаций РФ, Банк ВТБ и Ростелеком.

Приступаем. Начинаем с записи голоса. Передо мной листочек с тремя рядами цифр: от 1 до 0, в обратном порядке — от 0 до 1 и в некоем произвольном порядке без повторений. Так как тут записывался голос, то команду на начало чтения мне давали беззвучно — кивком головы. После окончания чтения некоторое время идёт на обработку записи на удалённом сервере. Результат (оценка качества) высвечивается на экране оператора.

С первого раза не получилось. Слишком тихо — надо погромче.

Повторил. Ждём результат. Снова неудача — слишком медленно, надо побыстрее.

С третьего раза — успех! Как говорится, Бог Троицу любит…

Теперь изображение. Оператор (строго говоря — работник в должности Главный финансовый консультант) как заправский фотограф просит меня придвинуться, повернуть голову, опустить подбородок. Результаты этих манипуляций оператор наблюдает в режиме реального времени на экране компьютера.

Минуточку… Пришёл ответ от удалённого сервера: результат неутешителен. Вновь корректируем положение головы — и вновь неудача. То же и в третий раз. Как я понял, проблемы возникали из-за недостаточной «горизонтальности» линии глаз.

Я уже упоминал, что камера удерживалась на штативе с лёгким перекосом. Вместе с Главным финансовым консультантом решили скомпенсировать этот перекос регулировкой длины ножек фотоштатива. Тут уж не знаю — то ли это помогло, то ли ещё что-то, но на этот раз (четвёртая попытка) всё закончилось успешно. Это обрадовало нас обоих! Мой визави удовлетворённо сообщил, что сегодня был ещё один желающий «сдать биометрию». У него сдать изображение получилось только с восьмой попытки (!).

Выскажу свое предположение/предложение (с ним согласился и Главный финансовый консультант): если бы на экране компьютера на изображение клиента накладывалась сетка из горизонтальных и вертикальных линий (как во всех современных фотоаппаратах и даже смартфонах), добиться качественного результата было бы намного проще (и быстрее!).

Ведём непринуждённый разговор с Главным финансовым консультантом.

— Много ли желающих «сдать биометрию»? — спросил я.

— Нет, 2–3 человека в неделю. Но вот сегодня — наплыв. С вами — два человека.

— А можно ли прямо сейчас попробовать систему в действии?

— Нет, сейчас идёт процесс сбора данных, следующий этап наступит только в 2019 году.

На этом содержательная часть завершилась, но моё общение с Главным финансовым консультантом не окончилось. Мне были предложены банковские продукты. Хит сезона — Мультикарта. Я вежливо ознакомился с предложением и взял время на размышление. На том и расстались. На всё ушло 50 минут.

* * *

Итак, «биометрия сдана». Но как это работает? Об этом надеюсь узнать в следующем году. Как говорится, продолжение следует.

ДОРОГО И СЛОЖНО, НО МОЖНО И НУЖНО

ОСОБЕННОСТИ ВЫПОЛНЕНИЯ ФИНАНСОВЫМИ ОРГАНИЗАЦИЯМИ НОРМ БЕЗОПАСНОСТИ РАБОТЫ С БИОМЕТРИЧЕСКИМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Анатолий АКСАКОВ
председатель Комитета Государственной Думы РФ по финансовому рынку

Федеральный закон от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» регулирует, как организации финансовой сферы должны обеспечивать безопасность работы с биометрическими данными граждан. Для информирования участников отрасли об оптимальном решении вопросов, возникающих на этом пути, проводятся различные мероприятия. Одним из них стало совещание в ПАО «Ростелеком» — официальном операторе Единой биометрической системы (ЕБС), проведённое в конце лета 2018 года.

БИОМЕТРИЯ: И УДОБСТВА, И БЕЗОПАСНОСТЬ

Интерес финансовых организаций к вопросам безопасности работы с биометрией понятен: от своевременных ответов на них зависит многое. Информационные технологии в финансовой сфере выполняют всё больше функций, помогают при помощи новых математических моделей и алгоритмов более широко оптимизировать бизнес-процессы. Но высокотехнологичному банку, применяющему цифровые технологии, приходится уделять повышенное внимание их безопасности.

Внедрение системы биометрической идентификации и аутентификации позволяет не только сокращать издержки на операционную деятельность, ускорять проведение транзакций и предоставлять клиентам новые сервисы. Есть и такой плюс, как снятие ряда информационных рисков. Например, возможностей компрометации пользовательского пароля или PIN-кода, которые злоумышленники могут подобрать или прочитать в случае неосторожной записи на видном месте.

Для финансовых организаций важно и выполнение требований информационной безопасности к работе с самими биометрическими данными. Каждой организации необходимо выстроить систему защиты информации, которая должна соответствовать как общим законодательным требованиям, так и учитывать специфику обрабатываемых биометрических персональных данных. Эти данные являются наиболее чувствительными к нарушениям режима обработки и потому подлежат усиленной защите.

Все эти вопросы требуют детальной проработки и очень аккуратной реализации. Чтобы получать «обратную связь» и давать ответы на вопросы, возникающие у финансовых организаций, проводятся различные мероприятия. Одним из них стало проведённое в конце лета 2018 года совещание ПАО «Ростелеком», который является официальным оператором Единой биометрической системы (ЕБС).

МНОГОСТОРОНЕЕ РЕГУЛИРОВАНИЕ

Одна из причин многочисленных вопросов, возникших у финансовых организаций, в том, что дистанционная биометрическая идентификация физических лиц регулируется не только ФЗ-482, который устанавливает базовый механизм. Также существуют многочисленные подзаконные требования государственных ведомств — регуляторов информационной безопасности ФСБ России и ФСТЭК России. Кроме того, есть отраслевой государственный регулятор финансовой сферы — Банк России, который тоже формулирует свои требования по обеспечению информационной безопасности.

Подробнее. Применение дистанционной удаленной идентификации клиентов в финансовой сфере в своих основных чертах регламентировано Федеральным законом № 482-ФЗ от 31 декабря 2017 года. Этим актом были внесены изменения сразу в несколько других федеральных законов: № 115-ФЗ «О противодействии легализации…», № 149-ФЗ «Об информации…», № 126-ФЗ «О связи» и № 152-ФЗ «О персональных данных».

Кроме того, был определен круг необходимых для принятия подзаконных актов — всего более двадцати. Соответственно главные регуляторные требования к системе защиты информации и технической реализации ЕБС были установлены именно на подзаконном уровне — Правительством РФ, Минкомсвязи РФ, ФСБ России, ФСТЭК России и Банком России. Таким образом, «удельный вес» требований, содержащихся в подзаконных нормативных актах регуляторов, существенно выше, чем законодательных.

Не могу не отметить, что на стадии обсуждения законопроекта и депутаты, и государственные регуляторы по ряду аспектов предлагали более мягкие требования, чем закрепленные в итоге в подзаконных ведомственных нормативных актах. Ужесточение было вызвано необходимостью более тщательно контролировать риски при обработке биометрических персональных данных. Но, как следствие, привело к усложнению процесса технической реализации установленных требований и удорожанию этого процесса.

Основные трудности для кредитных организаций при внедрении дистанционной биометрии заключаются в том, что необходимо выполнить все требования к информационной безопасности. Учесть сразу несколько нормативных актов, скоординировать с ними организационно-технические решения и при этом уложиться в сжатые сроки.

Главные регуляторные требования к системе защиты информации и технической реализации ЕБС были установлены именно на подзаконном уровне — Правительством РФ, Минкомсвязью РФ, ФСБ России, ФСТЭК России и Банком России

ЦЕЙТНОТ ПРЕОДОЛИМ

Ситуация усложняется тем, что подзаконная нормативная база, призванная урегулировать сбор, обработку и передачу биометрических персональных данных, продолжает находиться в стадии технической и юридической доработки. В этой связи завершение всех необходимых мероприятий в 20% офисов в установленный срок, не позднее 31 декабря 2018 года, представляется непростой задачей для любого банка.

Есть мнение участников рынка, что снять остроту цейтнота можно было бы, сократив число банков, обязанных осуществлять съем биометрических образцов, до, например, ста крупнейших. Предоставив таким образом другим банкам возможность делать это на своё усмотрение, или к более поздней дате.

Также предлагается вернуться к более гибкой модели нормативного регулирования доли офисов, в которых банки обязаны обеспечить снятие биометрии в каждом регионе присутствия. А именно дать банкам возможность самим выбрать офисы, наиболее технически подготовленные и экономически подходящие для этого. Такая возможность обсуждалась в ходе работы над ФЗ-482 на стадии законопроекта.

Представители финансовых организаций формулируют и ряд других проблем: не доверенную среду пользователей, угрозу заражения мобильных устройств и компьютеров через интернет, возможные уязвимости средств защиты, встроенных в программные продукты разработчиками систем дистанционного банковского обслуживания и интернет-банкинга.

Еще одна важная проблема — использование злоумышленниками для атаки на клиентов финансовых организаций социальной инженерии, попросту мошенничества. Чтобы противодействовать таким покушениям, крайне важна осведомлённость пользователей о необходимости выполнения элементарных требований личной компьютерной безопасности.

ЦЕНА ВОПРОСА ПРИЕМЛЕМА

Многие структурные подразделения, офисы кредитно-финансовых организаций пока не располагают техническими условиями, необходимыми для обеспечения требуемого класса защиты информации. В ряде случаев применение таких решений для получения биометрических образцов оказывается слишком дорогостоящим, что ставит под вопрос экономическую целесообразность.

Насколько значительны и посильны для участников финансового рынка затраты на соответствие законодательству о биометрии и соответствующей нормативной базе? Участникам проведённого в Ростелекоме со-

BIS-КОММЕНТАРИЙ

Глава Национального совета финансового рынка (НСФР) Андрей Емелин обратился в Госдуму с предложением собирать биометрию не всем банкам. Например, освободить от этого банки, ориентированные на корпоративных клиентов и обслуживание ипотеки, а также те отделения, где нет такой технической возможности. BIS Journal обратился за комментариями к экспертам.

— Почему не сразу стали говорить о том, что для многих банков биометрия не по карману?

Татьяна Станкевич, менеджер по продукту ООО «Газинформсервис»: На этапе пилота банки часто не задумываются о том, какие реальные затраты повлечет промышленная эксплуатация системы. По долгу службы часто сталкиваюсь с этим. При запуске любого пилота я сразу говорю заказчику, сколько ему будет стоить эксплуатация системы в будущем. К сожалению, ЕБС — не мой проект.

Михаил Савельев, директор по развитию бизнеса компании «Информзащита»: Считать чужие деньги — неблагодарное занятие. Но в данном случае предпосылки для этого имеются. Расстановка систем снятия биометрических данных, их обслуживание, изменение процессов — все это затраты. А вот позволит ли внедренная биометрия сократить издержки настолько, чтобы появился экономический эффект — вопрос. Особенно в ситуации, когда для клиента — это дело добровольное.

— Согласны ли вы, что не все банки должны собирать биометрию?

Татьяна Станкевич: Получение ипотеки или денежных средств для бизнеса удобно оформить при личной явке в банк, поскольку речь идет, как правило, о значительных суммах. А вот потребительские кредиты банк может выдавать и удаленно, так как в случае компрометации аутентификационной пользовательской информации, страховка покроет ущерб.

Михаил Савельев: Тут главную роль должна сыграть «невидимая» рука рынка. Время покажет, дает ли новая технология конкурентные преимущества? Сегодня важнее другая проблема: услуга мало востребована, люди не торопятся сдавать свои биометрические данные. Причины традиционные: недостаток информации, недоверие к нововведениям… Преимущества биометрии еще нужно доказать, объяснить, внедрить в сознание. На примере портала «Госуслуги» прекрасно видно, что привыкание к новой технологии такого уровня и масштаба длится несколько лет.

— Давайте подробнее, почему так мало людей регистрируется в ЕБС? Что нужно сделать, чтобы это исправить?

Татьяна Станкевич: Малое число граждан регистрируется в ЕБС по следующим причинам: во-первых, система запущена недавно. Во-вторых, не многие доверяют биометрической иден-

вещания был представлен базовый перечень элементов, необходимых для сбора биометрических данных. В него входят: сервер с HSM-модулем, операционная система и средства подписи снимаемой биометрии, антивирусное программное обеспечение и межсетевой экран.

Перечень базовых элементов позволяет рассчитать минимальные затраты. Так, для сбора биометрических данных и отправки их в ЕБС цена подключения банка с одним отделением начинается с 3 млн рублей. Из этой суммы на киберзащиту приходится половина затрат, так как один HSM-модуль стоит 1,5 млн рублей. Остальные расходы связаны с покупкой оборудования для снятия биометрических данных и передачи их в ЕБС.

За каждое следующее отделение придется доплатить примерно 130 тыс. рублей, из которых 30 тыс. рублей — это средства защиты, 60 тыс. рублей — оборудование для снятия биометрических данных для одного рабочего места, 40 тыс. рублей — производительный компьютер для сотрудника. Кроме того, работы по настройке оборудования, аттестация системы ЕБС, разработка модели угроз и модели нарушений, а также годовое обслуживание потребуют еще около 1,2 млн рублей. Большую часть из них, около 800 тыс. рублей, составляет стоимость годового обслуживания. В целом, такие затраты для основной части банков представляются посильными и обоснованными.

* * *

Специалисты Государственной Думы РФ ведут постоянный мониторинг всех перечисленных вопросов. Предложения, поступающие от участников финансовой сферы, готовятся и обсуждаются с профильными государственными регуляторами. Создаваемая единая система дистанционной биометрической идентификации и аутентификации клиентов — важное и перспективное новшество для финансовой сферы. Цель нашей работы в том, чтобы результаты для всех — и граждан, и государства, и банков — оказались наилучшими при максимальной защищенности и разумных затратах.

тификации, ведь со временем голос и лицо меняются. Это может быть связано с возрастными изменениями голосовых связок, с простудой, колебанием веса. Контур лица может меняться, например, при наборе массы или похудении, после травмы. Есть боязнь и несанкционированного использования биометрических данных, ведь большая часть населения не является технически грамотной в этой сфере. Посмотрите на рынок инфраструктуры открытых ключей. Сколько он существует и сколько там пользователей — физических лиц?

Михаил Савельев: С другой стороны, апробация технологии идет в центральных офисах банков, а, на мой взгляд, востребована эта услуга будет скорее в регионах. Первыми потребителями любых ноу-хау всегда становятся люди, и без того активно использующие передовые технологии. А у тех, кому данная услуга наиболее вероятно нужна, порой нет гаджетов с хорошей камерой и мало доступен мобильный интернет.

Ко всему прочему, даже в сообществе безопасников сильны сомнения. Голос и лицо — это то, что сегодня легко смоделировать. Любой может найти в интернете информацию о стартапах, занимающихся восстановлением 3D-структуры лица по фотографиям. Уже есть нейросети, способные заменить лицо персонажа в видеоролике на любое другое. Да, пока качество таких «поделок» низкое, но благодаря machine learning оно на глазах повышается. В результате вопрос создания качественной подделки для биометрии упирается только в вычислительные мощности и затраченное время. Хуже всего то, что компрометация биометрических параметров — фатальна, так как сменить их человек не в состоянии. Сейчас люди выкладывают в социальные сети столько фотографий, что их с лихвой хватит на создание десятков и сотен тысяч, если не миллионов цифровых двойников.

Кроме того, банки итак предоставляют своим клиентам множество сервисов дистанционно, через call-центры и мобильные приложения, к слову, давно используя биометрию как дополнительный фактор для идентификации. Так что убеждение людей в том, что нужно использовать новый метод, потребует заметных усилий.

На мой взгляд, для продвижения ЕБС надо проводить регулярные разъяснительные работы с населением, причем с детальной демонстрацией безопасности этих технологий.

* * *

Напомним, сбор биометрии является обязательным для всех банков, соответствующих установленным законом критериям. К банкам, не выполняющим требования закона о переходе 20% отделений на сбор биометрии к 1 января 2019 года, будут применяться меры, предусмотренные ст. 74 закона о ЦБ. Функция по надзору за сбором биометрии закреплена за регулятором.

ЕБС НАБИРАЕТ ВЫСОТУ

КАК БИОМЕТРИЯ СТАНОВИТСЯ ЧАСТЬЮ ЖИЗНИ В РОССИИ

Иван БЕРОВ
директор по цифровой идентичности ПАО «Ростелеком», руководитель направления по развитию удаленной идентификации и цифровому профилю ассоциации ФинТех

30 июня «Ростелеком» запустил «Единую биометрическую систему» (ЕБС), до конца 2019 году к ней подключатся все российские банки. Использование биометрии будет выгодно и банкам, и пользователям, и государству.

БИОМЕТРИЯ ПОВСЮДУ

Биометрия — это идентификация человека по уникальным биологическим и поведенческим характеристикам. Самые распространённые типы биометрии — отпечаток пальца, радужка глаза, изображение лица и голос. Большинство пользователей уже использует биометрию — почти все новые смартфоны разблокируются отпечатком пальца или снимком лица. Эти технологии используются всё чаще в различных отраслях от ритейла до государственных услуг. Главные преимущества набирающей популярность биометрии — удобство для пользователей, выгода и безопасность для бизнеса.

В 2017 году Правительство РФ приняло программу «Цифровая экономика РФ», её основная цель — развитие цифровых платформ и систем информационной безопасности. «Единая биометрическая система» была разработана в рамках данной программы, это — цифровая платформа, которая позволяет подтвердить личность человека удалённо по голосу и лицу. С её помощью граждане могут оформить кредит или открыть счёт в банке, не выходя из дома или из другой страны через интернет. Главная цель системы — повысить доступность услуг, требующих подтверждения личности.

Создать свой цифровой образ уже можно более чем в 120 городах России, с системой взаимодействует более 100 банков. До конца 2019 года горожане смогут создать цифровой образ в любом отделении банка.

Сегодня воспользоваться дистанционными услугами с помощью биометрии можно в нескольких крупнейших банках. Для этого они встроили интерфейс «Ключ Ростелеком» в свои интернет-банки и мобильные приложения.

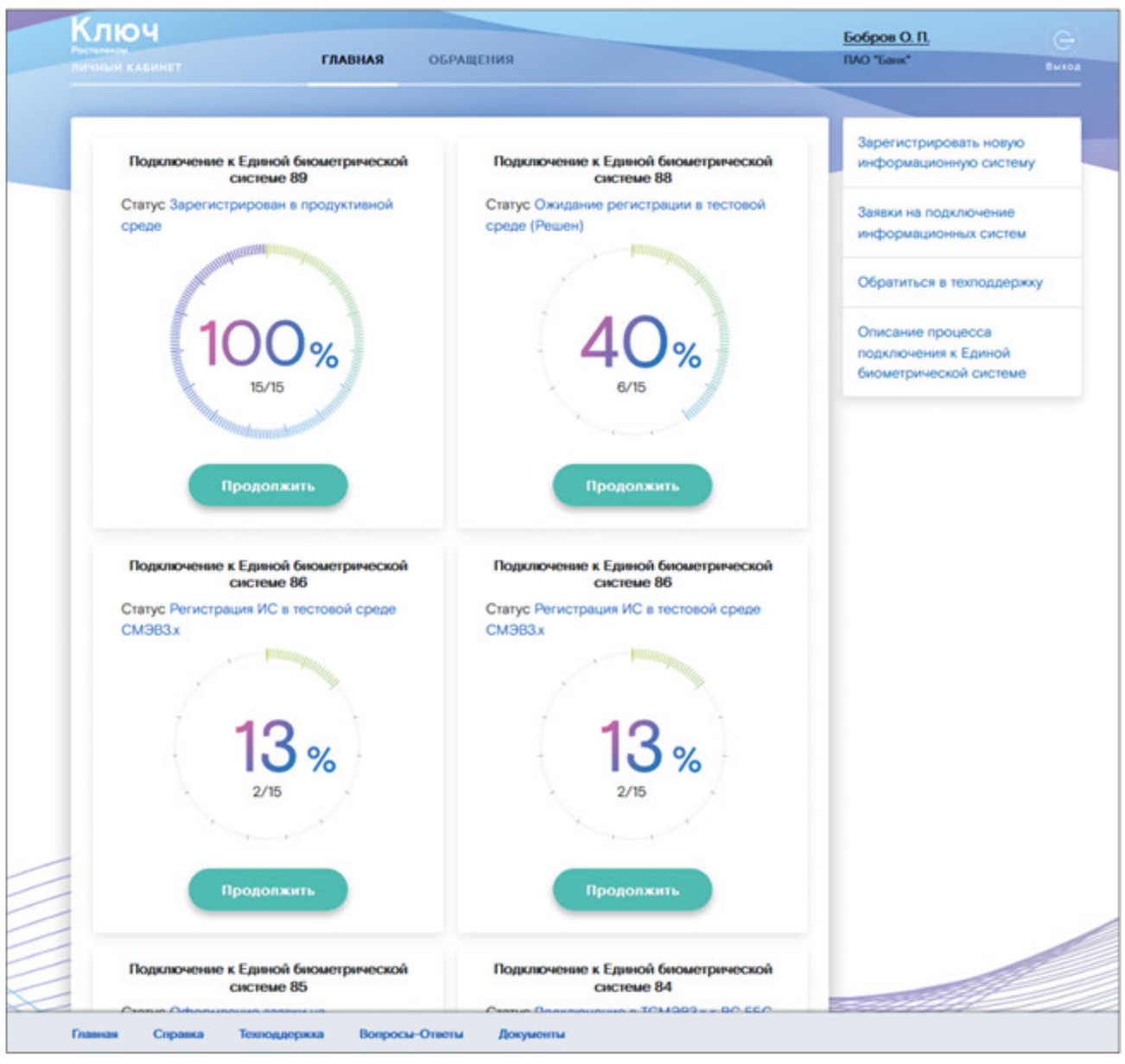


Рисунок 1. Личный кабинет кредитной организации на портале bio.rt.ru

ЦБ ОБЯЗАЛ, «РОСТЕЛЕКОМ» ПОДДЕРЖАЛ

По закону к концу этого года банки должны подключить к системе 20% своих отделений, к июлю 2019–60%, а к декабрю 2019 каждое отделение. Срок довольно короткий, особенно — для банков со множеством отделений, поэтому «Ростелеком» разработал несколько инструментов, которые помогут банкам регистрировать граждан и подключиться к системе.

Личный кабинет. На портале bio.rt.ru помимо документов и общей информации представители банков могут воспользоваться личным кабинетом, где описана последовательность действий, необходимых для подключения к Единой биометрической системе (рис. 1). Если раньше специалистам банков приходилось писать вопросы на почту техподдержки и долго ждать ответа, то теперь сотрудник поддержи быстро отвечает в чате на сайте. В ближайшее время в личном кабинете появится возможность отслеживать статистику зарегистрированных граждан и удалённых идентификацией, а также проводить взаиморасчёты с «Ростелекомом».

Модуль «Ассистент» и библиотека контроля качества. Библиотека для контроля качества собранных данных (БКК) проверяет и оценивает собранные в банках образцы до их отправки

в Единую биометрическую систему. С помощью бесплатного модуля «Ассистент» можно убедиться, что при фотографировании соблюдены необходимые условия. В режиме реального времени «Ассистент» оценивает наклон головы, углы поворота, освещённость, положение глаз, в некоторых случаях — мимику человека (рис. 2–3).

Типовое решение по ИБ. Типовое решение по информационной безопасности позволит банку встроить готовый программно-аппаратный комплекс в инфраструктуру, выполнив большую часть нормативных требований регуляторов (рис. 4). Использование типового решения позволит банку не проводить тематического исследования кода программной части криптографической защиты — исследования входят в типовое решение вместе с настройкой.

В состав типового решения входит:

- Программно-аппаратный комплекс HSM класса КВ 2
- Сервер с сертифицированной по требованиям ФСТЭК операционной системой
- Межсетевой экран класса 4 по требованиям ФСБ
- Система обнаружения вторжений класса Б
- TLS-клюз с поддержкой ГОСТ (класса КС3)
- Антивирус класса Б2
- Аппаратно-программный модуль доверенной загрузки (АПМДЗ)
- Специальное программное обеспечения для подписания биометрического образца электронной подписью

Типовое решение будет реализовано в четырёх комплектациях: два варианта производительности решения и два типа отказоустойчивого оборудования.

«Ростелеком» проектирует решение вместе с разработчиками продуктов по информационной безопасности и системными интеграторами, согласовывает его с ФСБ России.

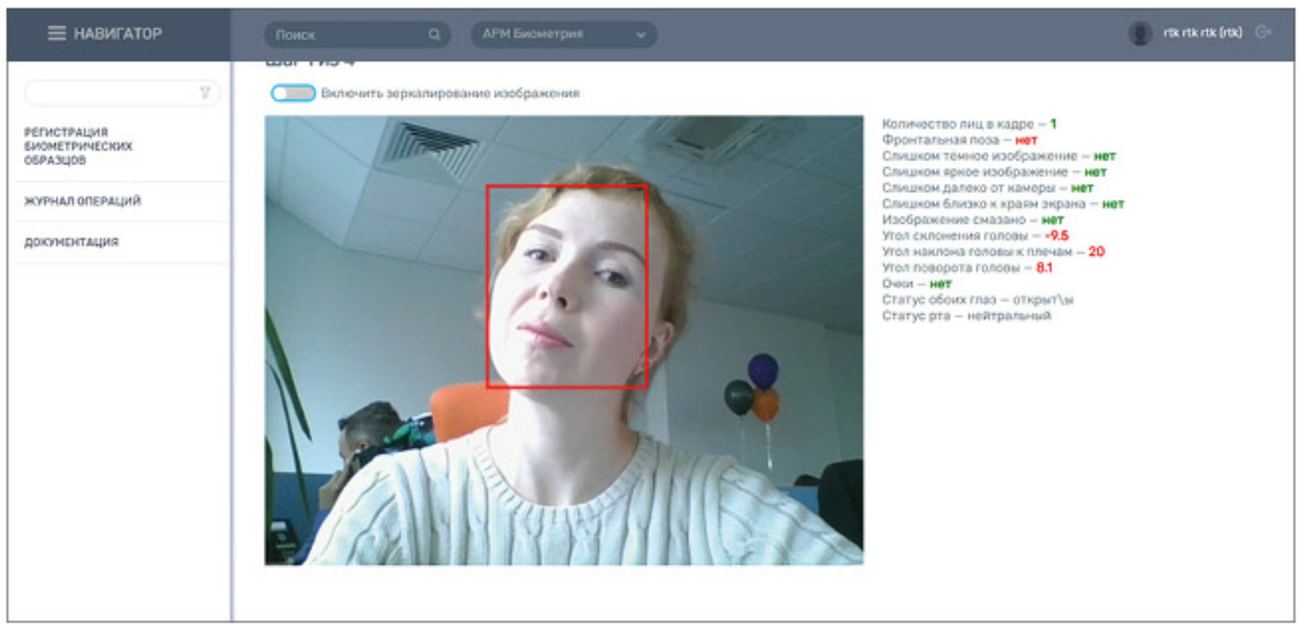


Рисунок 2. Ошибки фотографии проверяются с помощью модуля «Ассистент»

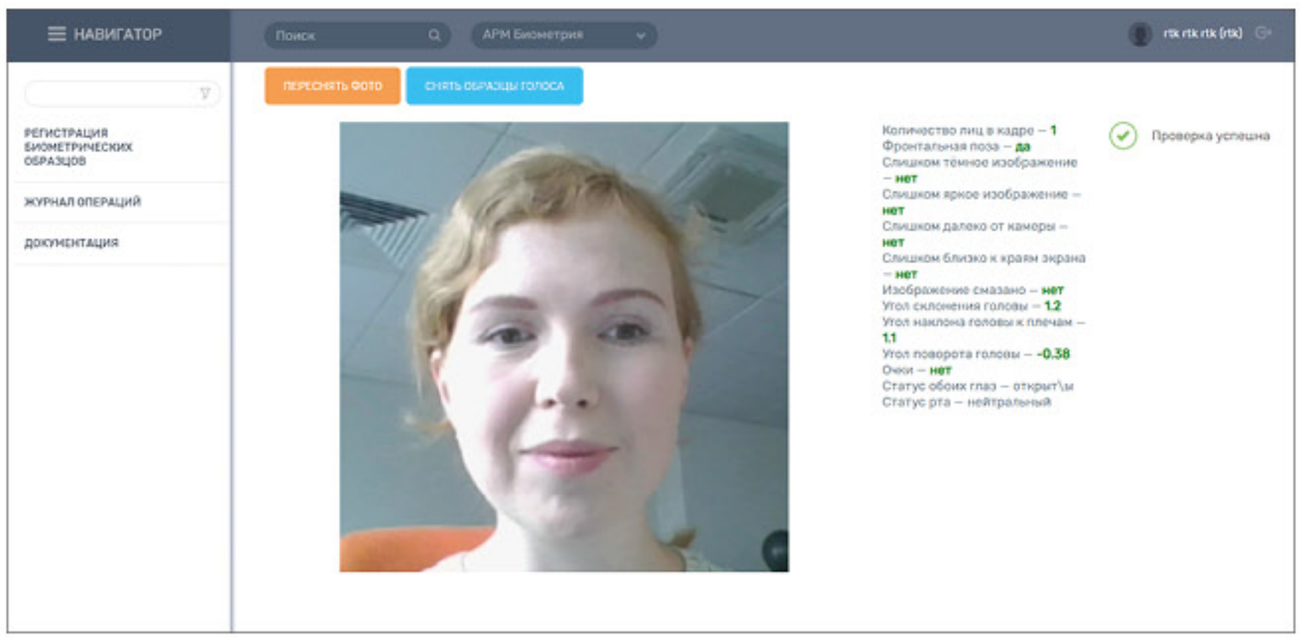


Рисунок 3. Фотография без ошибок. Проверка модулем «Ассистент»

«Ключ Ростелеком». В мобильном приложении «Ключ Ростелеком» клиенты могут пройти удаленную идентификацию. При обращении в мобильное приложение банка пользователь может выбрать услугу и способ ее предоставления. При выборе удалённой идентификации из приложения банка пользователя «перебрасывает» в «Ключ Ростелеком», где осуществляется сбор и передача видео. Вся работа с биометрией проводится в приложе-

Рисунок 4. Задачи в области информационной безопасности на этапе сбора биометрических данных

нии «Ростелекома», банк только получает результат сравнения биометрических данных с образцом в виде процента схожести видео пользователя с фотографией и записью голоса из шаблона. Таким образом «Ростелеком» снимает с банков часть работы и помогает минимизировать изменение бизнес-процессов в банке.

Персональный аккаунт-менеджер «Ростелекома». При подключении банка к ЕБС, «Ростелеком» закрепляет за проектной командой банка персонального менеджера, который помогает специалистам банка быстро подключиться к системе.

ЗАКОНОДАТЕЛЬСТВО НЕ БЫЛО ГОТОВО

При создании системы самой большой проблемой стала юридическая легитимация процессов: чтобы юридически подготовить применение биометрии для открытия счетов и кредитов, потребовался год работы «Ростелекома» совместно с Центральным Банком, Министерством цифрового развития, коммуникаций и связи и другими организациями. Было подготовлено множество нормативно-правовых актов, разработан ФЗ № 482, некоторые юридические аспекты до сих пор изменяются и дополняются.

BIS-КОММЕНТАРИЙ

Марина ФРОЛОВА
заместитель директора
по операционной деятельности
Росбанка

Разработка Единой биометрической системы (ЕБС) была полностью профинансирована Ростелекомом, оборудование для сбора биометрических данных приобретается и обслуживается банками самостоятельно с учётом требований, предъявляемых Министерством цифрового развития, связи и массовых коммуникаций РФ. Для запуска и использования сервиса сотрудники Росбанка прошли специальное обучение.

Итогом проделанной работы стал запуск 1 июля в офисах Росбанка сервиса по сбору и передаче биометрических данных граждан РФ в Единую биометрическую систему. 62 отделения Росбанка, расположенные в 34 регионах присутствия банка (40 городов по всей России), готовы принять и направить биометрические данные клиентов в ЕБС. До окончания 2018 года к системе будет подключено ещё более 40 отделений Росбанка.

После Москвы наибольшей популярностью услуга пользовалась в Приморском и Хабаровском крае. Жители г. Артёма, Находки и Хабаровска стали абсолютными лидерами по сдаче биометрии в отделениях Росбанка. В десятку городов, наиболее активно осваивающих систему, вошли Нижний Новгород, Красноярск, Екатеринбург и Улан-Удэ.

Система использования биометрических данных открывает огромные возможности по усовершенствованию и ускорению процесса взаимодействия с клиентом — от идентификации до продажи продуктов, поэтому банки активно поддерживают проект. Кроме того, это даёт преимущества не только жителям больших городов, но и — в большей степени — маленьких удалённых посёлков, где традиционно не очень широк выбор банковских отделений. Мы также ожидаем, что этот сервис повысит доступность финансовых услуг для маломобильных граждан. Наличие биометрических данных в ЕБС исключит необходимость личного посещения отделения и даст возможность пользоваться услугами любого банка, предоставляющего услуги с помощью удалённой идентификации, независимо от того, открыто его отделение в конкретном городе или нет.

Для Росбанка одним из главных цифровых проектов этого года является потребительский онлайн-кредит, который можно получить без бумажного договора и посещения отделения. Технология протестирована и уже доступна некоторым зарплатным клиентам банка. Весь процесс оформления кредита занимает 10–15 минут и деньги начисляются сразу на счёт клиента. В скором времени этот продукт станет доступен другим клиентским сегментам. Впоследствии кредит наличными можно будет оформить с помощью удалённой идентификации.

* * *

Росбанк также активно популяризирует биометрию среди населения. На данный момент банком опубликован ряд материалов с описанием сервиса и информацией о готовности отделений к сбору данных у граждан, первыми результатами сбора биометрических данных, а также с информацией о наиболее активно участвующих в программе регионах. Росбанк также находится в постоянном контакте со СМИ по вопросам биометрии, в частности, наши эксперты дают интервью и комментарии по различным аспектам внедрения и применения биометрической системы.

Когда биометрия начнёт использоваться в других отраслях, то там также возможно потребуется изменение законодательства.

Ещё одна сложность при внедрении биометрии для массовых продуктов и сервисов — психологическое восприятие технологии пользователями. Сейчас, когда люди разблокируют свой смартфон по отпечатку, они не воспринимают этот процесс как биометрическую идентификацию, потому что уже привыкли к этому. Когда те же пользователи слышат о биометрии, они испытывают страх перед кражей или подделкой данных. Основная причина такой реакции — простое незнание механики и сути биометрической идентификации. Необходимо некоторое время, чтобы граждане привыкли и приняли новую технологию, поняли механику работы и увидели на практике, что это удобно и безопасно.

Необходимо некоторое время, чтобы граждане привыкли и приняли новую технологию, поняли механику работы и увидели на практике, что это удобно и безопасно

БИОМЕТРИЯ КАК КОМПОНЕНТ ДИДЖИТАЛИЗАЦИИ

Биометрическая идентификация используется в различных странах уже 25 лет. В Евросоюзе, Молдове, Израиле и других странах биометрические данные используются при изготовлении паспортов — так государства борются с терроризмом и другими видами криминала, ведь подделать биометрические данные гораздо сложнее, чем бумажные документы. Если в обычном паспорте преступнику достаточно переклеить фотографию, то для подделки биометрии понадобится целый IT-отдел.

С точки зрения использования биометрии в федеральном масштабе, Индия является безоговорочным лидером. В 2009 году правительство Индии осознало проблему гражданского документооборота — всего у 20% населения были счёта в банке, а у большинства жителей не было действующих паспортов. В такой ситуации диджитализация и биометрическая идентификация стали идеальным решением. Государство ввело электронные паспорта, к которым привязана биометрия — AADHAAR. Сейчас в эту базу данных внесено 99,5% взрослого населения страны. Цифры ясно дают понять, что правительство приняло верное решение и прекрасно справилось с бюрократической волокитой — только в 2017 году было проведено 7 миллиардов транзакций с использованием отпечатков пальцев. 200 миллионов людей с низким уровнем дохода смогли воспользоваться банковскими услугами, 93 миллиона — медицинскими. Государство сэкономило 2 млрд долларов на выплате субсидий за счёт выявления подделных карт.

Во всём мире, в том числе и в России, крупные компании используют биометрическую идентификацию для удобства клиентов и оптимизации бизнес-процессов. Amazon сделал бескассовый магазин, распознающий клиентов по лицу и автоматически определяют продукты, которые он хочет приобрести. В «Тинькофф Банке» определяют личность клиента по голосу, когда он звонит с вопросом. Клиенту даже не надо представляться оператору — программа определяет его самостоятельно и сразу соединяет с нужным сотрудником. Единая биометрическая система вовсе избавит клиентов от необходимости идти в банк или звонить — оформить кредит или открыть счёт можно будет прямо со смартфона в любой точке страны и даже за её пределами. Биометрические технологии становятся логичной частью процесса цифрового преобразования коммерческих и некоммерческих организаций — диджитализации. И каждый участник рынка только выигрывает от такой перестройки. Бизнес автоматизирует процесс и экономит деньги, а клиенты и граждане могут быстро и качественно получать услуги и приобретать товары.

* * *

При создании Единой биометрической системы специалисты «Ростелекома» изучали практику использования биометрии в других странах, чтобы использовать лучшие решения и избежать ошибок. Система продолжает развиваться, к ней подключаются новые банки, всё больше граждан регистрируются в ней и получают с её помощью финансовые услуги. В будущем эта система будет задействована не только в финансовом секторе, но и в медицине, образовании и при оказании государственных услуг. Внедрение биометрических технологий для подтверждения личности сделает жизнь людей лучше и комфортней, а государственные и коммерческие услуги доступнее.

Артем ХАРЧЕНКО
руководитель отдела предотвращения мошенничества «Тинькофф Банк»

НОВЫЕ АКЦЕНТЫ — НОВЫЕ ЗАДАЧИ

ДЛЯ «ТИНЬКОФФ БАНКА» 2018 ГОД ПРОХОДИТ В ПОСТОЯННЫХ ДОРАБОТКАХ СОБСТВЕННЫХ ПРОЦЕССОВ И ДОВЕДЕНИИ ИХ ДО ИДЕАЛЬНОГО ВИДА

Сейчас можно утверждать — удалённая идентификация всё-таки запустилась. Более 10 банков собирают биометрию для Единой Биометрической Системы в своих отделениях в ряде регионов, а несколько банков смогли успешно реализовать процесс удалённого открытия счета. Мы в «Тинькофф Банке» смогли воплотить в жизнь оба сценария, хотя бизнес-модель банка существенно отличается от классической — у нас нет ни одного отделения.

РОЛЬ ПРЕДСТАВИТЕЛЯ БАНКА

Чтобы разобраться, как «Тинькофф Банк» работает с биометрией в самом широком смысле, а также в контексте удалённой идентификации, важно понимать, как именно выстроен процесс обслуживания клиента с помощью представителей банка. Именно эти сотрудники привозят потенциальному клиенту договор, пластиковые карточки — как самые первые, так и перевыпущенные в процессе обслуживания, различные справки — поэтому может показаться, что представитель является обыкновенным курьером, который занимается исключительно доставкой документов, а все остальные действия осуществляются в бэк-офисе банка.

На самом деле работа представителей намного более сложная и ответственная, ведь фактически представитель «Тинькофф Банк» и операционист в отделении банка с классической бизнес-моделью обладают одинаковым функционалом — начиная от проведения идентификации при открытии первого счета и предложением дополнительных продуктов, заканчивая помощью в установке мобильного приложения. Сотрудник взаимодействует с бэк-офисом банка с помощью специального приложения в смартфоне; все действия представителя, разумеется, фиксируются — таким образом, данные клиента защищены ровно в той же мере, что и при посещении стационарного офиса.

Несколько лет назад мы взаимодействовали с клиентами из труднодоступных регионов с помощью «Почты России», но по мере развития сети представителей таких клиентов становится меньше с каждым днём. Сейчас в банке трудятся более 2500 представителей, которые проводят около 24 тыс. встреч в день в 81 регионе России.

КАК ДЛЯ ЕБС, НО ДЛЯ ДРУГОГО

Итак, теперь стало понятно, представитель функционально олицетворяет классическое отделение. Он может рассказать про разные продукты банка и познакомить нового клиента с удобными сервисами. А ещё он уже несколько лет фотографирует клиентов во время встречи и с недавнего времени предлагает некоторым клиентам оставить свой голосовой слепок. Это очень похоже на сбор биометрии для Единой Биометрической Системы, но преследует совершенно другие цели.

Банк впервые начал фотографировать клиентов в 2011 году. В то время мы посчитали, что наличие фотографии в момент подписания договора может являться ещё одним доказательством подписания договора — некоторые особенно предприимчивые клиенты получали кредит, после чего отказывались от заключения договора. Фотография действительно минимизировала риск возникновения таких инцидентов — для потенциальных мошенников она действовала как превентивная мера, а через несколько лет оказалось, что наличие фотографии позволяет эффективно бороться с другим видом мошенничества. С выходом на рынок POS-кредитов банк столкнулся с регулярными обращениями серийных злоумышленников, которые использовали паспорта с переклеенной фотографией. Данных самой заявки для выявления мошенничества не хватало, ведь они принадлежали истинным владельцам паспортов и выглядели для нас абсолютно «нормально». Изображения же позволили сгруппировать все обращения от каждого из мошенников воедино — для начала стало проще консолидировать ущерб и обращаться в право-

охранительные органы, а далее на помощь пришли технологии распознавания лиц. С 2015 года мы используем их при принятии решения по заявкам на кредит. Например, фотография в текущей заявке сравнивается с уже известной нам фотографией того же заёмщика. Несовпадение фотографий является признаком для глубокого анализа верификатором, а совпадение, наоборот, позволяет избежать дополнительных проверок и, как следствие, принимать решение по заявке намного быстрее. Внедрение технологии распознавания лиц позволило нам значительно сократить потери из-за мошенничества с фальсификацией документов. По нашей оценке, за последние 3 года они уменьшились в 6 раз.

РАСПОЗНАВАНИЕ ГОЛОСА

История распознавания голоса в «Тинькофф Банке» развивалась по другому сценарию. Для банка без отделений особенное значение имеет колл-центр, ведь с помощью него можно совершить практически любую операцию, характерную для банка с отделениями. Операции обладают различными уровнями риска. Например, информацию о местонахождении банкомата можно предоставить любому собеседнику, а для изменения пин-кода карты или обновления доступов в интернет-банк нужно подтвердить личность клиента. Для этого банки, как правило, используют наборы вопросов, ответы на которые должен знать сам клиент, а злоумышленники — не должны. Например, наиболее привычным вопросом является кодовое слово. Тем не менее, такой процесс имеет существенные недостатки: ответы на ряд вопросов являются либо публичными (дату рождения детей или супруга часто указывают в роли кодовой), либо недостаточно защищёнными в случае использования социальной инженерии. Можно решать эту задачу с помощью большего числа вопросов, но в этом случае страдают уже сами клиенты (которых всё-таки больше, чем мошенников).

Мы же попробовали решить эту задачу с помощью алгоритмов распознавания голоса. Окончательно уйти от вопросов к собеседнику в любом случае невозможно — как и ранее нам требуется как минимум узнать цель обращения и иногда попросить клиента представиться, например, в случае звонка с ранее неизвестного нам номера. Далее процесс выглядит аналогично сверке фотографий. Если у нас уже есть качественная запись голоса клиента (мы называем её «эталонной»), то алгоритм используется для сравнения голосов в текущем и историческом звонках, а результаты интерпретируются в виде дополнительного фактора при ответе на вопрос (разрешить проведение конкретной операции или же отказать?). Ключевое отличие — в разработке алгоритма. Если распознавание лиц в России представлено широко, а подбор вендора не вызывает затруднений, то с распознаванием голоса мы прошли путь от использования стороннего решения до разработки собственного алгоритма, который с 2017 года обрабатывает весь телефонный трафик в банке. До внедрения технологии распознавания голоса подтверждение личности клиента в ходе телефонного разговора занимало у нас в среднем около 1 минуты, а сейчас снизилось до 15 секунд.

Другой важной задачей для увеличения эффективности процесса является обогащение базы «эталонных» голосовых слепков — не все клиенты обращаются в банк по телефону, поэтому возможна ситуация, в которой обращение с высоким уровнем риска является первым звонком клиента в колл-центр за всё время обслуживания. Сейчас мы пробуем собирать «эталонный» голосовой слепок клиента сразу после подписания договора. Клиенту поступает звонок из банка, и ему требуется всего лишь зачитать определённый текст во встроенный микрофон собственного телефона. Пока рано говорить, насколько быстро можно масштабировать этот процесс для всех клиентов, но уже понятно, большинство клиентов, которым мы предложили оставить голосовой слепок, положительно отнеслись к этому предложению.

ЕБС: НОВЫЕ АКЦЕНТЫ

До внедрения Единой Биометрической Системы ключевыми целями сбора фотографий и голосовых записей для «Тинькофф Банка» являлись повышение безопасности в дистанционном обслуживании и минимизация риска внешнего мошенничества, а также оптимизация времени обслуживания. Сбор биометрических данных для удалённой идентификации преследует иную цель — формирование достоверного биометрического профиля высокого качества, приемлемого для распознавания и сравнения несколькими вендорами в каждой из модальностей, поэтому требования к фотографии и записи голоса существенно отличаются от привычных нам. Для внутренних

До внедрения технологии распознавания голоса подтверждение личности клиента в ходе телефонного разговора занимало у нас в среднем около 1 минуты, а сейчас снизилось до 15 секунд

процессов, связанных с фотографией, мы долгое время никак не ограничивали представителей — как следствие, качество фотографии очень сильно зависит от сценария её сбора. Например, около 10% встреч проходят в автомобиле клиента или представителя, и из-за неравномерности освещения на лице клиента могут возникнуть тени, а фон, как правило, точно не однородный. Оказалось, что для решения внутренних задач такие фотографии пригодны, но использовать их в роли «эталонных» для удалённой идентификации точно не стоит.

Другой важной задачей в ходе интеграции с Единой Биометрической Системой для нас являлся подбор оборудования для сбора биометрии. Так как представитель уже оснащён мобильным устройством, то наиболее приемлемым для нас было, разумеется, использование того же смартфона для сбора и фотографии, и голосовой записи. С идеей использования встроенного микрофона пришлось сразу расстаться — процесс сбора голосовой записи не предполагает использование телефонии (как в сценарии внутри банка). К тому же, встроенный микрофон не обладает характеристиками, удовлетворяющими требованиям регулятора, поэтому нам пришлось искать внешние микрофоны, которые, с одной стороны, смогут передавать качественную запись, а с другой, будут удобными в использовании для представителя. Подтверждение пригодности основной камеры смартфона потребовало для нас больше усилий — совместно с оператором ЕБС банк провёл несколько тестов, результатом которых стало подтверждение возможности использования ряда устройств, позволяющих банкам-участникам использовать биометрию вне офиса.

ЗАПУСК СИСТЕМЫ

Запуск ЕБС состоялся 01.07.2018. В этот день мы начали принимать заявки на сбор биометрических данных у текущих клиентов. Для этого достаточно обратиться в колл-центр или чат банка, после чего мы назначим встречу, а наш представитель приедет в удобное для клиента место для сбора биометрии. Конечно, мы не рекомендуем встречаться в шумных или слабоосвещённых местах. Как правило, представитель при встрече сможет найти место, которое подойдёт для сбора качественного биометрического слепка. Среди заявок, поступивших к нам в первые дни после запуска проекта, было ожидаемо много коллег из других банков и IT-компаний, которые тестировали процесс на себе. Даже на их фоне встречались заявки, которые наглядно показывают назначение Единой Биометрической Системы. Например, запомнился клиент, постоянно проживающий за пределами России. Запуск совпал с его отпуском, который он решил провести на Родине, поэтому он решил сдать биометрию, чтобы позже иметь возможность дистанционно открывать счета в российских банках без посещения отделения.

УДАЛЁННАЯ ИДЕНТИФИКАЦИЯ

Параллельно с разработкой процесса сбора биометрии мы занимались реализацией второй части процесса, ради которой и создавалась Единая Биометрическая Система — удалённой идентификации. Пройти удалённую идентификацию можно двумя различными способами: с помощью посещения web-портала банка или через мобильное приложение.

Интересно, что клиентский путь для каждого из способов свой: если для открытия счета удалённо через портал банка потенциальному клиенту достаточно посещения самого портала, то в случае с мобильным приложением одного приложения банка будет недостаточно — потребуется скачать приложение оператора Единой Биометрической Системы. Это сказалось на времени реализации процесса — удалённую идентификацию через web-портал получилось сделать намного быстрее, и она уже работает в промышленной среде, а мобильную версию мы планируем запустить до конца года. Конечно, именно она должна стать самым перспективным каналом для открытия удалённых счетов, ведь камера и микрофон есть практически в любом смартфоне, в отличие от ноутбуков и настольных компьютеров.

Selfie же наиболее удобно делать на фронтальную камеру смартфона — очевидный факт, который мы подтвердили внутренними исследованиями. На всех формах банка мы просили потенциального клиента сделать фотографию во время заполнения заявки. Фотографии на мобильные устройства делают в полтора раза чаще, чем на планшеты, и в два с половиной раза чаще, чем на настольные компьютеры.

* * *

Для банков-участников Единой Биометрической Системы 2018 год проходит в постоянных доработках собственных процессов и доведении их до идеального вида. В прессе периодически появляются сообщения о том, что собрано недостаточно много биометрических шаблонов, но в этом нет ничего страшного, ведь со временем список банков, открывающих счета удалённо, будет расширяться, услуга будет предложена более широко, а значит, ещё больше клиентов захотят зарегистрироваться в ЕБС и создать свой биометрический профиль.

БИОМЕТРИЯ В АУТЕНТИФИКАЦИИ

СОВРЕМЕННЫЕ ПОДХОДЫ К УДОСТОВЕРЯЮЩИМ ПРОТОКОЛАМ

Мирослава БОНДАРЕНКО
преподаватель школы ИТ менеджмента РАНХиГС, кандидат технических наук

Сергей ТИХОНОВ
преподаватель школы ИТ менеджмента РАНХиГС, кандидат физико-математических наук

В протоколах доступа субъекта (человека) к информационным ресурсам центральную роль играют три понятия — идентификация, аутентификация и авторизация. Сторона, раскрывающая информацию обязательно должна убедиться, кто хочет получить доступ, чем он может себя удостоверить и есть ли у него разрешение на доступ. В этой статье мы рассмотрим современные подходы к аутентификации, то есть протоколам, которые позволяют субъекту себя удостоверить.

В простейшем случае протокол идентификации состоит в том, чтобы назвать свой логин (имя пользователя, учётную запись, персональный номер и др.), а протокол аутентификации в том, чтобы сообщить секретную информацию, которая есть только у субъекта (например, пароль).

Способы аутентификации можно разбить на три большие группы по общим признакам. Вот эти признаки, они же факторы:

- знание — логин и пароль;
- владение — токен, на котором хранится секретный ключ или сертификат, или устройство, выдающее код подтверждения;
- сущность — обладание признаками, однозначно идентифицирующими пользователя — биометрические данные.

При использовании способов из разных групп говорят о многофакторной аутентификации. Использование разных способов из одной группы (отправка первого кода подтверждения по электронной почте, а второго по СМС) не делает аутентификацию многофакторной.

Подтверждение сущности не требует от человека запоминания данных или хранения токенов.

ПРОТОКОЛЫ

При разработке протоколов аутентификации с использованием биометрии можно брать за основу существующие протоколы, разработанные для других факторов, расширяя их биометрической спецификой. Рассмотрим известное семейство протоколов выработки общего ключа с аутентификацией на основе пароля PAKE [1] и его биометрическое расширение BAKE [6,8].

Протоколы PAKE позволяют участникам обеспечить взаимную аутентификацию и установить безопасный канал связи [2]. Использование PAKE в TLS обеспечивает безопасную аутентификацию на стороне клиента, заменяя сертификаты на пароли для аутентификации своих идентификаторов. Такое решение удобно использовать при ограничениях в ресурсах, в скорости обработки, в доступности ресурсов [3], например, для Интернета Вещей (IoT).

ПРИМЕР BAKE

На рисунке 1 представлено высокоуровневое описание шагов в протоколе BAKE. Протокол PAKE и расширение BAKE основаны на алгоритме Диффи-Хеллмана для идентификации ключей. Отметим, что алгоритм Диффи-Хеллмана, как и многие алгоритмы, решающие задачу распределения ключей, уязвим против атаки с помощью квантового компьютера [4], но будем надеяться, что как минимум пять лет у нас есть. Несколько механизмов PAKE были стандартизированы на междуна-

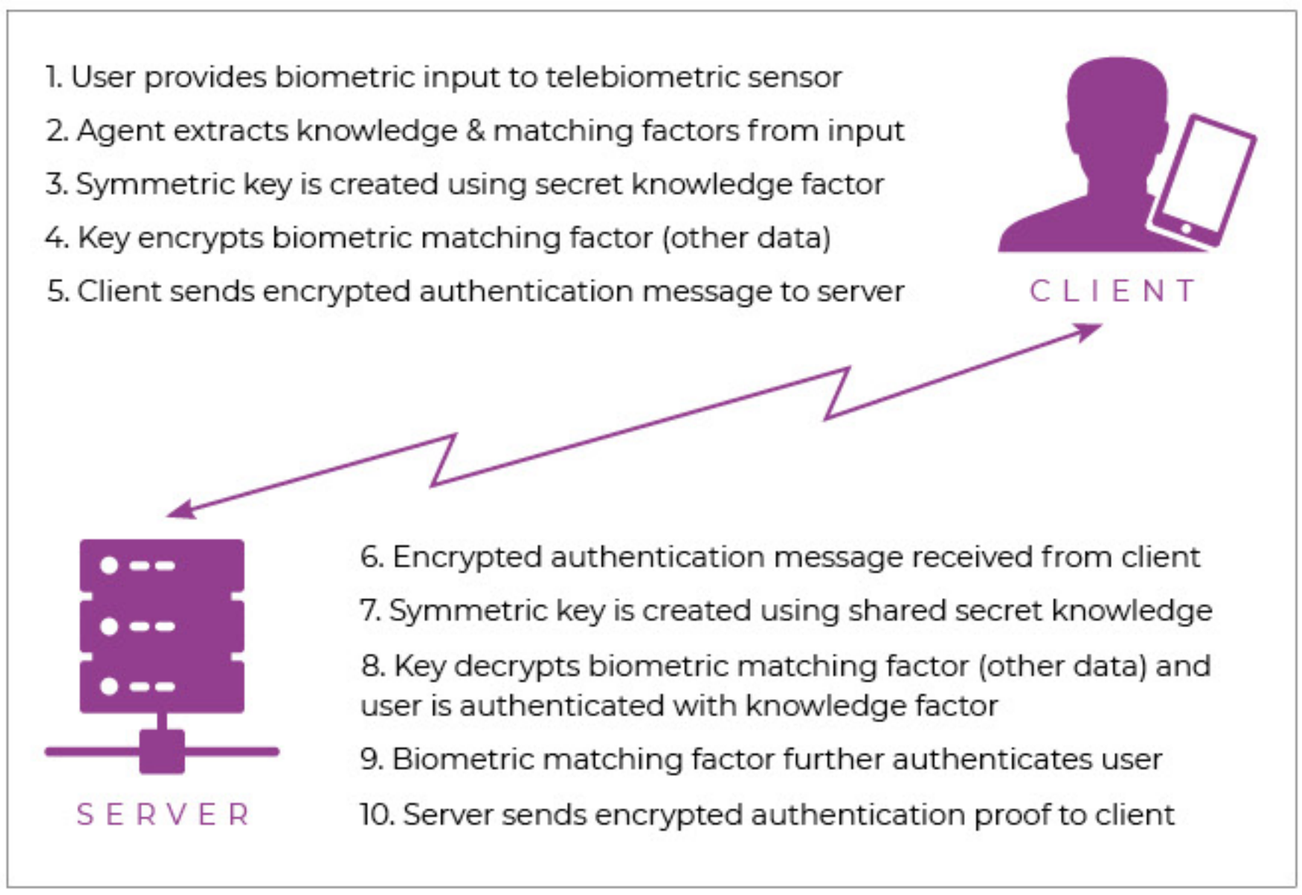


Рисунок 1. Пример. Биометрический обмен ключами с проверкой подлинности (BAKE) [6,8]

родном уровне в Рекомендации МСЭ-Т X.1035: ITU-T X.1035: «Password-Authenticated Key Exchange» (PAK) recommendation [5] и в Механизмах управления ключами ISO / IEC 11770–4, основанных на слабых (легко раскрываемых) секретах [6].

МНОГОФАКТОРНОСТЬ

Секретные знания, совместно используемые пользователем и сервером, могут быть собраны у пользователя и «представлены в систему разными способами и форматами» [5]. Они варьируются от простого пароля, введённого через клавиатурное устройство, до PIN-кода, введённого с помощью сенсорного экрана смартфона, и до человеческой речи, записанной микрофоном [5]. Как только данные, содержащие знания пользователя, собираются, их необходимо преобразовать или отобразить в подходящий строковый формат, прежде чем его можно будет внести в протокол PAKE.

Необходимые для аутентификации знания (секреты) пользователя могут быть извлечены из того же источника (тех же биометрических датчиков), из которого поступают пользовательские биометрические данные [6]. Многие типы биометрических данных содержат знания пользователя, но легко понятный пример — это голосовая биометрия. Пользователь может сообщить пароль голосом, передавая одновременно и знание (секретный пароль) и биометрию (характеристики голоса). Сохранённые необработанные данные датчика могут быть переданы системе биометрической проверки идентификации пользователя. Те же данные датчиков также могут обрабатываться с помощью средства распознавания речи, такого как Google Cloud Speech API [7], для преобразования речи пользователя в текст.

БИОМЕТРИЧЕСКАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ

Определение электронной подписи может варьироваться в зависимости от юрисдикции. В России это закон «Об электронной подписи». В США электронная подпись указывается в соответствии с Единым законом об электронных транзакциях (Uniform Electronic Transactions Act) и Законом об электронных подписях в глобальной и национальной торговле (Electronic Signatures in Global and National Commerce Act).

Версия ANSI стандарта X9.84 (2017 года) определяет три новых метода электронной подписи на основе биометрических данных. Этими методами являются биометрический токен электронной подписи (biometric electronic signature token, BEST), его модификация (signcrypted biometric electronic signature token, SBEST) и биометрический обмен электронной аутентификацией с использованием электронной подписи (biometric electronic-signature authenticated-key exchange, BESAKE).

Два из этих методов, BEST и SBEST, полагаются на функционирующую инфраструктуру открытого ключа (PKI). Техника BESAKE расширяет BAKE для создания протокола электронной подписи без необходимости использования цифровых сертификатов.

Эти три метода могут использоваться для электронного подписания соглашений любого

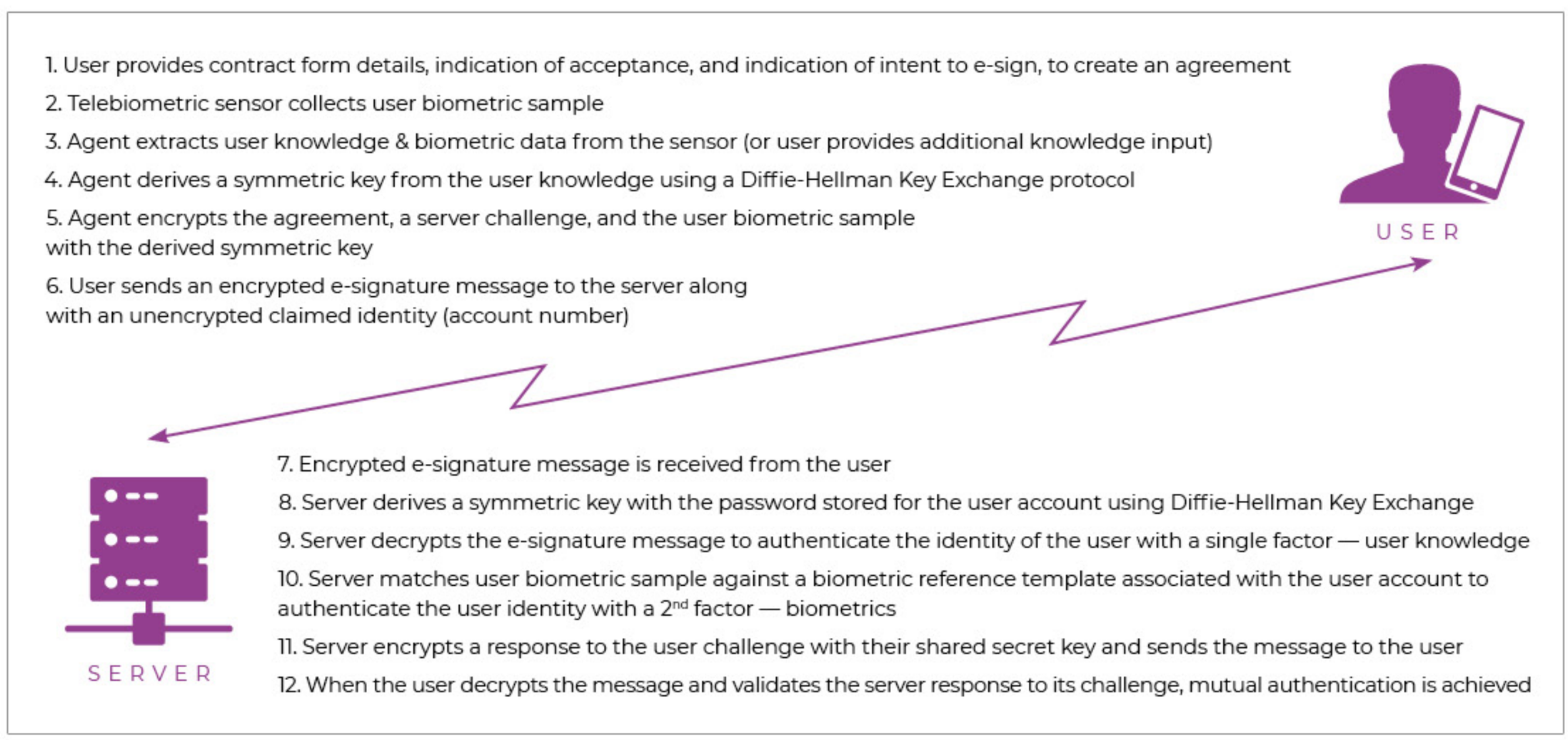


Рисунок 2. Пример BESAKE [8]

типа или формата. Все три метода предназначены для использования в электронной торговле и других случаях использования подписей, как коммерческих, так и правительственных. Они обеспечивают многофакторную аутентификацию пользователя и взаимную аутентификацию, а также защищают конфиденциальность биометрических данных электронного подписанта и другую информацию.

Методы биометрической электронной подписи X9.84 сочетают биометрическую аутентификацию с криптографией и подходят для использования в облачных средах и распределённом журнале (блокчейн), включая приложения смарт-контрактов.

На рисунке 2 описаны шаги протокола BESAKE и показано, как протокол BAKE может использоваться для целей, отличных от аутентификации пользователя, расширения TLS и создания безопасного канала связи. Шаги 1–6 показывают, как создаётся зашифрованный токен электронной подписи BESAKE. В токене содержится надлежащее соглашение электронной подписи, в том числе указание о принятии условий и намерений для электронного подписания. Токен также содержит биометрическую информацию пользователя, челлендж сервера и любые другие данные, необходимые для контрактного приложения.

Шаги 7–12 описывают обработку, требуемую при проверке достоверности заявленного идентификатора электронного подписывающего лица. Обработка собственно соглашения остаётся для контрактного приложения.

BESAKE может использоваться для авторизации передачи стоимости в смарт-контракте. Зашифрованные результаты шагов 1–6 на рисунке 2 можно безопасно разместить в облаке, распределённом журнале (блокчейн) или в среде смарт-контрактов. В контексте смарт-контракта код цепи приведёт к обработке шагов 7–12, когда событие смарт-контракта сигнализирует о том, что контракт выполнен.

БИОМЕТРИЧЕСКИЕ ПРОТОКОЛЫ. МЕЖДУНАРОДНАЯ ПРАКТИКА

Аутентифицированные протоколы обмена ключами, такие как BAKE на основе PAKE, могут использоваться для обеспечения надежной двухфакторной аутентификации пользователей. BAKE может быть реализован путём объединения биометрических данных и пользовательских знаний (секретов), извлечённых из одного биометрического датчика. Многие биометрические технологии могут обеспечить два фактора аутентификации, и всё это без накладных расходов TLS, цифровых сертификатов и правильно функционирующей PKI.

Протокол BAKE может использоваться для создания недорогих, удобных в использовании систем контроля доступа, которые могут помочь управлять рисками несанкционированного доступа к информации и обеспечивать безопасную связь в средах с ограниченными ресурсами, где не могут использоваться решения на основе сертификатов.

BAKE также может помочь улучшить практику аутентификации пользователей, создать доверие пользователей посредством взаимной аутентификации, гарантировать, что пользователи фактически подключены к системам, которым они планировали подключиться и которым они могут доверять. BAKE гарантирует, что учётные данные для проверки подлинности пользователя и другие конфиденциальные данные защищены от атак типа «человек-в-середине» и фишинга во время передачи учётных данных для проверки подлинности пользователя и во время последующих коммуникаций.

***

Кроме того, BAKE может быть расширен до протокола для электронных подписей BESAKE, для поддержки электронных подписей документов любого типа и формата.

ЛИТЕРАТУРА

1. Wikipedia, «Password-Authenticated Key Agreement,» *https://en.wikipedia.org/wiki/Password-authenticated_key_agreement.*
2. *Douglas Stebila,* «Secure Modular Password Authentication for the Web Using Channel Bindings,» *https://www.douglas.stebila.ca/research/papers/SSR-ManSteDen14/.*
3. SSR 2014, «Security Standardisation Research,» *http://ssr2014.com/.*
4. *S. Tikhonov, M. Bondarenko.* «Application of Quantum Technologies for Practical Tasks». ISSA Journal November 2017 *https://cdn.ymaws.com/www.issa.org/resource/resmgr/journalpdfs/feature1117.pdf*
5. ITU, «X.1035: Password-Authenticated Key Exchange (PAK) Protocol,» *http://www.itu.int/rec/T-REC–X.1035–200702-I/en*
6. *Phillip H. Griffin,* «Biometric Knowledge Extraction for Multi-Factor Authentication and Key Exchange,» Procedia Computer Science, Volume 61, 2015, Elsevier, freely available at *http://www.sciencedirect.com/science/article/pii/S1877050915029804*
7. Google, «Cloud Speech API,» *https://cloud.google.com/speech/.*
8. *Phillip Griffin,* ISSA Fellow, Raleigh Chapter, «Biometric Electronic Signatures.», ISSA Journal, January 2018

Василий ПИСКАРЕВ
председатель Комитета
Государственной Думы РФ
по безопасности
и противодействию коррупции

БЕЗОПАСНОСТЬ ТРЕБУЕТ ОТВЕТСТВЕННОСТИ

НАСТАЛО ВРЕМЯ ЗАКРЕПИТЬ НА МЕЖДУНАРОДНОМ УРОВНЕ ПРАВИЛА ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ В КИБЕРПРОСТРАНСТВЕ

Вступление мира в цифровую эпоху, когда повседневная жизнь человека всё больше и больше зависит от современных технологий, требует быстрой и своевременной реакции законодателей. В современном обществе всё большую угрозу несет развитие кибертерроризма. Если еще вчера мы сталкивались с действиями хакеров-одиночек, то сегодня это хорошо организованные и технически оснащенные группы, чьи действия не знают границ.

ЗАЩИТИТЬ ОТ КИБЕРУГРОЗ

Количество кибератак на российские ресурсы в этом году возросло на треть. По данным специалистов Сбербанка, возможный ущерб российской экономике от киберугроз составит свыше 1 трлн рублей, а мировая экономика недосчитается $ 1,5 трлн. Кибератаки стали угрозой не только для банков и электронных кошельков отдельных граждан, но и для объектов критической информационной инфраструктуры государств. Широко обсуждавшийся в СМИ случай, когда компьютерный вирус вывел в Тюмени из строя всю медицинскую аппаратуру во время сложнейшей нейрохирургической операции, — лишь один из примеров действия кибертеррористов, создающих угрозу жизням людей.

Если учесть, что в ближайшее время к сети интернет в нашей стране подключатся все медицинские и образовательные учреждения, то нужно серьёзно подумать об их защите. Более того, сегодня опасности кибератак подвергаются нефтегазовая, электроэнергетическая, транспортная системы, ядерные и военные объекты. И этого нельзя не учитывать. Нужна работоспособная система государственной и международной информационной безопасности, чтобы надежно защитить права личности, общества и государства в информационной сфере и обеспечить безопасность критической информационной инфраструктуры.

1 января 2018 года вступил в силу Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», которым установлены требования по обеспечению безопасности таких объектов, определен порядок создания государственной системы обнаружения, предупреждения и ликвидации компьютерных атак. Были также внесены изменения в Федеральные законы «О связи», «Об информации и информационных технологиях», «О противодействии экстремистской деятельности», «О противодействии терроризму», «О Государственной тайне», «О персональных данных», направленные на обеспечение информационной безопасности.

И эта работа будет продолжена, поскольку прогресс не стоит на месте, и с развитием новых технологий появляются все более изощренные методы воздействия на компьютерную технику и человека с террористическими и мошенническими целями. Для реализации закона «О безопасности критической информационной инфраструктуры РФ» в практической плоскости, чтобы обеспечить надежную защиту критически важных объектов, необходимо внедрение самых современных IT-решений. В России уже создана и по-

стоянно совершенствуется система противодействия компьютерным атакам (государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России — ГосСОПКА).

ЦИФРОВОЙ ЭКОНОМИКЕ — БЕЗОПАСНОЕ РАЗВИТИЕ

Важно понимать, что обеспечение кибербезопасности ни в коем случае не должно сводиться к тотальному контролю и ущемлению прав граждан и свободы предпринимательства. Наоборот, задача государства и международного сообщества — обеспечить все возможности для реализации личности и развития экономики. Об этом на Международном конгрессе по кибербезопасности в этом году говорил Президент России Владимир Путин, который подчеркнул, что «эффективное цифровое развитие может быть основано только на цифровой свободе: на свободе для бизнеса, общественных организаций, для граждан, на снятии барьеров, которые сдерживают, ограничивают прогресс».

В Государственной Думе РФ сейчас идет серьезная работа по законодательной поддержке цифровой экономики. Важно при этом обеспечить её безопасное развитие. Здесь можно отметить и уже вступивший в силу закон о противодействии хищению средств с банковских карт, и находящиеся в работе законопроекты о криптовалютах. В ходе осенней сессии Государственная Дума рассмотрит девять законопроектов, так или иначе связанных с развитием цифровой экономики. Среди них, например, инициативы, связанные с цифровой идентификацией личности (законодательное регулирование облачной цифровой подписи, смарт-контрактов).

В том, что касается законодательного оформления деятельности, связанной с производством и хождением криптовалют, российские парламентарии очень осторожны. С одной стороны, это явление уже существует, и необходимо придать ему законные рамки. С другой — хождение криптовалют уже сегодня создает массу возможностей для перевода средств, получаемых от наркоторговли и финансирования терроризма, не говоря уже о различных мошеннических схемах. Все эти обстоятельства законодатель должен учитывать, чтобы внедрение в экономику и финансовую систему новых технологий не приводило к ослаблению безопасности страны.

ОГРАДИТЬ ГРАЖДАН ОТ КИБЕРТЕРРОРА

Важным решением Государственной Думы стало принятие закона, направленного на противодействие так называемому «телефонному терроризму». Прошлой осенью было зафиксировано свыше 9 000 ложных сообщений о подготовке терактов во многих субъектах Российской Федерации. Причём большинство звонков были сделаны из-за рубежа с применением специальных компьютерных программ, чтобы нельзя было установить источник звонка.

Приходилось неоднократно эвакуировать людей из торговых центров, кинотеатров, учебных заведений, что требовало немало сил и средств, терпели убытки предприниматели. Мы оперативно приняли закон, который позволил операторам блокировать по запросам правоохранительных органов телефонные номера, с которых делались такие звонки. Была также ужесточена уголовная ответственность за ложные сообщения об актах терроризма.

Кроме того, недавно наш Комитет поддержал разработанные Заместителем Председателя Государственной Думы РФ Ириной Яровой и другими депутатами поправки в законодательство, направленные на укрепление информационной безопасности и противодействие деятельности, побуждающей детей к опасным для их жизни поступкам. Речь идет о прекращении доступа к интернет-страницам, содержащим противоправный контент, и проведении всестороннего расследования таких действий.

Не секрет, что в последние годы в интернет-пространстве, и особенно в соцсетях, появилось немало страниц и сообществ, так называемых «групп смерти», подобных нашумевшему «Синему киту» и некоторым другим, организаторы которых побуждают детей и подростков к суициду, потреблению наркотиков, романтизируют массовые убийства в американских школах. Подобная активность в Интернете — это тоже своеобразная форма кибертерроризма, и ее необходимо пресекать. Тем более, что, по свидетельству специалистов, подобные практики в интернет-сообществах включают в себя сложнейшие технологии перекодирования сознания подростков, отключения их критического мышления, доведения детей до такого состояния, когда они готовы выполнять любые задания организаторов смертельных игр.

Блокировка сайтов — это далеко не единственный метод борьбы с подобными явлениями. Но он важен. И вот почему. Рассматриваемый сейчас Госдумой РФ законопроект предлагает не удалять интернет-сайты, содержащие противоправный контент, а незамедлительно прекращать к ним доступ. Именно такой порядок действий позволит правоохранительным органам осуществлять сбор и фиксацию всех необходимых доказательств и проводить объективное и всесторонне расследование, а значит — выявить виновных в распространении запрещенной информации, привлечь организаторов подобных сообществ в интернете и их соучастников к ответственности и надолго изолировать их от общества.

Снижению уровня киберугроз должно способствовать создание в нашей стране системы автоматизированного обмена информацией об угрозах в цифровом пространстве и системы международного обмена такой информацией. Свое

Нужна работоспособная система государственной и международной информационной безопасности, чтобы надежно защитить права личности, общества и государства в информационной сфере

Председатель Комитета ГД по безопасности и противодействию коррупции Василий Пискарев и глава германского Совета по кибербезопасности Ханс Вильгельм Дюн — модераторы секции «Укрепление международной безопасности: роль парламентов» на Международном форуме «Развитие парламентаризма». Москва, июнь 2018 г. Фото предоставлено Пресс-службой Государственной Думы РФ

слово должны сказать и законодатели. Важен, в частности, обмен опытом законодательного регулирования и сближение норм, принятых в различных государствах.

ИНФОРМАЦИОННАЯ ОТВЕТСТВЕННОСТЬ НА МЕЖДУНАРОДНОЙ АРЕНЕ

Об этом мы говорили в июне с зарубежными коллегами на организованном Государственной Думой Международном форуме «Развитие парламентаризма». В работе секции «Укрепление международной безопасности: роль парламентов» принимал участие глава германского Совета по кибербезопасности Ханс Вильгельм Дюн. Ведущий европейский специалист в этой сфере выступил с инициативой об обмене информацией и налаживании международного сотрудничества в сфере кибербезопасности. Такое сотрудничество Россия уже развивает во взаимодействии со странами БРИКС, ШОС и ОДКБ. Со всеми странами БРИКС, а также с Кубой и Белоруссией заключены соглашения о сотрудничестве в сфере обеспечения международной информационной безопасности.

Организация оперативного обмена информацией о компьютерных инцидентах и уязвимостях систем поможет предотвратить действия кибертеррористов в отношении объектов критической инфраструктуры наших стран, защитить финансовые системы. По оценкам экспертов, массированная кибератака в Интернете с отключением компьютерных систем может привести к разорению пятой части средних компаний за несколько часов, и около половины компаний обрушатся в течение суток. Свыше трети банков будут разорены уже через несколько часов после такой катастрофы. Наверное, излишне прогнозировать к чему может привести кибератака на диспетчерские службы аэропортов, атомные электростанции, системы управления метро или водоканала.

Отмечу, что в России отрицательно относятся к попыткам чрезмерной политизации вопросов, связанных с кибербезопасностью. Западные страны стремятся легитимизировать на международном уровне проведение наступательных действий с использованием информационного оружия, ответных мер военного характера на киберугрозу, действия хакеров и т.д. Всему миру хорошо известно, как легко США и их союзники умеют назначать виновных и наказывать целые государства в соответствии со своими представлениями о справедливости и международной безопасности. При этом не утруждая себя предоставлением убедительных доказательств вины подвергаемого бомбардировкам государства.

Россия уже в течение 20 лет выступает с инициативами по формированию бесконфликтного информационного пространства. Среди наших приоритетов в международной сфере — выработка и принятие под эгидой ООН универсальных правил ответственного поведения государств в информационном пространстве. Проект таких правил активно прорабатывался Россией с её партнерами по ШОС и БРИКС. Он прошел в этом году квалифицированное экспертное обсуждение на международных конференциях, организованных при поддержке Комитета Госдумы РФ по безопасности и противодействию коррупции и активном участии первого заместителя председателя Комитета Эрнеста Валеева, в рамках «Инфофорума» в Москве, Ялте и Ханты-Мансийске.

По сути, Россия предлагает закрепить в цифровой сфере принципы Устава ООН — неприменение силы, уважение государственного суверенитета, невмешательство во внутренние дела других государств, соблюдение основных прав и свобод человека, а также гарантировать всем государствам равные права на участие в управлении интернетом.

* * *

Проект соответствующей резолюции наша страна 12 октября внесла на рассмотрение в Первом комитете Генеральной Ассамблеи ООН. И по этому документу уже развернулась активная дискуссия. На первоначальном этапе проект резолюции уже получил поддержку 12 государств, на территории которых проживает почти четверть жителей планеты. Утверждение на уровне ООН правил ответственного поведения государств в киберпространстве может стать важным шагом в укреплении международной безопасности в информационно-коммуникационной сфере.

Комитет Государственной Думы по безопасности и противодействию коррупции продолжает работу по совершенствованию законодательства о кибербезопасности и приглашает всех, чья деятельность связана со сферой информационных технологий, к сотрудничеству.

Артем СЫЧЕВ
первый заместитель директора
Департамента информационной
безопасности Банка России

АНТИФРОД: НОРМАТИВНЫЕ НОВАЦИИ

ЧТО ОЗНАЧАЕТ ДЛЯ ФИНАНСОВОЙ СФЕРЫ ОБНОВЛЕНИЕ ПОЛОЖЕНИЯ БАНКА РОССИИ № 382-П, ПРОИЗВЕДЁННОЕ СОГЛАСНО «ЗАКОНУ ОБ АНТИФРОДЕ»

Важными вехами развития нормативно-правовой базы информационной безопасности финансовой сферы стали Федеральный закон от 27 июня 2018 года № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» и обновлённое Положение Банка России № 382-П от 9 июня 2012 года.

ДОЛГОЖДАННЫЙ ЗАКОН

К сегодняшним переменам в сфере государственного регулирования информационной безопасности финансовой сферы Банк России шёл с 2015 года. Причиной послужил тогдашний серьёзный всплеск хищений денежных средств в сфере электронных платежей. Как у физических, так и у юридических лиц.

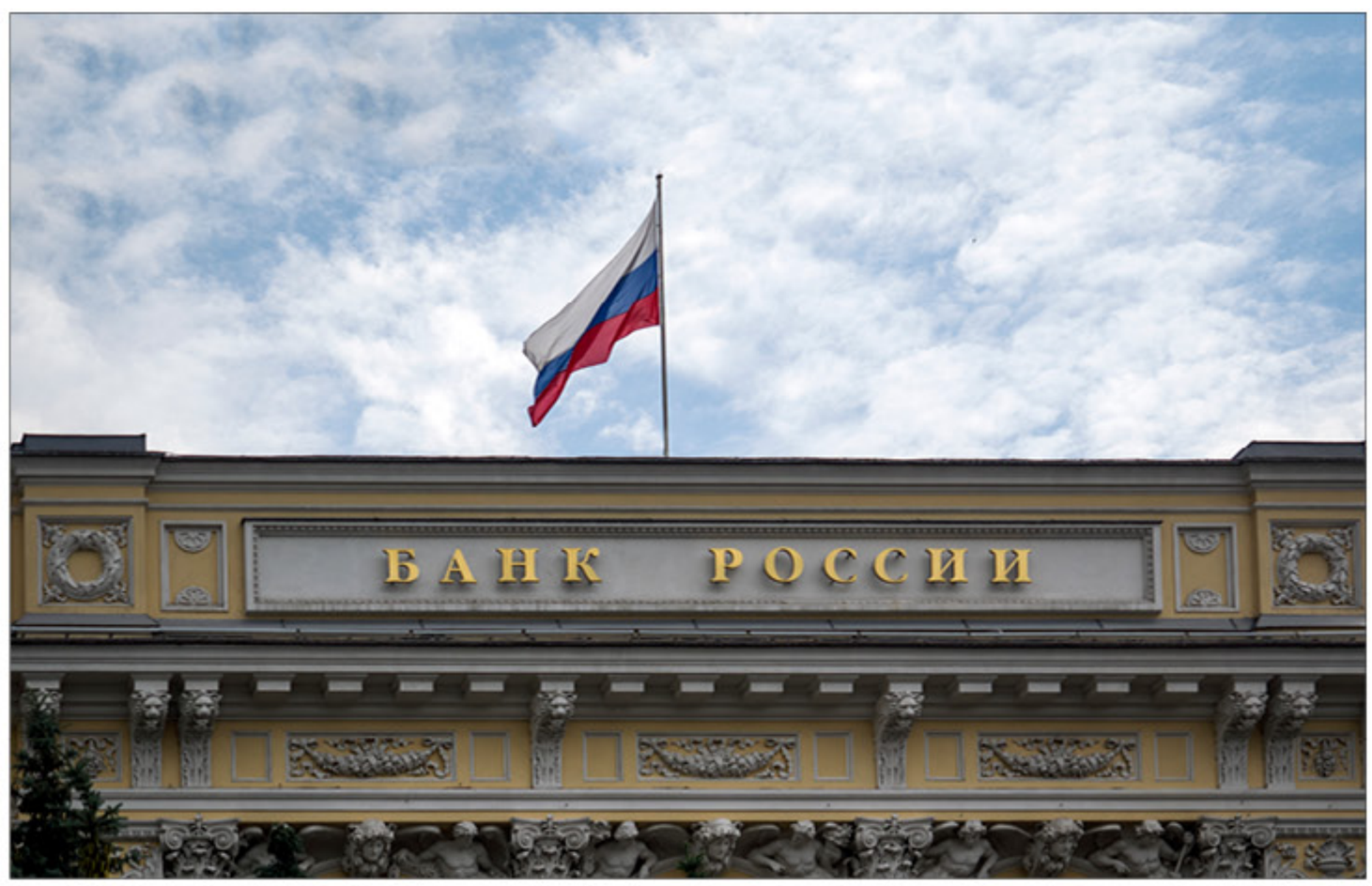
Напомним цифры: в 2015 году более одной тысячи подобных покушений на общую сумму почти в 4 млрд рублей. В 61 % случаев покушения завершались хищениями средств у законных владельцев. Более массовым и серьёзным оказался ущерб юридическим лицам, в основном малому и среднему бизнесу. Для них это могло быть крайне болезненным, означать потерю оборотных средств. Это довольно серьёзный, недопустимо высокий процент. Для его снижения предприняли срочные меры.

Обрисовался ряд проблем, среди самых острых — отсутствие законодательного регулирования мониторинга и обмена данными об инцидентах информационной безопасности в финансовой сфере и об участниках схем хищений денежных средств («дропперах»). Существовали ограничения возможностей государственного регулирования Банком России инфраструктуры платёжных сервисов.

Отсутствовали правовые основы определения, приостановки и возврата сомнительных платежей. Даже если банк-получатель денежных средств определил несанкционированную транзакцию, вернуть их законному владельцу было крайне сложно. Механизмов быстрого возврата для таких случаев не было. Представители банков много об этом говорили и на Уральском форуме, посвящённом информационной безопасности финансовой сферы, и на других подобных мероприятиях.

Выявленные проблемы обсуждались на уровне руководства страны. Для их решения была разработана программа действий по нескольким направлениям, в частности, проработки развития законодательной базы и расширения полномочий Банка России. Итогом этой работы и стало принятие Федерального закона от 27 июня 2018 года № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств».

Настоящий закон вступил в силу по истечении девяноста дней со дня его официального опубликования — 26 сентября 2018 года. Времени для подготовки к полноценному информационному обмену было достаточно у всех банков. Расчёт был на то, что все завершат подготовительные работы к концу лета, до 1 сентября. Мотивация понятная: всем по-



том станет намного проще, эффективнее работать. Особенно легко будет тем, кто и раньше старался соответствовать действующим нормам. Для них игра по новым правилам не потребует сколько-нибудь существенных затрат.

Для специалистов нормативно-правовые нововведения не стали неожиданностью. Как уже было сказано, многие статьи ФЗ-167 и новые нормы 392-П, направленные на усиление противодействия фроду, были сформулированы по итогам публичных дискуссий. Сначала говорили о необходимости развития регулирования, потом уже о его технических деталях. У многих банков наработан богатый опыт их выполнения на практике. На рынке есть предложения компаний-поставщиков решений.

ГЛАВНЫЕ НОВШЕСТВА

Первая важная новация этого закона — создание правовой основы механизма приостановки незаконных платежей и возврата уже переведённых денежных средств их настоящим владельцам. Раньше приостановка хищений и возвращение похищенных денег во многом зависели от воли и профессионализма сотрудников банков. Теперь это легальная, подробно описанная процедура, внесудебная и оперативно работающая.

Но в законе нельзя прописать все детали. Поэтому технические и организационные процедуры проверки подлинности платёжного поручения выбирают операторы платежей. Как оператор-отправитель (к примеру, дополнительное подтверждение поручения путём телефонного звонка и т.п.), так и оператор-получатель (запрос у клиента договора, на основании которого поступает платёж и т.п.).

Вторая важная новация — легализация в полном объёме антифрода, мониторинга для выявления мошеннических действий в сфере электронных платежей. Только тогда явно фиктивный платёж может быть вовремя выявлен и остановлен. Ранее эта работа не имела нормативно-правовой основы, была необязательной и велась по усмотрению руководства банков. Но для своевременного выявления и приостановки мошеннического перевода необходимо, чтобы мониторинг транзакций вели обе стороны: и банк-отправитель, и банк-получатель, причем во взаимодействии.

Противоположный момент — ошибочные приостановки банками платежей. В таких случаях банки обвиняются в превышении полномочий. Чтобы избежать обеих крайностей, в ФЗ-167 предусмотрена обязанность всех организаций, осуществляющих переводы денежных средств, вести антифрод-мониторинг. Банк России наделяется полномочиями определять и публиковать признаки мошеннических транзакций.

Среди них, например, большое количество платежей на крупные суммы со счёта юридического лица физическим лицам, находящимся в других регионах, в короткий промежуток времени. Необычные, странные назначения платежей. И другие отклонения от стандартного поведения клиентов. Каждая финансовая организация использует эти признаки применительно к собственной политике управления рисками и осуществления антифрода.

ФЗ-167 не обязывает банк заблокировать карту клиента в случае подозрения в мошенническом платеже. Есть большой перечень различных действий, которые может совершить оператор перевода денежный средств, чтобы проверить и подтвердить, что транзакция совершается с санкции клиента. Какие именно действия — зависит от того, что написано в договоре обслуживания. Если эти процедуры выполнены, оператор обязан совершить денежный перевод.

Третья значимая новация ФЗ-167 — формирование правовой базы для информационного обмена об участниках схем хищений денежных средств в электронных платёжных системах. Речь идёт о реквизитах банковских счетов, используемых злоумышленниками, их владельцах — физических и юридических лицах. Неформально такой обмен вёлся и раньше, но лишь там и тогда, когда у сотрудников разных банков возникало такое желание и им удавалось договориться друг с другом. Для такого информационного обмена не было необходимой правовой основы, его участникам могли угрожать санкции.

Задача ФЗ-167 — легализовать и формализовать обмен такой информацией, а в последующем превратить в систему обязательного характера. Теперь такие возможности появились: попытка хищения электронных денежных средств выводит злоумышленника из режима банковской тайны. Согласно ФЗ-167, Банк России может получать такую информацию и доводить её до разных организаций.

Банк России давно технически и организационно готовился к подобной работе, дело было только за принятием соответствующего федерального закона. Проект определения и организации информационного обмена о попытках несанк-

ционированных транзакций, формирования общей базы данных («Фид-Антифрод») был запущен и до конца 2018 года заработает на полную мощность.

Четвёртая новация ФЗ-167 — крайне важная — расширение полномочий Банка России по регулированию информационной безопасности не только банков, но и всех подведомственных финансовых организаций. Вплоть до микрофинансовых организаций, сельскохозяйственных кредитных потребительских кооперативов и ломбардов, а также не кредитных финансовых организаций — страховых, инвестиционных, брокеров, платёжных систем, пенсионных фондов.

ЛИКВИДАЦИЯ ГЛАВНОЙ БРЕШИ

Несмотря на значительные различия в профилях деятельности, всем финансовым организациям угрожают одинаковые риски информационной безопасности — нарушения целостности, доступности и конфиденциальности информации, фрод и т.п. Наглядный пример — ранее существовавшие многочисленные утечки баз данных клиентов страховых компаний — доказывают необходимость усилить государственное регулирование информационной безопасности всех финансовых организаций.

Нормы обеспечения информационной безопасности для крупных и малых финансовых организаций уже конструктивно обсуждались на заседаниях Технического комитета № 122 «Стандарты финансовых операций». Со временем этим стандартам может быть придан статус государственных — ГОСТ Р. Тогда, при соответствующих ссылках в нормативных документах, их нормы превратятся из рекомендательных в обязательные. Большинство технических терминов перемещаются из нормативных документов в тексты государственных стандартов.

Исследования методов деятельности злоумышленников, проведённые Банком России, привели к следующему выводу. Они не нападают на платёжные сервисы как таковые, а решают триединую задачу. Атакуют IT-инфраструктуру финансовой организации, захватывают управление и осуществляют нужные им операции. Такая методика используется независимо от типа и профиля объекта атаки, будь то банк или страховая компания, физическое или юридическое лицо.

Ранее у Банка России были полномочия формулировать требования к информационной безопасности только переводов денежных средств, но не к IT-инфраструктуре организаций, посредством которой они осуществляются. Но именно IT-инфраструктура финансовых организаций оказалась звеном, наиболее уязвимым для злоумышленников. ФЗ-167 помогает ликвидировать эту брешь: Банк России обрёл полномочия устанавливать требования к информационной безопасности IT-инфраструктуры финансовых организаций. По согласованию с двумя другими государственными регуляторами отрасли — ФСБ России и ФСТЭК России.

СНИЖЕНИЕ ДО ПРИЕМЛЕМОГО УРОВНЯ

Теперь о ключевых изменениях в Положении Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». Нормативные нововведения дополняют 167-ФЗ и рука об руку идут со статьями федерального закона.

Основная цель новшеств — снизить процент несанкционированных транзакций до минимального, приемлемого уровня. За 2017 год уровень мошеннических операций, совершённых с использованием платёжных карт, удалось сократить. По данным ФинЦЕРТ Банка России, он составил 0,0016%. Задача в том, чтобы снизить эту долю в общем объёме транзакций до 0,0005%.

Какие новые обязанности по обеспечению информационной безопасности появились у участников финансовой сферы? Теперь операторы электронных платежей в обязательном порядке должны информировать ФинЦЕРТ Банка России об инцидентах. Прежде участие в информационном обмене было добровольным, и количество участников достигло почти семисот.

После обновления 382-П такое информирование стало обязательным, что отвечает нормам Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ. Согласно этому закону, все финансовые организации, любые — от системообразующих банков до ломбардов — относятся к объектам критической инфраструктуры (КИИ) со всеми вытекающими последствиями, включая обязанность информирования государственного регулятора об инцидентах.

В 382-П нет конкретизации механизма обмена информацией об инцидентах и данными дропперов. Этот механизм и его формат прошли согласование с ФСБ России и обсуждение в органах стандартизации. О чём финансовые организации были уведомлены информационным письмом с организационно-техническими рекомендациями внедрения.

Субъекты Национальной платёжной системы обязуются противодействовать компьютерным атакам, направленным как на их инфраструктуру, так и на устройства клиентов. В собственной инфраструктуре выявлять и устранять уязвимости на двух уровнях: инфраструктурном (операци-

Банк России обрёл полномочия устанавливать требования к информационной безопасности IT-инфраструктуры финансовых организаций по согласованию с двумя другими государственными регуляторами отрасли — ФСБ России и ФСТЭК России

К 2024 году все HSM должны производиться в России и поддерживать алгоритмы шифрования не только зарубежные, но и российские

онные системы, СУБД, телекоммуникации) и прикладном (сертификация по российскому законодательству). Противодействие атакам на клиента включает дополнительные процедуры его идентификации и подтверждения транзакций, а также использование для этого раздельных технологий и возможность ограничения параметров финансовых операций.

ПЕРЕХОД НА ОТЕЧЕСТВЕННУЮ КРИПТОГРАФИЮ

Следующая нормативная новация обновлённого 382-П — создание основы технологической независимости национальной платёжной системы — имеет отложенные сроки действия до 2024 и до 2031 годов. Это требование использовать в национальной платёжной системе только отечественные аппаратные средства криптографической защиты информации. К 2024 году все HSM (Hardware Security Module) — аппаратные модули криптографической защиты, работающие в ключевых узлах платёжных систем, — должны производиться в России и поддерживать алгоритмы шифрования не только зарубежные, но и российские. В том числе и в процессах, которые обслуживают операции международных платёжных систем VISA и MasterCard. С картами национальной платёжной системы «Мир» уже работает отечественное оборудование.

Это требование важно в условиях возможных новых зарубежных санкций, учитывая, что аппаратные средства криптографической защиты информации — двойного назначения. Нет гарантий, что иностранные производители, два из которых являются крупнейшими глобальными монополистами, в «час икс» не наложат ограничения на дальнейшие поставки, поддержку техники или на длину криптографического ключа и снизят надёжность уже используемого в России оборудования. Нельзя допустить, чтобы платёжные карты россиян вдруг перестали работать из-за ненадёжных зарубежных поставщиков.

Чтобы обезопасить себя на подобный случай, придётся провести сложные технические мероприятия, на что отводится срок до 2024 года. Россия как страна, как государство должна быть суверенной, независимой, в том числе и в проведении электронных платежей. Есть как минимум три отечественные компании, готовые производить и поставлять требуемое оборудование. Предстоит большая работа, чтобы их продукция получила международную сертификацию, для чего потребуется помощь государства. Конкуренция за рубежом высока, и нас там никто не ждёт.

Второй отложенный срок — 2031 год, к этому времени вся инфраструктура платёжных карт должна работать с отечественными средствами криптографической защиты. Программа «Цифровая экономика Российской Федерации», утверждённая Распоряжением Правительства РФ от 28 июля 2017 года № 1632-р, включает необходимые для этого мероприятия. Предстоящие перемены готовились как логическое развитие предшествующих действий.

Предложения разрабатывались с участием рабочей группы Банка России, в которую входили эксперты из ФСБ России, Министерства промышленности и торговли РФ и Министерства цифрового развития, связи и массовых коммуникаций РФ, а также представители пяти крупнейших банков. Детально, по пунктам исследовались перспективы перевода современных платёжных технологий на отечественную базу, обеспечения безопасности, необходимые затраты. Банки оценили предполагаемые затраты как несущественные для себя, в границах обычных вложений в модернизацию инфраструктуры.

ГАРАНТИРОВАННАЯ ЗАЩИТА ПЛАТЕЖА

Ещё одна новация в 382-П — переход к внешней оценке реальной защищённости платёжных средств и технологий, используемых для денежных переводов. Раньше финансовая организация могла делать самооценку, но теперь этого совершенно недостаточно. Также появилась обязанность финансовых организаций проводить тесты на проникновение. Для большинства финансовых организаций это требование не внове. В рамках стандарта платёжных карт PCI DSS они подобные процедуры уже проводили. Новация 382-П в том, что такие же процедуры распространяются на все технологии передачи финансовых сообщений.

Для повышения надёжности защиты предлагается разделить два контура — подготовки и подтверждения платёжного поручения. Не нужно думать, что для этого пользователю обязательно понадобятся два мобильных телефона. Есть много других вариантов, когда при совершении операций через интернет оператор может гарантировать защищённость механизма перечисления клиентских денежных средств от воздействия вредоносного кода.

Оператор самостоятельно определяет, какими средствами решить эту задачу. Например, некоторые банки встраивают в свои мобильные приложения антивирусы, средства анализа защищённости устройства клиента. Для юридических лиц удобнее, может быть, специальное дополнительное устройство, на которое приходит контрольная информация для дополнительного подтверждения, одноразовый пароль.

* * *

Ещё одно важное новшество — информирование банками ФинЦЕРТа Банка России обо всех инцидентах информационной безопасности стало обязательным. Среди обязательных показателей отчётности остаются экономические, чтобы был понятен масштаб и значение инцидента. Передача этой информации будет осуществляться через автоматизированную систему, которая уже запущена в промышленную эксплуатацию и выйдет на полную проектную мощность к концу 2018 года.

Артем КАЛАШНИКОВ
руководитель ФинЦЕРТ
Банка России

ФИНЦЕРТ И БАНКИ: ОБМЕН СТАЛ ПРОЩЕ

ЧТО ИЗМЕНИЛОСЬ В ПРОЦЕДУРЕ ОБМЕНА ИНФОРМАЦИЕЙ О КИБЕРИНЦИДЕНТАХ МЕЖДУ БАНКАМИ И ФИНЦЕРТ ПОСЛЕ 26 СЕНТЯБРЯ?

Федеральный закон от 27 июня 2018 года № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств», Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и новая редакция Положения Банка России № 382-П от 9 июня 2012 года стали важными вехами развития нормативно-правовой базы информационной безопасности финансовой сферы.

УСТРАНЕНИЕ ПРОБЕЛОВ

Пять лет назад серьёзный всплеск хищений денежных средств со счетов физических и юридических лиц выявил ряд пробелов в сфере безопасности электронных платежей. Оказалось, что у банков нет ни четкого понимания, с чем и с кем им нужно бороться, ни юридического инструментария для такой борьбы. Сотрудники некоторых банков договаривались между собой об обмене данными об участниках схем хищений денежных средств («дропперах»), однако формально это было вне правового поля. Более того — участникам такого обмена могли угрожать санкции за разглашение конфиденциальной информации. Но даже если банки шли на такой риск и благодаря полученной от коллег информации обнаруживали сомнительные транзакции — правовые основы определения, приостановки и возврата таких платежей также отсутствовали.

Эту проблему решило принятие трех взаимодополняющих правовых документов, которые не только создали нормативную основу для легализации обмена данными об инцидентах в электронных платёжных системах, но и установили прямую обязанность кредитных организаций предоставлять такие данные в Центр мониторинга и реагирования на компьютерные атаки в финансовой сфере ЦБ РФ (ФинЦЕРТ). Налаженный информационный обмен с ФинЦЕРТ, в свою очередь, создает основу для упрощения выполнения банками требований закона о безопасности критической информационной инфраструктуры (КИИ) РФ, который обязывает банки как субъекты КИИ предоставлять информацию об инцидентах в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

Сейчас Банк России и ФСБ России разрабатывают нормативные документы, которые позволят ФинЦЕРТ выполнять функции ведомственного («отраслевого») центра ГосСОПКА в финансовой сфере, а участникам отрасли — избежать двойной отчётности в вопросах безопасности КИИ.

ЧТО ИМЕННО ИЗМЕНИЛОСЬ?

Первое и главное — поправки в закон «О национальной платежной системе», введенные 167-ФЗ, обязывают банки, платежные системы и операторов услуг платежной инфраструктуры информировать ЦБ обо всех случаях или попытках совершения несанкционированных переводов. Также новый закон легализует и формализует обмен сведениями об операциях, о счетах и вкладах, в отношении которых были зафиксированы случаи и (или) попытки осуществления переводов денежных средств без согласия клиента (в том числе с точки зрения нераспространения на него режима банковской тайны). Указанные данные кредитные организации должны предоставлять в Банк России, который, в свою очередь, будет проводить экспертизу полученных данных и в зависимости от ее результатов доводить информацию об угрозе до участников информационного обмена.

Второй блок нововведений касается предоставления в ЦБ технических данных, описывающих характеристики компьютерных атак, в формате, удобном для ГосСОПКА.

После принятия нового закона, в его развитие, Банком России будут изданы подзаконные нормативные акты, модернизирован стандарт обмена информацией с ФинЦЕРТом. Это откроет возможность работы в расширенном, более эффективном формате.

В 382-П ранее была уже установлена обязанность для ОПДС, ОПС, ОУПИ по выполнению требований к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагирования на них. Новая редакция Положения обязывает их также сообщать регулятору о намерении раскрыть информацию об инцидентах на своих официальных сайтах, в пресс-релизах или на пресс-конференциях как минимум за один рабочий день.

АСОИ

Чтобы упростить для банков процесс формирования и предоставления увеличившегося объема отчетности, ФинЦЕРТ запустил автоматизированную систему обработки инцидентов (АСОИ), в рамках которой будет создана общая база данных о данных счетов «дропперов» «Фид-Антифрод». В будущем пользоваться ею смогут остальные финансовые организации, для которых предоставление такой информации также будет становиться обязательным.

К АСОИ уже подключены все кредитные и многие некредитные организации (НКО, РНКО), имеющие лицензию, а также ряд иных организаций, являвшихся ранее участниками обмена информацией с ФинЦЕРТ.

Изменения в законодательстве, а также замена слабо защищенного канала взаимодействия (электронной почты) на сервис личных кабинетов АСОИ ФинЦЕРТ, обладающий персонифицированным доступом и криптографической защитой канала связи, уже привели к существенному увеличению (более чем в два раза) потока сообщений о событиях и инцидентах, получаемому ФинЦЕРТ.

ИЗ ЧЕГО СОСТОИТ АСОИ?

АСОИ ФинЦЕРТ 1-й очереди состоит из информационного портала, сервиса личных кабинетов, специализированных технологических подсистем и защищенной инфраструктуры, что позволяет реализовать процессы:

- получения данных от Участника (информации об инцидентах в организации и её клиентах, выявленных уязвимостях, угрозах, данных о раскрытии информации, запросах);
- передачи информации участнику и его оперативному информированию об актуальных угрозах ИБ в КФС (в том числе путем направления соответствующих бюллетеней);
- оперативного взаимодействия между участником и ФинЦЕРТ по соответствующим инцидентам и запросам;
- мониторинга атак на организации КФС;
- поддержки взаимодействия ФинЦЕРТ с регистраторами и хостерами по инициации разделегирования/блокировки мошеннических и вредоносных ресурсов.

АСОИ ФинЦЕРТ поддерживает получение информации как в унаследованном формате (файлы формата xlsx (формы INT, EXT и PUB) для передачи данных участников информационного обмена, содержащие информацию об инцидентах[1]), так и в современном формате (файлы формата json).

Прием информации от УИО в АСОИ ФинЦЕРТ может быть осуществлен следующими путями:

- заполнения интерактивных форм в личном кабинете;
- передачи информации в виде json-файлов, оформленных в соответствии с проектом стандарта «Технология подготовки, направления и формы электронных сообщений для информационного обмена с Банком России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации»[2] в личном кабинете (автоматизированный пакетный режим) или по e-mail (резервный канал);
- передачи информации в xlsx-файлах, соответствующих формам INT, EXT и PUB[3] в личном кабинете (автоматизированный пакетный режим) или по e-mail (резервный канал).

* * *

В целях выполнения норм Федерального закона от 27.06.2018 № 167-ФЗ (в части создания базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента и обеспечения возможности получения кредитными организациями данных из этой базы), на инфраструктурно-технологической платформе АСОИ ФинЦЕРТ Банком России создается АС «Фид-АнтиФрод». Прототип данной системы введен в эксплуатацию 27.09.2018 и реализует ряд базовых функций, обеспечивающих получение необходимой информации, взаимодействие с участниками информационного обмена по получению необходимой информации и формирование базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента.

[1] Порядок заполнения информации об инцидентах приведен во Временном регламенте передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (*http://cbr.ru/StaticHtml/File/14408/inforegl_23.pdf*) Формы INT, EXT и PUB опубликованы на сайте Банка России в разделе ФинЦЕРТ *https://cbr.ru/fincert/*, данные формы являются унаследованными и после перехода на стандарт «Технология подготовки, направления и формы электронных сообщений для информационного обмена с Банком России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации» они будут отменены.

[2] По состоянию на октябрь 2018 проект стандарта завершает процедуру его оформления.

[3] Порядок заполнения информации об инцидентах приведен во Временном регламенте передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (*http://cbr.ru/StaticHtml/File/14408/inforegl_23.pdf*). Формы INT, EXT и PUB опубликованы на сайте Банка России в разделе ФинЦЕРТ (*https://cbr.ru/fincert/*), данные формы являются унаследованными и после перехода на стандарт «Технология подготовки, направления и формы электронных сообщений для информационного обмена с Банком России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации» они будут отменены.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНСТИТУТ ЭКОНОМИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ITM
ШКОЛА IT-МЕНЕДЖМЕНТА

Для тех, кто готов подняться на новую высоту.

CIO MBA: Информационный менеджмент

CISO MBA: Информационная безопасность

PM+BI IT-МЕНЕДЖЕР: Менеджер проектов, Бизнес-аналитик

PM+IS Управление корпоративной информационной безопасностью

CEEMAN — IAC International Academy of CIO

- Первое место среди программ MBA по практикоориентированности по исследованию портала mba.su
- Программа MBA-CIO первой в России получила сертификат профессионально-общественной аккредитации на соответствие проф. стандарту
- Выпускники программы MBA-CIO получают диплом MBA и международный сертификат IAC (International Academy of CIO)
- Школа IT-менеджмента член международных ассоциаций CEEMAN и IAC
- Школа IT-менеджмента входит в ТОП-10 ведущих MBA программ России

119571, Россия, г. Москва,
проспект Вернадского 82
корп. 2, офис 126

+7 (495) 937 02 94
+7 (495) 933 96 00

info@itmane.ru
itm.ranepa.ru (сайт Школы)
ranepa.ru (сайт РАНХиГС)

Сергей ЛЕБЕДЬ
руководитель Службы кибербезопасности Сбербанка

КИБЕРБЕЗОПАСНИКИ ВСЕХ СТРАН, ОБЪЕДИНЯЙТЕСЬ!

СЕРГЕЙ ЛЕБЕДЬ РАССКАЗЫВАЕТ BIS JOURNAL О МЕЖДУНАРОДНЫХ ИНИЦИАТИВАХ СБЕРБАНКА В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

— Сергей Васильевич, Сбербанк становится флагманом в сфере ИБ не только на просторах отечества, но и в международном масштабе. В июле банк провёл Международный конгресс по кибербезопасности. Расскажите, пожалуйста, получилось ли достичь поставленных целей?

— Очевидно, что обеспечение кибербезопасности требует пристального внимания на самом высоком уровне. Масштабные вирусные атаки и крупнейшие хищения последних лет стали хорошим стресс-тестом для мирового сообщества, встряхнули его и заставили задуматься о мерах противодействия.

В Сбербанке кибербезопасность стала одним из стратегических приоритетов развития около четырех лет назад. И мы пришли к выводу, что должны эффективнее реагировать на кибератаки и запускать постоянно обновляющиеся механизмы проактивной защиты. Из-за глобальной природы киберпреступности, доступности технологий нападения справиться в одиночку с проблемой киберугроз не может ни одна компания. Но сделать цифровой мир безопаснее возможно, если объединить усилия бизнеса, государств и экспертов.

Именно эта вера привела нас к мысли организовать Международный конгресс по кибербезопасности, который прошёл в июле. Для нас организация подобного мероприятия была совершенно новым опытом. В очень сжатые сроки нам необходимо было решить весьма амбициозную задачу — создать площадку для объединения мирового сообщества перед лицом всё нарастающих киберугроз. Чтобы решить эту задачу, мы должны были в первую очередь сформировать самую злободневную повестку, угадать самые горячие темы. Здесь нам помог наш собственный опыт борьбы с киберпреступностью: ведь именно бизнес — главный объект киберугроз, а Сбербанк — цель № 1 в России для киберпреступников. И, конечно, нужно было собрать максимально представительный экспертный состав участников и спикеров.

У нас получилось. Свыше 2200 участников, около 700 организаций, более 50 стран — масштаб очевиден. И, конечно, особое настроение и значимость конгрессу придало присутствие на нём Владимира Путина.

На самом высоком уровне признан термин «кибербезопасность», и это очень важно. Мы живем в век цифровой революции, и сегодня организации ведут свою деятельность в киберпространстве и актуальность угроз, возникающих для них гораздо выше угроз «классической» информационной безопасности. Поэтому термин «кибербезопасность» наиболее точно отражает дух времени, суть функции, обеспечивающей защиту цифровой организации.

Озвучил Президент и необходимые меры по повышению безопасности киберсферы, и это важное событие для нас, для России и международного сообщества. Прозвучала мысль о необходимости единого ответственного за кибербезопасность в стране, и мы с нетерпением ждем, когда произойдут эти изменения, и всем нам удастся консолидировать усилия и быстрее добиваться результата.

Наконец, привлечено внимание к ключевым вопросам кибербезопасности, в том числе к вопросу кибергигиены.

Повторюсь, что главной нашей задачей было создание площадки, которая поможет объединить усилия в области кибербезопасности в

Свыше 2200 участников, около 700 организаций, более 50 стран — масштаб очевиден. И, конечно, особое настроение и значимость конгрессу придало присутствие на нём Владимира Путина

Выступление Владимира Путина на пленарном заседании Международного конгресса по кибербезопасности. Фото: Михаил Метцель, ТАСС (kremlin.ru)

глобальном масштабе. Мы понимаем, что принести желаемые результаты подобное мероприятие может только на регулярной основе, и поэтому уже сейчас приступили к подготовке следующего конгресса, который состоится 20–21 июня 2019 года в Москве.

Что касается непосредственно Сбербанка, то мы в рамках конгресса подписали соглашение о сотрудничестве в области кибербезопасности со Всемирным экономическим форумом. А немногим позже вошли в число партнёров-основателей Центра по кибербезопасности ВЭФ.

— С какой концепцией и программой Сбербанк стал первым из шести партнёров-основателей Центра кибербезопасности Всемирного экономического форума?

— Мы с самого начала принимали активное участие в создании Центра, который становится площадкой для коллаборации мировых бизнес-лидеров, ключевых игроков на международном рынке кибербезопасности и представителей правоохранительных органов с целью противодействия глобальной киберпреступности. Мы с готовностью делимся опытом и информацией с мировым сообществом, поэтому одним из первых наших предложений, вынесенных на обсуждение в Центре по кибербезопасности ВЭФ (C4C), была реализация автоматизированного обмена данными между членами Центра. В состав участников C4C входят крупнейшие глобальные корпорации, которым приходится ежедневно бороться с огромным количеством кибератак. Каждая из них может поделиться уникальным опытом по противодействию киберпреступлениям и помочь предотвратить заражения других членов Центра. Участники C4C, в свою очередь, способны распространить эту информацию дальше, в рамках своей отрасли и страны, способствуя повышению защищённости международного сообщества.

— Можете ли вы охарактеризовать ситуацию с кибербезопасностью в России и в мире в целом?

— Конгресс помог нам прийти к нескольким важным выводам. Во-первых, потери мировой экономики и России от киберпреступности беспрецедентны и продолжают постоянно расти. В 2017 году, по данным ВЭФ, общие мировые потери от кибератак составили $1 трлн. Этот показатель растёт год от года: ВЭФ прогнозирует, что через несколько лет эти потери могут достичь $8 трлн. По оценке Сбербанка, потери России в 2017 году составили $10 млрд и мы видим, что и в нашей стране эти суммы становятся всё больше.

Во-вторых, кибербезопасность отстаёт на 2–5 лет от развития технологий. Цифровые компании используют новейшие технологии: искусственный интеллект, большие данные,

Пленарная сессия «Транспарентный цифровой мир — ловушка или благо?». Фото: www.icc.moscow

машинное обучение, интернет вещей, однако наработанный практический опыт обеспечения безопасности таких технологий пока отсутствует. Более того, по ряду причин недостаточно хорошо обеспечивается кибербезопасность и традиционных технологий. В-третьих, остро не хватает квалифицированных кадров. Мировой дефицит специалистов в области кибербезопасности к 2022 году составит 1,8 млн.

Наконец, сегодня киберпреступники чувствуют себя безнаказанно. У них нет национальных границ, они действуют на глобальном уровне, хорошо организованы, их преступления трудно доказывать в судах. Для успешной борьбы с киберпреступностью необходимо эффективное международное сотрудничество.

— Что позволяет структуре кибербезопасности Сбербанка ощущать себя лидером как внутри страны, так и за её пределами?

— Мы соревнуемся сами с собой: постоянно повышаем для себя планку, что заставляет нас всё время расти. Делать это нас мотивируют доверие миллионов наших клиентов и ответственность перед ними. В своей работе мы руководствуемся несколькими приоритетами.

Во-первых, это люди. В кибербезопасности всё упирается в профессионализм команды, знания и компетенции каждого сотрудника. Мы развиваем команду Службы кибербезопасности и помогаем всей огромной команде Сбербанка освоить и успешно применять навыки, необходимые для личной киберзащиты и киберзащиты банка в целом.

Во-вторых, процессы — при масштабах Сбербанка линейное увеличение численности специалистов и масштабное внедрение технологий защиты без выстроенных процессов результата принести не может. Мы создали крупнейший в Европе банковский SOC, с помощью которого мы непрерывно отслеживаем и оцениваем обстановку в режиме реального времени, прогнозируем кризисные ситуации и моментально реагируем на киберугрозы. Возможности Центра позволяют одновременно контролировать все бизнес-системы и средства защиты банка. Это достигается в том числе благодаря сбору, анализу и обработке в реальном времени данных от более чем 500 тыс. источников — элементов инфраструктуры банка, суммарный объём которых превышает 3 млрд событий в сутки.

Кстати, наш SOC стал первым подобным банковским центром в России, который сертифицирован Британским институтом стандартов на соответствие международному стандарту ISO 27001:2013. Этот сертификат с одной стороны подтверждает, что процессы мониторинга и реагирования на кибератаки банка соответствуют международным требованиям, с другой — обязывает нас соответствовать высокому уровню и постоянно развивать и совершенствовать свои процессы.

И ещё один наш приоритет — постоянные улучшения, применение передовых подходов и практик, регулярный их мониторинг и анализ. Мы построили уникальную экосистему кибербезопасности на уровне мировых лидеров и сегодня обеспечиваем 0 минут простоя банковских систем и сервисов от DDoS-атак и бесперебойное обслуживание клиентов. Но при этом считаем абсолютно невозможным останавливаться на достигнутом. Мы постоянно анализируем рынок, новые системы и решения, и стараемся использовать в своей работе лучшее, что есть на сегодняшний день.

— На конгрессе в очередной раз прозвучала мысль об изначально встроенном ИБ-иммунитете в IT-проекты и IT-продукты, но достойного ответа со стороны профессионального сообщества, как обычно, не прозвучало. Эта мысль звучит не впервые, кажется здравой, но почему-то не поддерживается и не опровергается. Просто замалчивается. Почему?

— Мы убеждены, что безопасность проекта или продукта должна быть встроена изначально. У меня нет ощущения, что вопрос о встроенной безопасности замалчивается. Другое дело — не все разработчики умеют работать по этому принципу, не во всех компаниях взаимодействие между владельцами продукта и «безопасниками» заложено на уровне культуры бизнеса, далеко не везде к безопасности применяется комплексный подход. Думаю, что все точки над «i" здесь расставит рынок: безопасность продукта становится его конкурентным преимуществом. В результате преимущество получают разработчики, которые задумываются о безопасности и инвестируют в неё ещё на этапе создания концепции продукта.

Однако важно понимать, что безопасность отдельно взятого продукта — это далеко не всё. Продукт — часть цифровой среды, у которой есть ещё множество составляющих. Поэтому правильнее всего говорить о безопасности цифровой среды в целом. И, естественно, не просто говорить, а всерьёз заниматься этим вопросом.

Мы построили уникальную экосистему кибербезопасности на уровне мировых лидеров и сегодня обеспечиваем 0 минут простоя банковских систем и сервисов от DDoS-атак и бесперебойное обслуживание клиентов

— Что бы вы хотели изменить в мире кибербезопасности? Насколько это осуществимо?

— На мой взгляд, сегодня уже невозможно говорить о «мире кибербезопасности» как о чём-то замкнутом. Дело в том, что кибербезопасность касается практически каждого, другой вопрос — далеко не все пока это осознали. Отсюда вытекает и «верхнеуровневая» цель — сформировать в России культуру кибербезопасности. Мы обучаем наших клиентов, снабжаем их навыками защиты от кибермошенников. Объясняем им, что без их осознанного участия в собственной киберзащите эту задачу решить невозможно. Конечно, это небыстрый процесс — ведь речь идёт о том, чтобы поменять образ мысли, а такие задачи в одночасье не решаются. При этом история демонстрирует нам схожие трансформации: к примеру, человечество научилось чистить зубы и мыть руки перед едой, безопасным образом переходить дорогу.

Разумеется, должны расти и компетенции руководителей компаний в области кибербезопасности, и интеграторов, и, конечно же, профессионального сообщества в целом. Радует, что мы видим реальные сдвиги в мышлении, поведении, и они позволяют нам смотреть в будущее с оптимизмом.

Что касается работы нашей Службы кибербезопасности, то одна из главных задач, которую я ставлю перед собой, — это развитие нашей команды. Мы в целом и каждый из нас по отдельности должны постоянно расти над собой, повышать уровень знаний, развивать ключевые профессиональные и личностные компетенции.

И ещё один момент, который нельзя обойти, — это проблема разрыва между высшей школой и бизнесом. Наши вузы не в состоянии готовить качественных специалистов в области кибербезопасности — они находятся в «другом измерении», они совершенно не успевают за ходом времени. О причинах этой проблемы и путях её решения можно долго говорить — это тема для отдельной беседы. Но если мы её не решим, то успех борьбы с киберпреступностью окажется под большим вопросом.

Иван ЯНСОН
бизнес–партнер по информационной безопасности Сбербанка

ПРАВО НА ЕИСПСА

СОТРУДНИЧЕСТВО БАНКОВ И ОПЕРАТОРОВ СОТОВОЙ СВЯЗИ В БОРЬБЕ С МОШЕННИЧЕСТВОМ

Банки регулярно пользуются услугами операторов сотовой связи при обслуживании клиентов. Но в определённых случаях сервисы операторов могут быть использованы и злоумышленниками для атак на клиентов банков. Такие случаипривели к необходимости совместной работы банков и операторов по обеспечению безопасности своих клиентов и сервисов. Первым наиболее значимыммоментом в истории совместного противодействия банков и операторов сотовой связи мошенничеству в системах дистанционного банковского обслуживания (ДБО) была история, связанная с подменой сим-карт у клиентов.

ПОДМЕНА СИМ-КАРТ

Поскольку многие системы ДБО используют для подтверждения платежей и/или для подтверждения входа в систему разовые пароли, направляемые с помощью СМС-сообщений, то появился такой вид мошенничества, как атака на клиента с использованием подмены сим-карт. В результате таких атак у мошенников оказывается мобильный номер, принадлежащий клиенту. Если они при этом сумели завладеть и другими реквизитами, то могут войти в систему ДБО от имени клиента, создать и подтвердить платежи — ведь они сами же и получат разовые пароли для подтверждения. Клиент при этом не подозревает о том, что происходит, потому что в этот момент его сим-карта неактивна, телефон молчит. Он может только обратить внимание на то, что ему долго никто не звонит. Когда клиент догадывается о проблеме, он обращается к оператору и выясняет, что у него произошла смена сим-карты. Потом он может обнаружить, что в период смены сим-карты были списаны деньги в интернет- или мобильном банке.

Таким образом, у банков появилась потребность получать информацию о смене сим-карт и запрашивать у клиента подтверждение легитимности события.

Атака методом подмены сим-карты привела и к изменениям Положения Банка России 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств…». В Положении появился пункт 2.8.8, который обязывает банк в случае, если ему стало известно о признаках, указывающих на изменение получателя информации, направленной оператором по переводу денежных средств и используемой при аутентификации клиента, приостанавливать пересылку таких сообщений и осуществление переводов в системе ДБО. К указанным признакам может быть отнесена информация о замене сим-карты клиента, прекращении обслуживания или смене номера телефона, указанного в договоре с клиентом.

ПЕРВЫЕ ШАГИ ПО ИНФООБМЕНУ

Для защиты платежей в системах ДБО Сбербанк и другие банки обратились к операторам сотовой связи и компаниям, через которые в то время банки в основном направляли СМС-сообщения: к так называемым СМС-агрегаторам. Произошло это в 2008 году после массовой атаки по подмене сим-карт на клиентов одного из банков. У операторов сотовой связи тогда ещё не было сервисов по отслеживанию смены сим- карт, и в целом они не были особо заинтересованы в оказании такой услуги банкам. Что касается агрегаторов, то они довольно быстро сумели предложить подходящую услугу. Суть её состояла в том, что агрегаторы могли в ответ на запрос банка предоставить хэш-значение идентификатора IMSI, который хранится на сим-карте и при смене сим-карты тоже меняется. Этот идентификатор брался из сигнальных сетей операторов, которые в то время были полностью открыты для агрегаторов. Услуга по предоставлению хэша IMSI позволяет банку отследить смену сим-карт.

Как это делается? Банк создаёт базу хэш-значений идентификаторов IMSI, и когда клиент производит операцию в системе ДБО, запрашивает у агрегатора текущее значение хэша. Если оно отличается от хранимого в базе, то возникает подозрение на смену сим-карты. В результате операция приостанавливается, и банк просит клиента подтвердить легитимность смены сим-карты лично в банковском отделении.

Минус такой интеграции в том, что банку приходится запрашивать информацию каждый раз, когда клиент совершает операцию в системе ДБО. Банку приходится платить за каждый такой запрос и нагружать ими как свои системы, так и системы агрегаторов. Но этот первый шаг

по информационному обмену стал безусловным прогрессом по сравнению с полным отсутствием информации и решал задачу противодействия фроду. Кроме того, банкам было удобно интегрироваться с одним агрегатором, не озадачиваясь интеграцией со всеми операторами.

РАЗВИТИЕ ИНФООБМЕНА

Но через несколько лет (примерно в 2013–2014 годах) банки начали вести переговоры непосредственно с операторами сотовой связи. С одной стороны, у банков было желание оптимизировать затраты на получение информации и не платить за запрос хэш-значения IMSI при каждой операции в ДБО. С другой стороны, мошенники начали использовать новые способы атак на клиентов. Например, появились вирусы для смартфонов, которые умели перехватывать пароли для подтверждения операций в системах ДБО и позволяли мошенникам подтверждать несанкционированные операции, скрывая их от клиентов. Соответственно, возникла потребность в дополнительной информации, свидетельствующей о несанкционированном доступе или об управлении мобильным устройством клиента мошенниками (например, информации о заражении мобильных устройств), которой СМС-агрегаторы в принципе не располагают, так как она доступна только операторам. Кроме того, операторы стали ограничивать доступ агрегаторов к своим сигнальным сетям, в связи с чем банкам пришлось обращаться за услугой по предоставлению хэша IMSI непосредственно к операторам.

В результате Сбербанк и другие банки вместе с операторами сотовой связи на базе нескольких банковских ассоциаций создали рабочие группы по информационному обмену в целях защиты операций клиентов в системах ДБО.

В процессе совместной работы банки и операторы определили перечень событий, потенциально свидетельствующих о доступе или управлении мобильным устройством третьими лицами. Такими индикаторами могут быть следующие события:

- смена абонентом телефонного номера;
- переход абонента к другому оператору;
- изменение владельца номера;
- переадресация голосового вызова;
- замена сим-карты или абонентского устройства;
- расторжение договора и приостановление оказания услуг;
- подозрение на заражение абонентского устройства вредоносным ПО;
- смена операционной системы мобильного устройства и самого устройства.

Причём Сбербанк и другие банки отметили, что в большинстве случаев события удобнее получать в режиме мониторинга, а не в режиме запроса, так как такой режим меньше нагружает автоматизированные системы банков и операторов и позволяет быстрее, почти в онлайн-режиме, получать информацию о потенциально рисковых событиях. Операторы и банки договорились о протоколе информационного обмена и со временем реализовали в своих системах сервисы по автоматизированному обмену информацией о перечисленных выше событиях. В настоящее время ряд банков уже ведёт инфообмен в рамках прямых договорных отношений с отдельными операторами. Однако если в технологическом плане у такого взаимодействия особых проблем не возникло, то остались неразрешёнными некоторые правовые вопросы. Речь идёт о правовом статусе передаваемой информации.

ПРАВОВОЙ СТАТУС ИНФООБМЕНА

При проработке способов информационного обмена банки и операторы рассматривали не только возможный перечень событий, которые могут свидетельствовать о нарушении безопасности мобильных устройств клиентов, и не только технологические вопросы обмена информацией о таких событиях, но и правовые вопросы. Дело в том, что информация, которую мы имеем возможность получать от операторов, может быть отнесена к сведениям об абоненте, а также к персональным данным. Участвовавшие в работе упомянутых рабочих групп по организации информационного обмена юристы операторов указали на то, что есть риск получения претензий от клиентов в связи с тем, что обмен информацией о статусе их обслуживания у операторов, о статусе и состоянии их мобильных устройств осуществляется без их согласия. Другими словами, правовой статус информации о передаваемых событиях и его трактовка стали определённым риск-фактором, который нельзя не учитывать.

Минимизировать этот риск можно, получив согласие абонента, владельца этих данных. Рабочие группы банков и операторов рассмотрели и оценили разные способы получения согласия.

В процессе совместной работы банки и операторы определили перечень событий, потенциально свидетельствующих о доступе или управлении мобильным устройством третьими лицами

ЕИСПСА может использоваться не только для противодействия мошенничеству в сфере ДБО, но ещё и для расширения способов дистанционной идентификации

Если получать его, используя собственноручную подпись, то понятно, что это будет очень неудобно и для банка, и для оператора, и для клиентов. Если добавить согласие в договор оферты о ДБО и попросить клиента подтвердить его простановкой галочки в личном кабинете системы ДБО, это тоже означало бы дополнительные действия для клиента и банка. Поэтому лучше всего было бы, если бы такое согласие не требовалось в принципе. Это позволило бы устранить лишние действия для клиентов, не ухудшать клиентский опыт и создать условия для повышения безопасности всех клиентов, а не только тех, кто согласился. В этой связи Сбербанк и инициативная группа операторов при участии Национальной платёжной ассоциации провели совместную работу по созданию законопроекта, который позволял бы осуществлять такой инфообмен в целях безопасности клиентов без получения отдельных согласий.

Это оказался довольно длинный, но интересный путь, в результате которого законопроект был разработан и отправлен на согласование в Банк России. Изменения предлагалось внести в закон «О связи», так как необходимая информация обрабатывается в автоматизированных системах операторов сотовой связи, и именно операторам в первую очередь необходимо снять вопросы правовой неопределённости. В рамках разработки законопроекта от Минкомсвязи было получено разъяснение о том, что сведения, содержащиеся в информационном обмене[1] в соответствии с требованиями федерального закона «О связи», не относятся к сведениям об абонентах. При этом ведомство отмечало, что предоставление информации о физлицах должно осуществляться с соблюдением требований федерального закона «О персональных данных».

СОЗДАНИЕ ЕИСПСА

В начале 2017 года Банк России предложил идею о создании централизованной системы информационного обмена между банками и операторами — так называемой Единой информационной системы проверки сведений об абоненте (далее ЕИСПСА). Система должна представлять собой специальный шлюз, через который передаются необходимые сведения от операторов банкам. Она сама не хранит данные, а только обеспечивает направление запросов и получение данных. В дополнение к тому перечню данных, который мы привели выше, система позволяет верифицировать данные абонента: направив запрос с номером телефона клиента, его ФИО и номером документа, удостоверяющего личность, можно получить ответ о том, совпадают ли эти сведения с хранимыми у оператора или нет. Таким образом, ЕИСПСА может использоваться не только для противодействия мошенничеству в сфере ДБО, но ещё и для расширения способов дистанционной идентификации при оказании финансовых и иных услуг (при условии достаточной консистентности данных об абонентах в базах данных операторов).

ЗАКОНОПРОЕКТ

Вместе с концепцией централизованной системы информационного обмена Банк России тогда же в 2017 году разработал законопроект об изменении закона «О связи», который вводит понятие упомянутой системы ЕИСПСА. При разработке законопроекта учитывался и упомянутый выше законопроект о прямом информационном обмене, то есть он позволяет кроме информационного обмена через ЕИСПСА и прямой обмен на основании договорных отношений между банками и операторами.

Это важно, так как прямой инфообмен уже технически реализован всеми операторами, многие банки уже сейчас используют его для защиты своих систем ДБО, и необходимо обеспечить правовую основу для его беспрепятственного использования и тиражирования.

В настоящее время законопроект внесён на рассмотрение Государственной думы как проект федерального закона № 514780–7 и опубликован на сайте проектов нормативных правовых актов. Некоторые его положения вызвали бурную дискуссию. Один из дискуссионных пунктов — введение обязанности по проверке сведений о клиентах в ЕИСПСА при проведении процедуры упрощённой идентификации и при отправке СМС-сообщений должникам. Возражения вызывает именно обязанность. Вызвано это, в первую очередь, тем, что данные об абонентах у операторов не полностью актуальны. Происходит это по разным причинам: например, из-за того, что данные устаревают при смене паспортных данных у абонентов, из-за того, что была распространена продажа сим-карт без идентификации абонентов и без заключения с ними договоров, а также из-за того, что многие

[1] Имеются в виду сведения, перечисленные в настоящей статье.

абоненты добросовестно пользуются номерами, зарегистрированными на своих родственников.

Проблема неактуальности сведений об абонентах известна давно, и законодатели уже предприняли шаги по её решению. В июне 2017 года был издан закон № 245-ФЗ «О внесении изменений в Федеральный закон «О связи»», который направлен на обеспечение чистоты данных, имеющихся у операторов о пользователях абонентских номеров. В частности, согласно данному закону с июня 2018 года предусмотрена обязанность запрашивать данные абонентов при заключении договоров и проводить проверку их достоверности. При этом согласие на передачу персональных данных оператору связи не требуется. В целях проверки операторам связи обеспечен доступ к единой системе идентификации и аутентификации, единому порталу госуслуг, другим информационным системам госорганов. Сейчас операторы актуализуют данные и по ранее заключённым договорам, используя ресурсы госорганов через СМЭВ. Но очевидно, что операторам понадобится время на актуализацию данных. Кроме того, остаётся случай добросовестных граждан, которые используют номера своих родственников — о таких случаях государственные базы, включая базу МВД о паспортах, ничего не знают. Всё-таки номер телефона пока ещё не является идентификатором, по которому можно точно установить гражданина. А может быть, никогда таковым и не станет.

Следовательно, при введении обязанности проверки сведений при упрощённой идентификации мы вынуждены будем отказывать части клиентов в проведении операций, при отправке СМС-сообщений должникам не будем оповещать часть клиентов о важной для них и для банка информации. Соответственно, это вызовет отрицательный клиентский опыт в одном случае, а в другом случае может привести к росту просроченной задолженности и даже, может быть, к росту мошенничества.

Кроме того, услуга проверки сведений через ЕИСПСА платна. Очевидно, что операторам потребуется провести интеграцию своих систем с системой ЕИСПСА, а далее им потребуются средства для сопровождения работы с этой системой. Аналогичным образом стартовые и регулярные расходы будут и у самого оператора ЕИСПСА. Применение сервиса не всегда может быть экономически оправдано. Дополнительные затраты банка могут привести к ухудшению тарифов за оказание услуг для клиентов.

КАК ДОПОЛНИТЕЛЬНЫЙ ИСТОЧНИК

Вместе с тем, на наш взгляд, возможность проверки сведений об абонентах может быть полезна банкам как дополнительный источник информации при работе скоринговых и антифрод-систем.

В случае несовпадения данных у оператора и банка можно было бы включать дополнительные контрольные процедуры при подключении услуг, привязанных к конкретным номерам телефонов (например, таких как СМС-банкинг, СМС-оповещение об операциях и т.п.), тем самым проактивно обеспечивая безопасность клиентов и/или банка. Информация операторов об абонентах-клиентах может использоваться в работе антифрод-систем, чтобы улучшить модели этих систем, точнее выявлять мошенников и их активности, снизить число ложных срабатываний и затраты на контроль операций.

Такой сервис потенциально можно использовать и для развития дистанционных услуг. Например, в случае совпадения данных о клиенте, введённых в кредитной заявке, с имеющимися по номеру телефона у оператора, можно было бы дистанционно получать согласие клиента на запрос банком о нём кредитной истории в бюро кредитных историй с помощью его телефона (получив от него ответное СМС-сообщение о согласии).

Кроме того, создание ЕИСПСА обеспечит банки универсальным интерфейсом доступа для работы с операторами. Это большой технологический плюс для всего сообщества, так как даже крупным банкам не под силу напрямую работать со всеми операторами. Появление ЕИСПСА также способствовало бы стандартизации протоколов информационного обмена. Использование опыта крупных операторов и банков может снизить стартовые затраты на создание системы и интеграцию с ней.

* * *

В этой связи мы считаем, что целесообразно создать ЕИСПСА, предоставив банкам право (не обязанность!) работы с данной системой. Также однозначно поддерживаем закрепление права банков и операторов на осуществление информационного обмена перечисленными в настоящей статье видами событий как через ЕИСПСА, так и в рамках прямых договорных отношений, в целях обеспечения безопасности клиентов при работе в системах ДБО. Таким образом, мы предлагаем доработать законопроект с учётом озвученных замечаний и в адаптированном виде утвердить его. Наличие нового закона и создание новой системы позволит банкам и операторам сотовой связи совместно на качественно новом уровне повысить безопасность предоставляемых клиентам дистанционных банковских услуг.

Виктор МИНИН
председатель
правления АРСИБ

ОСТАНОВИТЬ ЦУНАМИ

МОБИЛЬНЫЕ ТЕХНОЛОГИИ И ОБЕСПЕЧЕНИЕ ИХ БЕЗОПАСНОСТИ

Александр ПЕРШИН
руководитель
Рабочей группы
по безопасности
мобильных
технологий АРСИБ

МАЛЬЧИК ВЫРОС

«Детские годы» мобильных технологий уже в прошлом. «Мобильные технологии превратились из вспомогательных и инновационных решений для бизнеса в ключевые пользовательские технологии для корпоративной среды. Устройства и приложения изменили характер выполнения функциональных обязанностей, мобильные прикладные платформы и сервисы создали новую модель бизнеса и возможности взаимодействия участников. Для получения преимуществ от этого, организации должны знать взаимосвязи, зависимости и требования по всем аспектам мобильных технологий, от аппаратного обеспечения и устройств до управления и разработки платформ, безопасности и сервисов». Фил Хохмут (Phil Hochmuth), программный директор IDC.

На рынок мобильных технологий вышли крупные компании, которые ранее ими не занимались: IBM, Oracle, Dell, SAP, Hewlett-Packard, CheckPoint, Symantec, Citrix, VMware и др. Произошли многие слияния и поглощения.

На рисунке 1 представлена статистика роста количества мобильных устройств и пользователей Интернет (млн) с 2005 по 2017 годы.

Статистика использования мобильных ОС (по данным Gartner на 2-й квартал 2016 г.) приведена на рисунке 2.

ОБРАТНАЯ СТОРОНА

Мобильные технологии, как и любые другие инновационные решения, имеют обратную сторону: они могут использоваться как инструмент для совершения противоправных действий. Например, террористическая деятельность, деятельность различных спецслужб, несанкционированный доступ к персональным или критичным корпоративным данным (данным, составляющим коммерческую тайну), подмена/блокировка данных критической информационной инфраструктуры и пр.

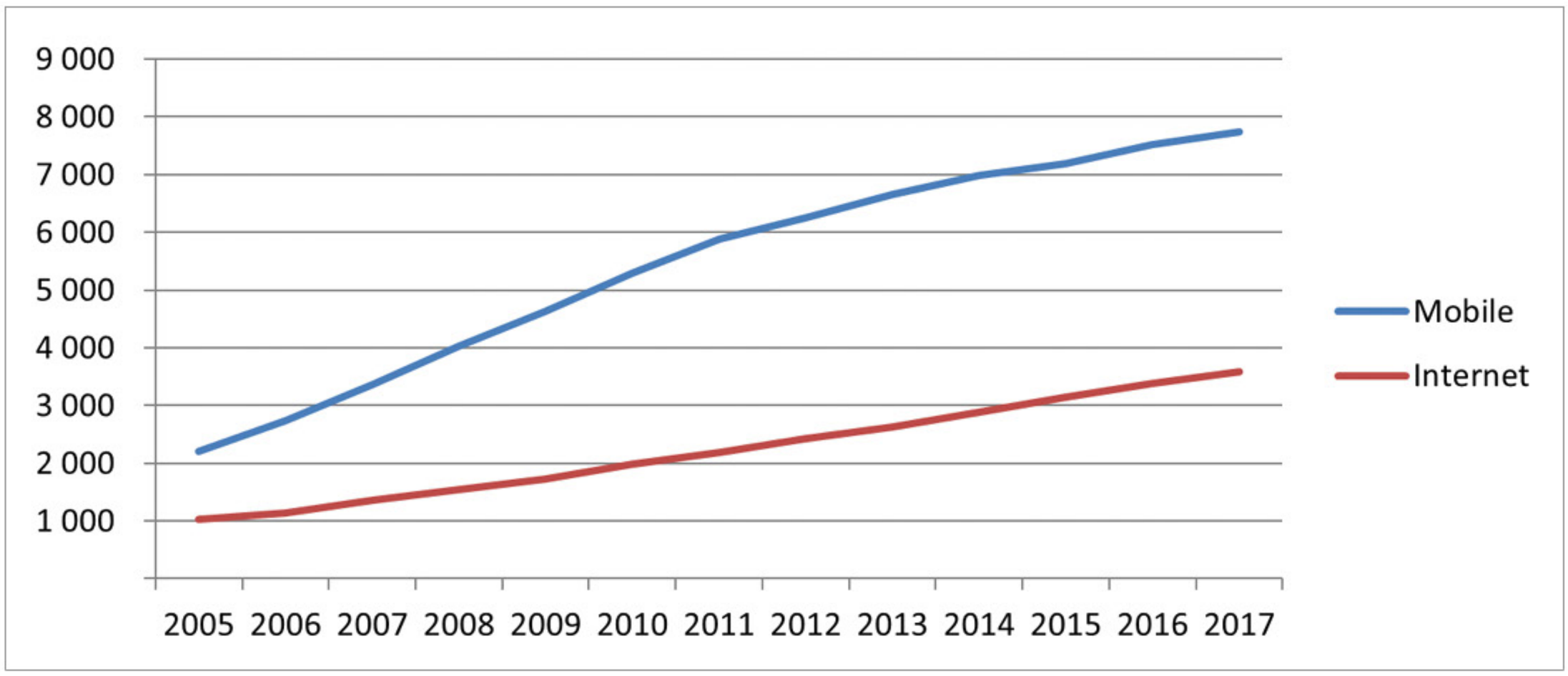


Рисунок 1. Статистика роста количества мобильных устройств и пользователей Интернет (млн.) с 2005 по 2017 годы (по данным Международного союза электросвязи)

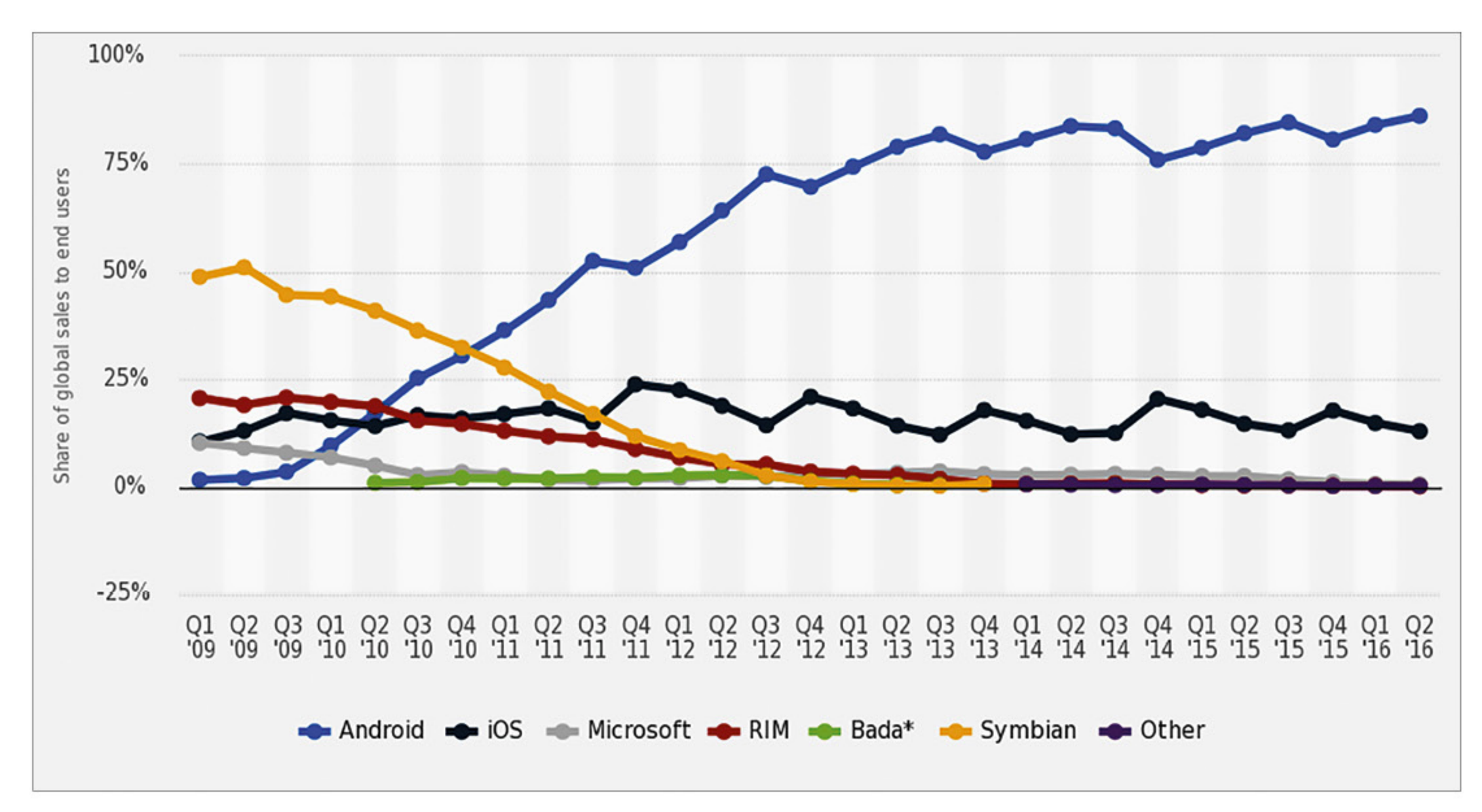


Рисунок 2. Статистика использования мобильных ОС (по данным Gartner на 2-й квартал 2016 г.)

КИБЕРВОЙНА ГАЛОПИРУЕТ

Текущую ситуацию можно охарактеризовать как «кибервойна галопирует», о чем свидетельствуют многочисленные факты, информация о которых опубликована в российских и зарубежных СМИ, на сайте WikiLeaks, а также в пресс-релизах ФСБ России.

В декабре 2016 г. Центр общественных связей ФСБ России сообщил, что «ФСБ России получена информация о подготовке иностранными спецслужбами в период с 5 декабря 2016 года масштабных кибератак с целью дестабилизации финансовой системы Российской Федерации, в том числе деятельности ряда крупнейших российских банков».

7 марта 2017 г. сайт WikiLeaks опубликовал следующие данные: средства, которыми располагает ЦРУ, позволяют «взламывать» мобильные ОС iOS и Android. Инфицированные смартфоны могут несанкционированно пересылать данные о местонахождении, звуковые и текстовые сообщения, а также по команде извне включать/отключать камеру и микрофон. Об этих и других фактах сообщают The Independent и ряд российских изданий.

Кроме того, по данным российской компании Group-IB за два года финансовая система России потеряла от кибератак около 6,9 млрд рублей. В 2017 г. была выявлена новая тенденция — похищение информации через мессенджеры. Мобильные угрозы направлены в первую очередь на пользователей ОС Android из-за ее большой популярности, отмечают в компаниях Dr. Web и Eset Russia. ОС Android более популярна у злоумышленников, поскольку она занимает около 80% рынка мобильных устройств. В 2017 г. ежемесячно появлялось до 400 новых угроз для ОС Android, в то время как в 2016 г. — около 300, а в 2015-м — 200.

ОТНОШЕНИЕ ГОСУДАРСТВА

Мобильные устройства стали неотъемлемой частью бизнес-процессов[1] компаний и государственных организаций и важным инструментом по повышению эффективности работы сотрудников. С декабря 2016 г. тема информационных технологий и обеспечения их безопасности постоянно была в центре внимания, принят ряд нормативных документов, направленных на повышение уровня информационной безопасности:

1. Доктрина информационной безопасности Российской Федерации.
2. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы.
3. Программа «Цифровая экономика Российской Федерации».
4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[1] Под терминами «бизнес», «бизнес-процессы» будем понимать деятельность, действия, процессы организаций любых форм собственности.

и сопутствующие ему нормативно-правовые акты: Указы Президента РФ, Постановления Правительства РФ, нормативные документы ФСБ России и ФСТЭК России.

5. Указ Президента РФ от 7.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» (далее — Указ).

Также внесены изменения в ранее принятые Федеральные Законы «Об информации, информационных технологиях и о защите информации», «О связи», «О персональных данных».

НОВЫЕ ВЫЗОВЫ И УГРОЗЫ

Такое внимание к вопросам обеспечения информационной безопасности обусловлено усилением противостояния в киберпространстве, о чем свидетельствуют события последнего времени. Задачи обеспечения информационной безопасности в полной мере относятся и к мобильным технологиям. При этом стремительно развивающиеся мобильные технологии влекут новые вызовы и угрозы:

- Наличие недекларированных возможностей (НДВ) в программно-аппаратном обеспечении устройств и приложениях сторонних компаний.
- Съем голоса/данных «по воздуху» (от пользователя устройства до базовой станции оператора связи).
- Манипуляции с данными при передаче (подмена, блокировка).
- Внедрение вредоносного программного обеспечения.
- GPS/Геолокация (трассировка, подмена местонахождения).
- Утеря или кража устройства (возможен доступ к ресурсам организации).
- Использование недоверенных («серых», непроверенных или пользовательских) устройств, сетевых сервисов или их неправомочное использование («человеческий фактор»).
- Отслеживание действий пользователей через приложения (с использованием НДВ).

Эти вызовы и угрозы обусловлены в том числе и специфическими особенностями мобильных технологий:

- для мобильных технологий понятие «периметр контролируемой зоны» отсутствует;
- существует потенциальная возможность неограниченного во времени и в пространстве несанкционированного доступа к мобильному устройству.

Таким образом, перечисленные и др. особенности, по отдельности или в сочетании, в случае возникновения специфических для мобильных технологий вызовов и угроз, в совокупности могут являться угрозой национальной безопасности.

По данным Лаборатории Касперского более 98% известного вредоносного кода создано для ОС Google Android. При этом рост продаж устройств совпадает с ростом количества вредоносного кода

ДОМИНИРОВАНИЕ США

«Джошуа Купер Рамо, автор книги „Седьмое чувство“, утверждает, что в сетевую эпоху победитель часто получает все. Он отмечает, что сегодня существует девять глобальных технологических платформ (Google Chrome, Microsoft Office, Facebook и пр.), которыми пользуются более одного миллиарда человек. Все они доминируют на соответствующих рынках и имеют американское происхождение». Фарид Закария, The Washington Post, 29.05.2016. Эта цитата применима и к области мобильных технологий.

ВЫВОДЫ АРСИБ

Межрегиональная общественная организация «Ассоциация руководителей служб информационной безопасности» (АРСИБ) совместно с экспертами по информационной безопасности, проанализировав сложившуюся ситуацию, пришли к выводу, что использование мобильных устройств под управлением ОС Google Android для федеральных, муниципальных и иных органов исполнительной и законодательной власти, государственных учреждений и компаний с государственным участием, особенно для тех из них, в которых мобильные технологии используются в критической информационной инфраструктуре, государственных информационных системах и информационных системах персональных данных небезопасно в силу следующих ключевых факторов:

1. Высокая популярность среди пользователей.
2. Низкая вероятность своевременного выхода и установки обновлений ОС для устройств под управлением ОС Google Android.
3. Архитектура и правовая политика Google в отношении ОС Google Android не позволяет полноценно управлять передачей пользовательских и технических данных.
4. Лицензионные и санкционные риски: компания-разработчик ОС имеет право в одностороннем порядке изменить функционал и условия использования ОС или ограничить

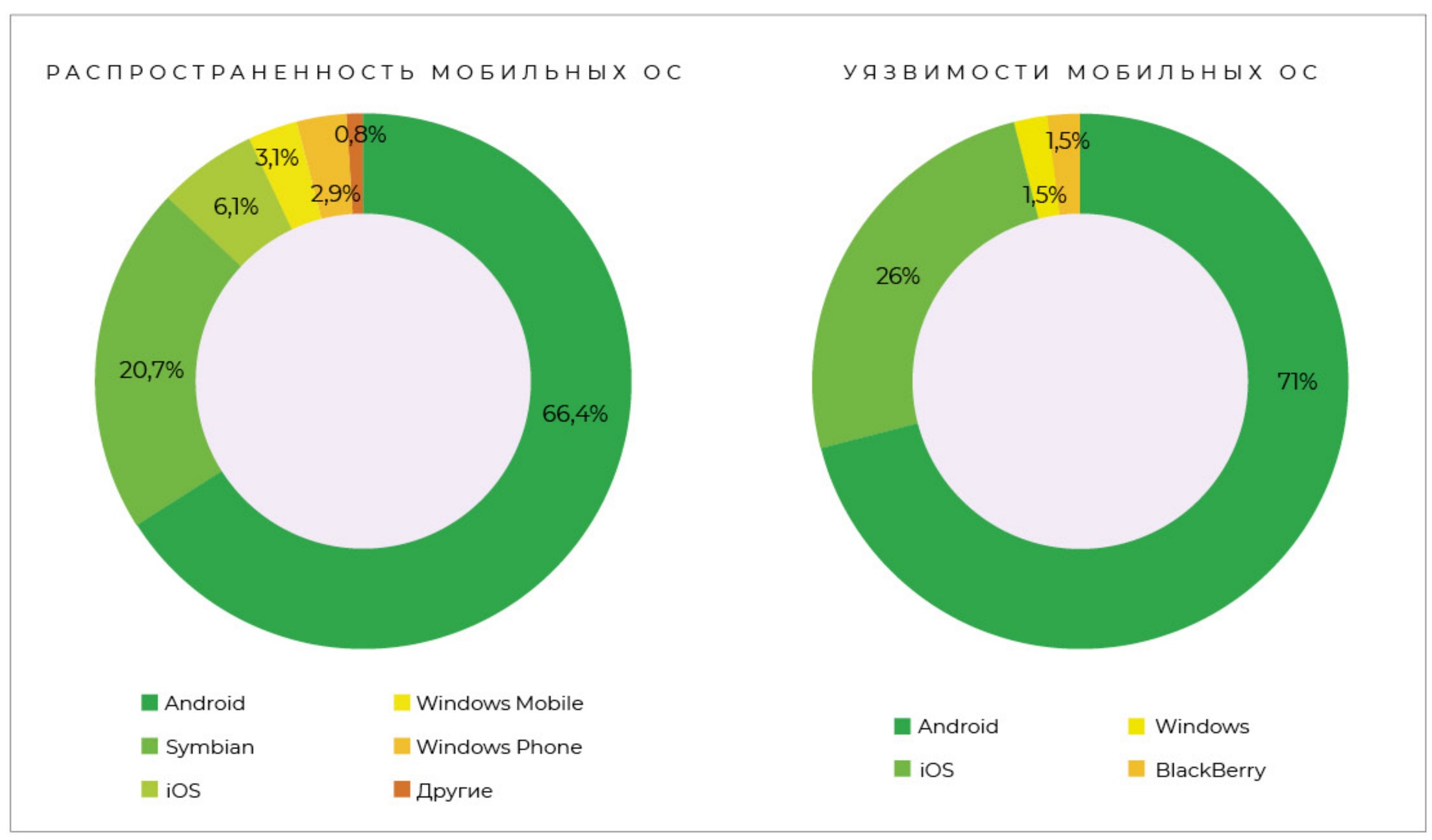


Рисунок 3. Распространенность и уязвимости мобильных ОС

ее использование на определенных территориях или категорией пользователей.

5. Исходный код системы или некоторых ее компонент, в том числе сторонних разработчиков, не позволяет провести проверку на отсутствие НДВ и верификацию источника (магазина) приложений.

ПО ДАННЫМ ИССЛЕДОВАНИЙ

По данным Лаборатории Касперского более 98% известного вредоносного кода создано для ОС Google Android. При этом рост продаж устройств совпадает с ростом количества вредоносного кода, а многообразие поведений идентично вредоносному коду для ОС Windows (нет только паразитирующих вирусов). Самые многочисленные атаки проходят с использованием назойливых рекламных троянцев.

Кроме того, количество уязвимостей для мобильных ОС прямо пропорционально их распространенности. Об этом свидетельствуют результаты исследования, проведенного компанией «Код безопасности» в 2016 г. (рисунок 3).

КАК ЗАЩИТИТЬ?

Всем известны основные правила обращения с персональной информацией: не сообщать PIN-код посторонним, не хранить его вместе с банковской картой. Но с развитием мобильного банкинга важно следить и за приложениями, которые вы устанавливаете на смартфон. Как отмечают в компании Dr. Web, мошенники встраивают вредоносный функционал в невинные на первый взгляд программы, такие как программа-фонарик. Внимательнее нужно быть и при переходе по ссылкам из писем и SMS, которые могут вести на сайт, маскирующийся под популярную компанию или банк, где неопытный пользователь может ввести свой логин и пароль и, таким образом, попасться на удочку мошенников.

Риски и угрозы, связанные с использованием мобильных технологий в корпоративном секторе, могут быть минимизированы следующим образом:

Применением систем управления мобильными устройствами и приложениями, реализующими какую-либо форму контейнера, и средств криптографической защиты информации в канале связи между мобильным устройством и корпоративной системой.

Использованием мобильных платформ и систем управления ими, содержащих встроенные средства защиты, включая криптографические.

При этом желательно, чтобы применяемые средства защиты, как на уровне мобильного устройства, так и на уровне системы управления, были сертифицированы соответствующим регулятором. Эксперты АРСИБ не рекомендуют использовать мобильные технологии в бизнес-про-

цессах с использованием мобильных устройств под управлением как ОС Google Android, и ОС Apple iOS, без дополнительных мер защиты.

Рекомендации, как и приведенные выше риски, в полной мере распространяются и на другую популярную мобильную ОС — iOS, устанавливаемую только на мобильные устройства компании Apple, несмотря на декларируемую этой компанией политику защиты пользовательских данных.

ОТКРЫТОЕ ПИСЬМО

Наряду с техническими мерами защиты необходимо применять и организационные (политика безопасности), которые, не заменяя технических, позволяют достаточно эффективно минимизировать риски и противодействовать специфичным угрозам.

Более подробную информацию по теме можно узнать из брошюры «Безопасность мобильных технологий. Общие рекомендации», версия 2.0, электронная версия которой размещена на сайте АРСИБ. Кроме того, АРСИБ разработан трехдневный учебный курс «Безопасность бизнес-процессов, использующих мобильные технологии». Курс включает основы мобильных технологий: определения, варианты использования, угрозы и меры противодействия, системы управления, возможности мобильных технологий для реализации бизнес-процессов и обеспечения их безопасности, а также обзор некоторых российских и зарубежных систем управления, сценарии их применения и практические рекомендации. Более подробную информацию можно получить в АРСИБ.

Также, АРСИБ подготовлено Открытое письмо «О безопасности мобильных технологий», с которым можно ознакомиться в Интернете и на сайте АРСИБ.

ТРИ ТЕЗИСА

В заключение можно сформулировать три тезиса:

- Обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере является одной из национальных целей развития Российской Федерации на период до 2024 (п. 1ж Указа).
- Цифровое взаимодействие все больше основывается на беспроводных (в быту — мобильных) технологиях (см. рисунок 1).
- Новые технологии без обеспечения информационной безопасности приведут только к хаосу. Необходим баланс между эффективностью, повышением производительности и удобством, с одной стороны, и обеспечением безопасности с другой.

НАЦИОНАЛЬНАЯ МОБИЛЬНАЯ ПЛАТФОРМА

Как результат, неизбежно встает сакраментальный для России вопрос: «Что делать?». Помимо перечисленных выше рекомендаций по минимизации рисков и угроз, связанных с использованием мобильных технологий, также необходимо минимизировать риски и угрозы на более низком уровне. А именно: создать независимую от зарубежных поставщиков программно-аппаратную мобильную платформу. Эта концепция, сформулированная как Национальная мобильная платформа и изложенная в разделе 12 упомянутой брошюры, в полной мере соответствует п. 11 Указа.

В числе основных компонентов Национальной мобильной платформы:

1. Доверенная аппаратная платформа. Может быть российской или частично зарубежной сборки, в первую очередь — микропроцессора, произведенного, например, в КНР или странах Юго-Восточной Азии, с использованием российских комплектующих с обязательным контролем приемки в соответствии с правилами, принятыми в Российской Федерации, и выдачей сертификата установленного образца.
2. Доверенная мобильная ОС, включающая встроенные или сторонние средства защиты информации от несанкционированного доступа, а также криптографические средства защиты информации (на уровне ядра ОС).

Создание Национальной мобильной платформы необходимо в целях противодействия новым вызовам и угрозам, а также обеспечения национальной безопасности в сфере мобильных технологий. Кроме того, некоторые другие страны (например, страны ЕАЭС, БРИКС или ШОС), вероятно, хотели бы иметь свою национальную мобильную платформу, но ее создание сопряжено со значительными трудностями. Причина в том, что развитую криптографическую науку, современные криптографические алгоритмы и реализующие их средства в состоянии создавать, развивать и внедрять очень немногие страны (в первую очередь — Россия и США, а также некоторые другие страны).

В России есть возможности и квалифицированные специалисты для выполнения этих работ.

* * *

Необходимо отдавать себе отчет в том, что, если не приступить к решению этих задач немедленно, то наблюдаемые в настоящее время волны кибервойны могут перерасти во всепоглощающее цунами, результатом которого может стать мобильный хаос.

Промедление может дорого обойтись.

БАНК, ЕГО АУТСОРСЕР, ИХ РАБОТНИКИ И РАЗРАБОТКА БАНКОВСКОГО ПО

ОБ ОСНОВАНИЯХ И СПОСОБАХ ОФОРМЛЕНИЯ КРЕДИТНОЙ ОРГАНИЗАЦИЕЙ ДОПУСКА РАБОТНИКОВ ВНЕШНЕГО ПОСТАВЩИКА УСЛУГ (ИСПОЛНИТЕЛЯ, АУТСОРСЕРА) К РАБОТАМ С ЕЁ АВТОМАТИЗИРОВАННЫМИ СИСТЕМАМИ И ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Федор ДЗЕРЖИНСКИЙ
главный эксперт — координатор системной экспертизы ООО «ТехноСофт»

В связи с изданием стандарта Банка России СТО БР ИББС-1.4–2018 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге» [1], рядом юристов отмечено наличие проблемы, суть которой сводится к следующему.

Для некоторых видов работ, передаваемых банком для исполнения стороннему исполнителю при аутсорсинге, трудно полностью исключить возможность доступа персонала внешнего исполнителя работ к защищаемой информации банка, включая сведения, составляющие банковскую тайну. Но при этом законодательство РФ не предусматривает никаких возможностей для передачи банком данной категории сведений внешнему исполнителю. Решение проблемы предлагается искать на пути изменения российских законов [2].

Цель настоящей статьи — рассказать о поисках не требующего изменения законов подхода к решению отмеченной выше проблемы, которыми автору довелось заниматься в начале 2015 г. — задолго до появления стандарта [1]. Эти поиски выполнялись в порядке «теоретической» проработки вопроса применительно к специфическому классу ситуаций — аутсорсингу внутренних функций и процессов банка в области разработки ПО. Этот класс ситуаций пояснён ниже.

Суть подхода состояла в предложении оформлять отношения между банком, организацией-аутсорсером и ее работником, допускаемым к работам с системами банка, подписываемым всеми ими *«трехсторонним протоколом»,* положения которого, насколько возможно, позволяли бы соблюсти в отношении работника аутсорсера все те требования, которые действующее законодательство РФ и Банк России предъявляют *к служащим кредитной организации.*

В качестве желаемого итога такого оформления отношений рассматривалось принятие на себя работником обязательств равнозначных обязательствам служащего банка. В идеале — создание оснований для того, чтобы банк имел возможность рассматривать такого «чужого» работника, после прохождения им необходимых проверок и допуска к работам, в качестве *«внештатного служащего»* банка.

Три года назад предложенный подход и набросок положений такого протокола в течение какого-то времени активно обсуждались, в том числе с юристами, представителями иных банковских служб и подразделений, претерпели ряд доработок, но так и не получили практического использования. В тот момент это казалось полной неудачей предпринятых усилий.

Однако ныне, с учётом ряда новых обстоятельств, в том числе растущего внимания к упомянутой выше проблеме и другим, подобным ей, есть вероятность, что рассматриваемый опыт всё-таки окажется кому-то полезен. По крайней мере, как повод для размышлений и дискуссии.

АУТСОРСИНГ РАЗРАБОТКИ БАНКОВСКОГО ПО

Представим себе некий банк, имеющий «по историческим причинам» серьёзные внутренние ресурсы разработчиков банковского прикладного программного обеспечения (ПО). Эти ресурсы обеспечивают создание, сопровождение и развитие ряда применяемых банком автоматизированных систем (АС), в том числе критически важных для бизнеса банка.

В какой-то момент банк принимает «стратегическое» решение о том, чтобы вывести целиком соответствующие подразделения разработчиков ПО «на аутсорсинг» путём перевода всего персонала этих подразделений в специально созданную, внешнюю, но аффилированную с банком коммерческую организацию. И возложить на эту организацию (аутсорсера) осуществление тех же самых функций, которые раньше выполняли внутренние разработчики ПО в банке. Но теперь эти функции должны выполняться по договору между этой организацией, как исполнителем, и банком, как заказчиком. (Есть очень много возможных оснований как для вывода из банка ресурсов по разработке программного обеспечения на аутсорсинг в отдельное юридическое лицо, так и для сохранения их внутри банка или даже для их возвращения снова в банк. Интересное рассмотрение этого вопроса содержится в [3]. Для целей настоящей статьи важно лишь наличие решения об аутсорсинге, а не причины его принятия).

Возникает вопрос, как банку в этой ситуации правомерно, безопасно и экономично предоставить допуск работникам организации аутсорсера ко всей той информации, которая им необходима для выполнения своих функций без существенного снижения эффективности этой работы по сравнению с периодом, когда они выполняли соответствующие функции, будучи работниками банка? При том что эти функции в банке могли включать, например, анализ требований реальных бизнес-процессов, отладку и тестирование приложений на реалистичных и даже реальных исходных данных, выполнение заявок от бизнеса на устранение проблем, связанных с конкретными производственными ситуациями и т.д., подразумевать нахождение в помещениях банка, использование его инфраструктуры, постоянное общение со многими его работниками.

Можно указать три подхода к организации работ в подобной ситуации, допускающие применение в том или ином сочетании:

- Первый подход — «совместительство» — состоит в том, чтобы банку принять в свой штат по совместительству (на ту или иную «долю ставки») тех работников аутсорсера, которым по роду их обязанностей наиболее необходим доступ к защищаемой информации банка.
- Второй подход — «работа по правилам» — для всех или некоторых переведённых из банка в организацию-аутсорсер работников технически и организационно исключить доступ ко всей той части защищаемой информации банка, к которой доступ могут иметь лишь служащие банка. Несмотря на то что это повлечёт нарушение сложившейся организации работ, процессов разработки ПО, их существенное удорожание и замедление, риски для бизнеса банка.
- Третий подход — «принятие рисков» — действия в порядке исключения исходя из конкретных обстоятельств, индивидуальные меры по минимизации рисков и принятие рисков.

Первый из перечисленных подходов наиболее надёжен в плане решения проблемы, упомянутой в начале данной статьи. Однако все они в той или иной степени обременительны для банка и для аутсорсера.

О СТАТУСЕ СЛУЖАЩЕГО БАНКА

Чем отличается статус «служащего» кредитной организации от статуса работников её организации-аутсорсера?

Начнём с того, что в первом абзаце Статьи 26 «Банковская тайна» Федерального закона РФ «О банках и банковской деятельности» сказано: *«… Все служащие кредитной организации обязаны хранить тайну об операциях, о счетах и вкладах её клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.» Помимо собственно банковской тайны, эта формулировка позволяет банку устанавливать в качестве охраняемой законом тайны также иную «внутреннюю информацию»* — например, о методах защиты информации.

Работники банка проходят процедуру проверки и допуска к информации и документам, состоят в банке на кадровом учёте, обязаны выполнять требования внутренних документов банка, регулярно проходят ознакомление с внутренними документами банка, нередко под подпись.

Работники сторонней организации-подрядчика, не являющиеся «служащими» банка, формально не несут ни такой же обязанности хранить тайну, ни обязанности соблюдать требования внутренних документов банка. И при этом содержательно о них банку «известно» гораздо меньше, чем о работниках банка. Допуская первых к исполнению служебных ролей, фактически эквивалентных ролям своих штатных работников, банк рискует допустить нарушение уста-

новленного для рынка финансовых услуг принципа «знать своего работника» (см. [4], п. 6.10).

Это создаёт одно из принципиальных, формальных препятствий для аутсорсинга функций и процессов применения информационных технологий (ИТ), которые способны влиять на информационную безопасность банка, т.е., практически в любой существенной области применения ИТ в банке.

Далее, основная, если не бóльшая часть требований, предъявляемых к банку касающимися информационной безопасности и защиты информации нормативными документами Банка России, применимыми стандартами в этой сфере, так или иначе сводится к необходимости издания некоторых внутренних документов банка, назначения ответственных лиц или подразделений банка и строгого, контролируемого соблюдения этих документов.

Если будет осуществляться аутсорсинг, и фактические исполнители работ (не работники банка) не будут обязаны соблюдать все требования внутренних документов именно банка, а не только аутсорсера, то это будет равнозначно отсутствию пригодных для применения документов банка и невыполнению банком соответствующих требований Банка России (возможности передать сторонней организации ответственность за их соблюдение банк не имеет).

Наконец, есть две структуры банка — служба внутреннего контроля (СВК) и служба информационной безопасности (СИБ), которые в соответствии с требованиями закона и документов Банка России должны иметь «особые» полномочия и обязанности в отношении осуществляемых в банке функций и процессов в сфере ИТ (в том числе по получению доступа на рабочие места, в помещения, к информации, материалам, документам, техническим средствам, получению разъяснений от работников и руководителей подразделений). Если в отношении каких-либо существенных аспектов этих функций и процессов, переданных на аутсорсинг, возможности СВК и СИБ будут ограничены, то это фактически будет означать нарушение требований закона и(или) требований Банка России.

О ТРЁХСТОРОННЕМ ПРОТОКОЛЕ

С учётом всего отмеченного выше и была предпринята попытка разработать «четвёртый» подход, основанный на использовании некоторой формы соглашения (трёхстороннего протокола) между банком, аутсорсером и работниками аутсорсера, а также внутренних документов банка, которые позволили бы:

(1) насколько возможно, юридически приравнять допускаемых к работам в рамках аутсорсинга работников сторонней организации к «внештатным служащим» банка, предусмотрев присвоение им банком статуса «допустимый исполнитель работ» (его получение подразумевает подписание протокола, проверку, согласование и допуск к работам банком каждой кандидатуры);

(2) обеспечить обязательность для всех допущенных к работе работников всех внутренних документов банка,

(3) обеспечить беспрепятственное осуществление полномочий СВК и СИБ в отношении всех допущенных к участию в работах работников сторонней организации.

* * *

Набросок основных положений «трёхстороннего протокола» представлен в Приложении настоящей статьи. При его использовании необходимо учитывать, что он представляет собой не юридический документ, а материал организационно-технического характера, рассчитанный на критическое рассмотрение и существенную переработку квалифицированными юристами — работниками юридического подразделения банка, вместе с СИБ и подразделениями ИТ.

ЛИТЕРАТУРА

1. Стандарт Банка России СТО БР ИББС-1.4–2018 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге. — Москва, 2018
2. *Канашевский В.А.* Банковская тайна и использование банками услуг аутсорсинга информационной безопасности // Lex russica, 2018. N7. С. 92–97. — *http://lexrussica.ru/articles/article_104479.html?issue=lexrussica-7–2018*
3. *Philip G. Armour,* «Business of Software: Owning and Using»//Communications of the ACM, June 2014, Vol. 57, No. 6, pp. 29–30.
4. ГОСТ Р 57580.1–2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. — Москва, Стандартинформ, 2017.

ПРИЛОЖЕНИЕ

Протокол об условиях допуска к участию в выполнении работ с АБС и ПО банка

... далее именуемое Банк, в лице ..., действующего на основании ...,

... далее именуемое Контрагент, в лице ..., действующего на основании ...,

и ..., далее именуемый Гражданин, являющийся работником Контрагента, чьи трудовые обязанности могут включать участие в выполнении в соответствии с договором или договорами, которые заключены или могут быть заключены в будущем, между Банком, как «Заказчиком», и Контрагентом, как «Исполнителем», работ по созданию, модернизации и (или) техническому обслуживанию применяемых Банком автоматизированных банковских систем (АБС) и программного обеспечения (ПО),

далее совместно именуемые Стороны, настоящим подтверждают нижеследующее:

1. Основные понятия

Для целей настоящего Протокола следующие понятия используются в соответствии с приводимыми ниже определениями.

1.1. Работы по созданию, модернизации и (или) техническому обслуживанию применяемых Банком АБС и ПО (далее для краткости — «Работы с АБС и ПО Банка») — работы и мероприятия технического и научно-технического характера по разработке (в т.ч. в рамках определения, проектирования, создания, развития, сопровождения, модернизации, адаптации), исследованию (анализу, отладке, тестированию, техническому контролю, оптимизации характеристик), оформлению, документированию, внедрению, техническому обслуживанию при эксплуатации и плановому выводу из эксплуатации АБС и ПО, применяемых или планируемых к применению в рамках бизнес процессов, платежных технологических процессов, информационных технологических процессов и (или) реализации информационных потоков Банка.

1.2. Банковская информация ограниченного доступа (ИОД) — создаваемая и обрабатываемая в рамках деятельности Банка, как кредитной организации, информация, в отношении которой в соответствии с действующим законодательством РФ установлено требование об обеспечении ее конфиденциальности и сохранении тайны о ней, в том числе информация, не подлежащая передаче или раскрытию Банком и всеми его служащими третьим лицам, включая Контрагента. Для целей настоящего Протокола выделяются нижеследующие категории ИОД (пп. 1.2.1 — 1.2.5).

1.2.1. Банковская тайна — тайна об операциях, о счетах и вкладах клиентов и корреспондентов Банка (ст. 26 «Банковская тайна» Федерального закона РФ «О банках и банковской деятельности»), тайна банковского счета и банковского вклада, операций по счету и сведений о клиенте (ст. 857 ГК РФ).

1.2.2. Внутренняя информация Банка — иная, чем сведения, составляющие банковскую тайну (п. 1.2.1) или персональные данные (п. 1.2.3), информация, установленная Банком на основании абзаца первого ст. 26 «Банковская тайна» Федерального закона РФ «О банках и банковской деятельности», тайну о которой обязаны хранить все служащие Банка (в том числе, сведения, раскрытие или ненадлежащее использование которых может повлиять на защиту информации, в т.ч. банковской тайны, обеспечение информационной безопасности Банка и др.).

1.2.3. Персональные данные — персональные данные тех или иных субъектов (Федеральный закон РФ «О персональных данных»).

1.2.4. Коммерческая тайна — сведения о принадлежащих Банку или третьим лицам секретах производства (ноу-хау) или иные, в отношении которых Банком приняты меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны.

1.2.5. Прочая ИОД — иные, чем перечисленные в пп. 1.2.1 — 1.2.4, категории банковской информации ограниченного доступа (например, инсайдерская информация и др.).

Примечание. В отдельных из внутренних документов Банка для упоминания ИОД по историческим причинам могут использоваться условные термины «банковская и коммерческая тайна» или иные.

2. Общие положения

2.1. Банк, Контрагент и Гражданин понимают и признают нижеследующее.

2.1.1. В связи с участием Гражданина, в рамках трудовых обязанностей по отношению к Контрагенту, в выполнении Работ с АБС и ПО Банка, может быть необходим и фактически осуществляться доступ Гражданина к отдельным элементам ИОД Банка, а именно, к Внутренней информации Банка, необходимой для посещения Гражданином охраняемых помещений Банка, взаимодействия с работниками Банка, с системами электронного документооборота Банка и для решения поставленных задач в рамках выполняемых Работ.

2.1.2. Кроме того, не может быть полностью исключен риск того, что в силу случайных, чрезвычайных или особых обстоятельств, в том числе ошибки, недосмотра или ненадлежащих действий персонала (например, вследствие ошибочной адресации электронного сообщения), сбоя, отказа и реализации уязвимости программно-технических средств, нештатной ситуации и др., Гражданин фактически получит доступ или возможность доступа к каким-либо сведениям, составляющим иную, чем Внутренняя информация, категорию ИОД.

2.3. В связи с отмеченным, обязательным условием допуска Гражданина в качестве работника Контрагента к участию в Работах с АБС и ПО Банка, вытекающим из действующего законодательства и требований Банка России, Банк считает принятие на себя Гражданином обязательств по соблюдению конфиденциальности ИОД Банка и по выполнению требований внутренних документов Банка в области информационной безопасности наравне со штатными служащими Банка, работающими в Банке по трудовому договору, и присвоение Банком Гражданину, по результатам проведенной в отношении него Банком процедуры предоставления допуска к участию в Работах, статуса Допустимого исполнителя Работ с АБС и ПО Банка (сокращенно — Допустимый исполнитель работ, ДИР), на основании заверений и обязательств Гражданина и Контрагента, изложенных в последующих разделах настоящего Протокола.

3. Заверения и обязательства Гражданина

3.1. Гражданин настоящим ходатайствует перед Банком о допуске его Банком к участию в Работах с АБС и ПО Банка в статусе Допустимого исполнителя работ и добровольно принимает на себя в связи с этим обязательство выполнять все требования по неразглашению ИОД Банка и по обеспечению информационной безопасности Банка, установленные в соответствии с действующим законодательством РФ, нормативными актами Банка России и внутренними нормативными актами Банка для служащих Банка и нести ответственность за последствия нарушения указанных требований наравне со штатными служащими (работниками) Банка.

3.2. Гражданин настоящим подтверждает свое согласие на обработку Банком персональных данных Гражданина в целях выполнения проверок в рамках процедур предоставления доступа к работам, в составе и способами, аналогичными предусмотренным в отношении штатных служащих (работников) Банка (за исключением данных, связанных исключительно с трудовыми отношениями между Банком и его работниками, таких как данные для расчетов по оплате труда и для медицинского страхования), включая согласие на запрос Банком данных о Гражданине у третьих лиц, а также в целях ведения Банком персонального учета Гражданина в качестве Допустимого исполнителя Работ с АБС и ПО Банка, при соблюдении предусмотренных законодательством РФ требований по защите персональных данных.

3.3. Гражданин настоящим подтверждает свое согласие на передачу Контрагентом Банку и Банком Контрагенту персональных данных Гражданина в целях осуществления проверок и кадрового учета, указанных в п. 3.2, при соблюдении предусмотренных законодательством РФ требований по защите персональных данных.

3.4. Гражданин настоящим обязуется строго выполнять требования предоставляемых уполномоченными работниками Банка Гражданину для ознакомления внутренних документов Банка, касающиеся обращения с ИОД и обеспечения информационной безопасности Банка, обязательные для штатных служащих (работников) Банка. Гражданин обязуется своевременно, в установленный срок знакомиться с новыми документами и их измененными версиями, в том числе, если предусмотрено — под роспись.

3.5. Гражданин настоящим обязуется при участии в Работах с АБС и ПО Банка выполнять правомерные требования уполномоченных работников профильных подразделений Банка в сфере внутреннего контроля, безопасности и информационной безопасности.

3.6. Гражданин настоящим заверяет Банк в том, что во всех случаях получения доступа, в том числе случайно к любой информации (устной, материалам, документам и др.) в помещениях Банка, с помощью технических средств Банка, от штатных служащих (работников) Банка или от других Допустимых исполнителей Работ с АБС и ПО Банка лично, по телефону или по электронным каналам, Гражданин будет считать, что полученная информация может содержать ИОД Банка, и обращаться с информацией в соответствии с требованиями по обращению с ИОД Банка, если только Гражданину достоверно не известно обратное.

3.7. Гражданин подтверждает, что ему известно о том, что любая ИОД Банка, не переданная официально Банком Контрагенту, которая может стать известна Гражданину и иным работникам Контрагента, допущенным к участию в Работах с АБС и ПО Банка в статусе Допустимых исполнителей работ, должна рассматриваться в качестве полученной ими как Допустимыми исполнителями Работ с АБС и ПО Банка, а не как представителями Контрагента. Такая ИОД Банка не является переданной и не подлежит передаче Контрагенту, а также каким-либо его работникам, не являющимся служащими Банка или Допустимыми исполнителями Работ с АБС и ПО Банка.

3.8. Гражданин подтверждает, что ему известно о том, что как Банк, так и Контрагент вправе в любое время приостановить или прекратить действие предоставленного Гражданину статуса Допустимого исполнителя Работ с АБС и ПО Банка в случае нарушения Гражданином требований внутренних документов Банка в области ИОД и информационной безопасности, а также по иным основаниям, и что в этом случае дальнейшее участие Гражданина в Работах с АБС и ПО Банка будет невозможно.

В случае прекращения трудовых отношений между Контрагентом, как работодателем и Гражданином, как работником, действие предоставленного Гражданину статуса Допустимого исполнителя Работ с АБС и ПО Банка прекращается немедленно или в сроки, согласованные Сторонами.

3.9. Гражданин подтверждает, что в случае приостановления или прекращения по любым основаниям действия предоставленного Гражданину статуса Допустимого исполнителя Работ с АБС и ПО Банка все обязательства Гражданина о неразглашении ИОД Банка продолжают действовать и действуют бессрочно.

4. Заверения и обязательства Контрагента

4.1. Контрагент настоящим подтверждает, что Гражданин действительно является работником Контрагента, и что Гражданину предполагается поручить участие в осуществлении Работ с АБС и ПО Банка.

4.3. Контрагент настоящим обязуется в течение всего срока действия предоставленного Банком Гражданину статуса Допустимого исполнителя Работ с АБС и ПО Банка обмениваться с Банком информацией об изменениях персональных данных Гражданина в целях обеспечения достоверности и актуальности данных персонального учета Гражданина в качестве Допустимого исполнителя Работ с АБС и ПО Банка.

4.2. Контрагент настоящим обязуется незамедлительно уведомить Банк о предстоящем прекращении трудовых отношений между Контрагентом, как работодателем и Гражданином, как работником, а также о приостановлении или прекращении, по инициативе Контрагента, действия предоставленного Гражданину статуса Допустимого исполнителя Работ с АБС и ПО Банка.

4.3. Контрагенту известно, что Банк вправе в любое время в одностороннем порядке приостановить или прекратить действие предоставленного Гражданину статуса Допустимого исполнителя Работ с АБС и ПО Банка, и что в этом случае дальнейшее участие Гражданина в Работах с АБС и ПО Банка будет невозможно.

4.4. Контрагенту известно, что любая ИОД Банка, не переданная официально Банком Контрагенту, которая может стать известна Гражданину в связи с участием в Работах с АБС и ПО Банка, известна ему как Допустимому исполнителю Работ с АБС и ПО Банка, а не как представителю Контрагента, и что эта ИОД Банка не передана и не подлежит передаче Контрагенту. Контрагент обязуется не требовать от Гражданина отражения такой ИОД Банка в каких-либо документах и материалах Контрагента, а также предоставления Гражданином такой ИОД Банка какому-либо работнику Контрагента, не являющемуся служащим Банка или Допустимым исполнителем Работ с АБС и ПО Банка или являющемуся одним из них, но не обладающему правом доступа к соответствующей ИОД.

В случае противоречия данного пункта настоящего Протокола каким-либо положениям трудового договора или иных договоров меджду Контрагентом и Гражданином, данный пункт настоящего Протокола имеет преимущественную силу.

5. Заверения и обязательства Банка

5.1. Банк настоящим подтверждает, что по результатам проведенной проверки Граж-

данину предоставлен статус Допустимого исполнителя Работ с АБС и ПО Банка, и что Гражданин может быть направлен Контрагентом и допущен Банком к участию в Работах с АБС и ПО Банка.

5.2. Банк обязуется своевременно предоставлять Гражданину для ознакомления подлежащие соблюдению Гражданином, как Допустимым исполнителем Работ с АБС и ПО Банка, внутренние номативные документы Банка в области ИОД и информационной безопасности.

5.3. Банк обязуется обеспечивать, со своей стороны, необходимые условия для выполнения Гражданином требований по обращению с ИОД и обеспечению информационной безопасности Банка, в соответствии порядком, установленным для штатных служащих (работников) Банка, и с учетом особенностей, обусловленных отсутствием трудовых отношений между Гражданином и Банком.

5.4. Банк обязуется незамедлительно уведомить Контрагента о приостановлении или прекращении, по инициативе Банка, действия предоставленного Гражданину статуса Допустимого исполнителя Работ с АБС и ПО Банка.

6. Заключительные положения

7. Реквизиты и подписи Сторон

Примечание:

Настоящий «Протокол» — © Федор Дзержинский, 2018. Разрешено безвозмездное, свободное использование, без ограничений по сроку и территории, при условии соблюдения общепринятых норм научно-технической и деловой этики.

BIS-КОММЕНТАРИЙ

Василий ОКУЛЕССКИЙ
заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук

Автор предложил интересный подход к передаче на аутсорсинг разработки программного обеспечения, при котором возможна минимизация рисков информационной безопасности при передаче некоторой защищаемой в банке информации.

Предложенный подход не отражает ещё одну существенную проблему — обеспечение доверия банка к организации-аутсорсеру, в первую очередь, к компетенции этой организации в вопросах обеспечения защиты информации, что является неотъемлемым требованием СТО БР ИББС-1.4–2018 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге». С точки зрения стандарта, подтверждением компетенции является наличие лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации.

Можно подробно рассматривать конкретные пункты лицензии и что стоит за ними. Хочу остановиться только на общих для всех пунктах — требованиях к подготовке сотрудников организации-лицензиата.

Основные требования к ним сфокусированы на направлениях защиты:

- Информация
- Технические средства
- Программное обеспечение
- Информационные технологии
- Средства защиты информации

Казалось бы, исчерпывающий список направлений, однако идём дальше. От чего будем их защищать? Смотрим требования:

- Защита от утечки информации по техническим каналам
- Защита от несанкционированного доступа (НСД) к информации
- Защита от воздействия без использования криптографической защиты

Здорово! А теперь начинаем смотреть, на что больше уделяется внимания в типовых учебных курсах по ТЗКИ (500 с лишним часов)? А там эти самые технические каналы — акустика, виброакустика, ПЭМИН, электроакустика — занимают львиную долю учебного времени. И это при том, что специфика банковского бизнеса в 99% случаев признаёт эти каналы утечки для банков неактуальными.

Ну, хорошо, знания лишним не бывают. И тут неувязочка. Особенности технологических и информационных банковских процессов и систем в рамках этих курсов не изучаются. Особенности построения моделей угроз банковских процессов, да и вся банковская специфика (!), отсутствуют. Нет требований к организации-аутсорсеру соответствовать требованиям, например, Положения Банка России № 382-П или требованиям СТО БР ИББС-1.0–2014. Хотя примеры такой практики есть в серии стандартов PCI DSS, где разработчики должны выполнять требования по безопасности в рамках своего специального стандарта.

* * *

Сейчас специализированные учебные центры, а таких уже довольно много, разработали и успешно читают программы по обучению вопросам обеспечения безопасности в соответствии с требованиями Положения Банка России № 382-П. Если бы банки при заключении аутсорсинговых договоров требовали от своих партнеров не только лицензии ФСТЭК по ТЗКИ, но и свидетельства о подготовке их специалистов по таким программам, то уровень доверия к ним был бы значительно выше.

А БЫЛ ЛИ МАЛЬЧИК?[1]

ЭССЕ НА ТЕМУ СТАТЬИ «БАНК, ЕГО АУТСОРСЕР, ИХ РАБОТНИКИ И РАЗРАБОТКА БАНКОВСКОГО ПО»

Сергей ВИХОРЕВ
руководитель направления информационной безопасности НТЦ «Вулкан»

Начну, пожалуй, с цитаты профессора В.А. Канашевского, которого вполне можно поставить в один ряд с юристами, упоминаемыми автором в начале статьи: «…В процессе исследования установлено, что Стандарт СТО БР ИББС-1.4–2018 де-факто позволяет передавать на аутсорсинг поставщикам услуг (т.е. третьим лицам) информацию, относящуюся к банковской тайне, что противоречит действующему законодательству».[2]

Позволю себе порассуждать на эту тему, используя дефиниции ряда нормативных документов Банка России.

Проблема в статье поднята широкая, охватывающая все аспекты аутсорсинга. Но автор, в силу академического подхода, сосредотачивается только на одном — разработке заказного банковского ПО. Наверное, идея о заключении «трёхстороннего пакта» — правильная и может решить юридическую проблему взаимоотношений разработчика заказного ПО и банка. Но! Давайте разберемся: а есть ли вообще такая проблема?

Следуя определению, изложенному в СТО БР ИББС-1.4–2018 «аутсорсинг» — это передача организацией БС РФ на основании договора на длительный срок сторонней (внешней) организации — поставщику услуг выполнения бизнес-функций организации БС РФ, которые являются необходимыми для её деятельности и которые в обычных условиях (без привлечения поставщика услуг) осуществлялось бы организацией БС РФ самостоятельно. Как видим, регулятор отходит от канонического определения понятия «аутсорсинг» и вносит некоторые ограничения, сужая область возможного аутсорсинга. На мой взгляд, ключевыми квалификационными признаками аутсорсинга в определении регулятора являются:

- передача именно бизнес-функций организаций БС РФ;
- длительность отношений организации БС РФ и аутсорсера.

Каковы же бизнес-функции организации БС РФ? Ответ на этот вопрос можно найти в ст. 5 Федерального закона «О банках и банковской деятельности». Причём, список разрешённой таким организациям деятельности, приведённый в законе, довольно обширный, но конечный. Он касается деятельности, связанной с привлечением и размещением денежных средств и различными операциями с ними (наверное, другого и ожидать не стоило). Кроме того, в этой же статье есть прямая императивная норма: кредитной организации запрещается заниматься производственной, торговой и страховой деятельностью, хотя и не возбраняется заключать различные гражданско-правовые договоры. Что из этого следует? Да только то, что разработка ПО не является бизнес-функцией организации БС РФ. И хотя в преамбуле к СТО БР ИББС-1.4–2018, в качестве одного из основных видов бизнес-функций организаций БС РФ, рассматриваемых в качестве приоритетных для возможной передачи на аутсорсинг, упоминаются функции, связанные с применением информационных технологий и, в частности, с разработкой ПО, тезис этот, именно в части разработки ПО, вызывает сомнения, как противоречащий федеральному закону.

Теперь о втором квалификационном признаке аутсорсинга — о длительности отношений между организацией БС РФ и аутсорсером. Регулятор определяет длительность таких отношений сроком не менее 1 года. В остальных случаях передача таких функций определяется, как разовая, на которую этот стандарт не распространяется. Но разработка ПО в редких случаях может превышать 1 год. (Может быть, именно поэто-

[1] М. Горький, «Жизнь Клима Самгина»

[2] Канашевский В.А. Банковская тайна и использование банками услуг аутсорсинга информационной безопасности // Lex russica, 2018. N7. С. 92–97.

му регулятор ввёл в преамбуле в понятие основных бизнес-функций разработку ПО с соответствующей оговоркой в дальнейшем?).

Об услуге. Согласно определениям регулятора, поставщик услуг — обслуживающая организация, специализирующаяся на предоставлении услуг, которой организации БС РФ передают выполнение своих бизнес-функций на аутсорсинг. А что такое услуга? Гражданский Кодекс РФ рассматривает услуги как самостоятельный объект гражданских прав[3], поэтому для регулирования взаимоотношений субъектов, возникающих при оказании услуг, должны применяться не только общие положения ГК РФ, но и его специальные разделы, в частности, положения главы 39. Согласно ГК РФ, услуги выполняются на основании договора возмездного оказания услуг, то есть договора, по которому исполнитель обязуется по заданию заказчика оказать услуги (совершить определённые действия или осуществить деятельность), а заказчик обязуется оплатить эти услуги. Особенностью деятельности по оказанию услуг является также то, что заказчик оплачивает не сам результат, а деятельность по его созданию[4]. Некоторые авторы отличительной чертой услуг считают то, что результат деятельности по оказанию услуги невозможно перепродать, в отличие от результатов работ, выполненных по другим формам договоров. Согласно общему словарю под понятием «услуга» понимается действие, приносящее пользу, помощь другому. Применительно к экономической сфере, под этим понятием понимается работа, выполняемая на заказ и не приводящая к созданию самостоятельного продукта, товара[5].

Договор на услуги в принципе не подходит на рассматриваемую нами роль, поскольку его предметом выступает осуществление определённой деятельности, а не создание ПО и передача на него прав. Услуги по определению реализуются и потребляются в процессе их оказания и не имеют материального выражения. Безусловно, в результате оказания услуг может создаваться в том числе ПО, но такая деятельность является вторичной и, соответственно, права заказчика на такое ПО не защищаются должным образом по договору возмездного оказания услуг.

В отличие от договора на оказание услуг, возможность использования для разработки ПО договора подряда прямо предусмотрена законодательством[6]. Предметом такого договора является выполнение задания заказчика по созданию конкретного ПО. Результатом, в отличие

[3] ГК РФ, часть 1, ст. 128

[4] К примеру, по договору подряда (согласно которому подрядчик обязуется на свой риск выполнить определенную работу по заданию заказчика, а заказчик обязуется уплатить вознаграждение за выполнение задания) оплачивается только готовый результат труда, сданный заказчику.

[5] При этом, выделяется отдельная группа услуг: «услуги нематериальные» — услуги, направленные на удовлетворение потребностей человека как индивидуума и как члена общества. К таким услугам относятся потребности в образовании, медицине, средствах сообщения, информации, духовном развитии, культурном досуге, социальной защите, внешней и внутренней безопасности. Различают нематериальные услуги, оказываемые отдельным лицам (личные или индивидуальные), группам лиц (коллективные) и обществу в целом.

[6] ГК РФ, ст. 1296

от услуг, всегда выступает определённый материальный объект. В рассматриваемом случае таким результатом является программное обеспечение с необходимыми заказчику характеристиками. Таким образом, договор подряда на создание ПО главным образом направлен на разработку такого ПО в строгом соответствии с требованиями заказчика, изложенными в технической документации, и его последующую передачу заказчику. Здесь исполнитель сориентирован именно на результат, а не осуществление имитации деятельности. Помимо этого, так как такой договор направлен на передачу разработанного ПО заказчику, одновременно с ним заказчику переходит исключительное право на заказное ПО, как результат интеллектуальной деятельности, если иное не предусмотрено соглашением сторон.

Обратим внимание на то, что существенным условием договора подряда является наличие чёткого и полного технического задания (ТЗ), описывающего требования к результату работ (требования к функциональности ПО), а также в некоторых случаях — способы реализации ПО, в частности, языки программирования, архитектура приложений и т.д. А на что нас нацеливает документ Банка России? «Организации БС РФ следует применять соглашения об уровне предоставления сервиса ИБ (SLA) для контроля качества услуг аутсорсинга ИБ. SLA — это дополнение к соглашению об аутсорсинге между организацией БС РФ и поставщиком услуг, определяющее предоставление сервиса с заданным уровнем качества[7]». То есть, регулятор определяет, что главным является SLA, а не ТЗ. А SLA — это свойственно именно услугам, а не подряду.

Итак, все эти рассуждения приводят к мысли о том, что разработка ПО — это совсем даже не аутсорсинг, а подряд и, следовательно, вряд ли при заключении договора на разработку ПО целесообразно применять положения СТО БР ИББС-1.4–2018.

Ну, а теперь, наверное, главное, что оставили на десерт — это то, что, по мнению уважаемого профессора В.А. Канашевского, стандарт СТО БР ИББС-1.4–2018 де-факто позволяет передавать на аутсорсинг поставщикам услуг (то есть третьим лицам) информацию, относящуюся к банковской тайне. Есть ли такая опасность? В принципе, если следовать букве закона, то — нет. Рассматриваемый нами документ Банка России охватывает только одну специфическую сторону аутсорсинга — проблему установления требований к управлению и контролю риска нарушения информационной безопасности при аутсорсинге. Но ведь есть и другие документы регулятора. Например, Положение Банка России № 382-П однозначно говорит о том, что организации БС РФ обеспечивают реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры[8]. А новый ГОСТ Р 57580.1 содержит специальную норму СМЭ.6: «выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и (или) модернизации АС, в том числе тестирования ПО и СВТ (далее — сегмент разработки и тестирования)[9]».

Следуя этим действующим нормам регулятора, разработка ПО на «боевой» информации, действительно содержащей сведения, относимые к банковской тайне, в принципе невозможна. Это категорически запрещено. То есть, ситуация, описанная в комментируемой статье — принципиально невозможна, так как противоречит нормативным требованиям. И в подтверждение этому дефиниция из рассматриваемого СТО БР ИББС-1.4–2018: «Политика аутсорсинга должна среди прочего однозначно определять возможность аутсорсинга только в случае соблюдения требований законодательства РФ в области обработки ПДн и информации, составляющей банковскую тайну»[10].

Между тем, рассматриваемая автором статьи ситуация, в принципе не исключается, например, при передаче на аутсорсинг сопровождения и технической поддержки действующего «боевого» ПО. В этом случае опыт и рекомендации автора статьи по заключению «трёхстороннего пакта» будут весьма полезны.

* * *

В заключение напоминаю, что жанр эссе выражает индивидуальные впечатления и соображения по конкретному поводу или вопросу и заведомо не претендует на определяющую или исчерпывающую трактовку предмета.

---

[7] СТО БР ИББС-1.4–2018, п. 12.6

[8] Центральный Банк Российской Федерации. Положение от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», п. 2.5.5

[9] ГОСТ Р 57580.1. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер защиты информации. п. 7.3. 1.2.

[10] СТО БР ИББС-1.4–2018, п. 6.2

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

СКЗИ В ВИРТУАЛЬНОЙ СРЕДЕ

Виртуализация не только словом, но и делом, а точнее рублём, доказала свою эффективность. В сфере информационной безопасности (ИБ), например, работа ряда продуктов для защиты от zero-day атак — «песочниц» — основана на виртуализации. Кроме того, упрощается решение задач по предоставлению сервисов безопасности, автоматизации, моделированию и тестированию. Но в силу национальной специфики помимо технологической составляющей не менее важно мнение по этому вопросу регуляторов российского рынка ИБ.

НОРМАТИВНАЯ БАЗА

ГНИИИ ПТЗИ ФСТЭК России и Технический комитет по стандартизации «Защита информации» (ТК 362) разработали ГОСТ Р 56938–2016 «Защита информации при использовании технологий виртуализации», содержащий описание объектов, перечень угроз, а также особенности реализации мер защиты в виртуальной среде. Кроме того, в статусе проекта находится документ ГОСТ «Требования по защите информации, обрабатываемой с использованием технологии облачных вычислений» с перечнем угроз ИБ для поставщиков и потребителей облачных услуг. В финансовой сфере также существует отраслевой документ Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологии виртуализации» (РС БР ИББС-2.8–2015), содержащий рекомендации по разделению потоков в виртуальной среде, обеспечению безопасности виртуальных машин (ВМ), их образов и терминалов, а также мониторингу ИБ и разграничению полномочий.

В нормативной базе ФСТЭК России меры по обеспечению защиты среды виртуализации присутствуют в приказах № 17, 21, 31 и 239. При этом ФСТЭК не имеет специальных руководящих документов по сертификации виртуальных сред, но ряд производителей сертифицировали свои продукты на соответствие техническим условиям. Средства защиты, работающие в виртуальной среде, могут быть сертифицированы, например, как межсетевые экраны уровня логических границ сети в программном исполнении (тип «Б»). ФСБ же занимается сертификацией в более узких областях ИБ, в основном криптографией, и ряд сертифицированных средств криптографической защиты информации (СКЗИ) могут работать в виртуальной среде при соблюдении ряда дополнительных требований, указанных в правилах пользования.

ИСПОЛЬЗОВАНИЕ СКЗИ

Рассмотрим вопрос: реально ли использовать СКЗИ в виртуальной среде с соблюдением правил пользования, согласованных при сертификации?

Сразу нужно сказать, что на данный момент СКЗИ разных производителей, работающие в виртуальной среде, сертифицированы в ФСБ России по классу КС1. Прецедентов повышения класса до КС2 пока не было, связано это с более жёсткими требованиями в части защиты от несанкционированного доступа. Реализовать их можно с помощью средств доверенной загрузки или сертифицировав гипервизор. На российском рынке перечень таких продуктов крайне ограничен, широкого распространения они пока не получили. В связи с этим рассмотрим общие принципы правил пользования для СКЗИ, сертифицированных по классу КС1, при работе в виртуальной среде.

ВАЖНО!
С-Терра Шлюз и С-Терра Клиент, сертифицированные в ФСБ России как СКЗИ по классу КС1, могут использоваться в виртуальной среде.

РАЗМЕЩЕНИЕ

При эксплуатации СКЗИ, работающих в виртуальной среде, должны соблюдаться требования по физическому размещению, аналогичные требованиям для аппаратных средств. В частности, охрана, пропускной режим, контроль периметра и т.д. В большинстве современных серверных и тем более в центрах обработки данных эти требования выполняются.

Использование виртуализации подразумевает удалённый доступ к ресурсам с клиентских мест, соответственно потребуется защита самих терминалов, запрещается оставлять их без контроля.

ГИПЕРВИЗОРЫ

Перечень гипервизоров и их версии фиксируются на этапе тематических исследований. Для каждого гипервизора производитель СКЗИ описывает требования к эксплуатации (например, перечень файлов для контроля целостности). При этом рекомендуется регулярно устанавливать пакеты обновления безопасности, обновлять инструменты виртуализации, а также утилиты, используемые для управления средой виртуализации.

Учитывая наличие множества уязвимостей, а также динамику роста их количества, пренебрегать установкой обновлений точно не стоит. Например, за последний год было выявлено множество уязвимостей аппаратной части — процессоров Intel, начиная от оригинальных Spectre и Meltdown до L1TF (L1 Terminal Fault), которые с разной степенью надёжности закрываются патчами, выпускаемыми производителями гипервизоров. Теоретически возможна ситуация, когда пользователю требуется новая версия гипервизора (или версия с патчем), которая отсутствует в документации производителя СКЗИ. В этом случае производитель СКЗИ инициирует работы испытательной лаборатории по контролю изменений и далее обращается к регулятору. Если производитель СКЗИ имеет аккредитацию испытательной лаборатории, как, например, «С-Терра СиЭсПи», то сроки выполнения таких работ существенно сокращаются.

АДМИНИСТРИРОВАНИЕ

Гипервизор имеет возможность влиять на функционирование СКЗИ, поэтому потребуется разграничение полномочий администраторов. Необходимо как минимум две роли — администратор виртуальной инфраструктуры, осуществляющий управление ВМ, серверными компонентами, системой хранения данных, а также администратор безопасности, формирующий политику безопасности, ключевую информацию и другие настройки непосредственно СКЗИ. Требование реализуется штатными средствами большинства популярных гипервизоров, а также организационными мерами.

ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ ВИРТУАЛЬНЫМИ МАШИНАМИ (ВМ)

Для защиты от несанкционированного доступа (НСД) требуется контроль информационного обмена между ВМ, в том числе общих областей оперативной памяти хоста. Актуальность угроз этого типа подтверждает целый ряд указанных выше уязвимостей. Защита реализуется встроенными средствами гипервизора или отдельными средствами защиты от НСД. Помимо этого, нужно помнить, что меры безопасности следует применять не только к ВМ с СКЗИ и гипервизору, но и ко всем другим машинам на этом гипервизоре.

На ВМ с СКЗИ, а также на другие ВМ не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность редактирования и просмотр кода и памяти СКЗИ, а также приложений, использующих СКЗИ. Обычно для реализации достаточно организационных мер защиты.

МИГРАЦИЯ И ОТКЗОУСТОЙЧИВОСТЬ

При передаче (миграции) ВМ с СКЗИ по каналам связи вне контролируемой зоны необходимо обеспечить защиту этих каналов сертифицированными средствами защиты.

После ввода в СКЗИ ключевой информации на файл с образом, а также на последующие снапшоты и резервные копии распространяются требования по обращению с ключевыми носителями.

* * *

ФСБ России не накладывает вето на сертификацию СКЗИ в виртуальной среде, множество средств защиты сертифицированы по классу КС1. Для каждого продукта существует ряд ограничений и рекомендаций по использованию в виртуальной среде, исходя из специфических угроз виртуализации. Ограничения делают её эксплуатацию менее удобной, но не перечёркивают большинства преимуществ.

ВАЖНО!

С-Терра Виртуальный Шлюз — виртуальная машина для гипервизоров VMware, Citrix XenServer, Microsoft Hyper-V, KVM и Huawei Fusion, по возможностям аналогичная С-Терра Шлюз в аппаратном исполнении.

Параметр	ПАК	ВМ
Цена	ПО — в рублях, АП — в у.е.	ПО — в рублях
Срок поставки	Недели	Дни
Масштабирование производительности	Новая (более мощная) АП	Новая лицензия
Резервирование	Горячий или холодный резерв с дополнительными затратами	Средствами системы виртуализации без дополнительных затрат
Сертификация ФСБ России по требованиям к СКЗИ	КС1, КС2, КС3	КС1
Сертификация ФСТЭК России по требованиям к МЭ	Тип «А» или «Б»	Тип «Б»

Антон СВИНЦИЦКИЙ
директор по консалтингу
АО «ДиалогНаука»

БЕЗОПАСНОСТЬ ФИНАНСОВ

СТАНДАРТ ГОСТ Р 57580.1–2017 — ПЕРВЫЙ В НОВОЙ ЭКОСИСТЕМЕ РЕГУЛИРОВАНИЯ ИБ В КОМПАНИЯХ, ПОДОТЧЁТНЫХ ЦЕНТРОБАНКУ

В августе 2017 года Ростехрегулирование утвердило национальный стандарт ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер». На данный момент национальный стандарт является рекомендательным, но в нём содержится, например, такое положение: «настоящий стандарт применяется путём включения нормативных ссылок на него в нормативных актах Банка России и (или) прямого использования устанавливаемых требований во внутренних документах финансовых организаций, а также в договорах». Банком России разработаны и опубликованы проекты положений, устанавливающих обязанность кредитных и некредитных финансовых организаций выполнять требования ГОСТ Р 57580.1–2017, начиная с 2021 года. Более того, ссылки на необходимость выполнения требований данного стандарта установлены в приказе Министерства цифрового развития, связи и массовых коммуникаций РФ для информационных технологий и технических средств, использующихся при обработке, включая сбор и хранение параметров биометрических персональных данных в целях идентификации (Приказ от 25.06.2018 г. № 321).

«...И ВОТ ОПЯТЬ»

Исторически Банк России разрабатывает собственные рекомендательные стандарты серии БР ИББС начиная с 2004 года, включающие в себя как базовые документы, содержащие требования к реализации системы обеспечения информационной безопасности и описание порядка проведения оценки соответствия (в том числе методику оценки соответствия), так и рекомендации по реализации отдельных процессов управления и обеспечения ИБ, таких как оценка рисков ИБ, менеджмент инцидентов ИБ, обеспечение ИБ на стадиях жизненного цикла автоматизированных банковских систем и другие. Область применения СТО БР ИББС определялась организацией банковской системы самостоятельно.

С выходом Положения Банка России 382-П были формализованы требования по обеспечению информационной безопасности при осуществлении переводов денежных средств, которые учитывали специфичные процессы и используемые информационные технологии: информационные системы дистанционного банковского обслуживания (в том числе использование мобильных приложений), терминальные устройства дистанционного банковского обслуживания (банкоматы и платёжные терминалы). При этом общие требования к основным процессам обеспечения информационной безопасности в большей степени дублируют положения СТО БР ИББС.

ГОСТ 57580.1–2017 является логичным продолжением многолетней работы Банка России в области стандартизации вопросов обеспечения информационной безопасности, так как в область его «потенциального» действия входят не только банки, но и другие финансовые организации (микрофинансовые организации, бюро кредитных историй, страховые компании и другие).

ОСНОВНЫЕ ПОЛОЖЕНИЯ

Стандарт ГОСТ Р 57580.1–2017 разработан совместно Центробанком и НПФ «КРИСТАЛЛ» (является одним из разработчиков документов Банка России в области стандартизации СТО БР ИББС) и внесён на рассмотрение в Ростехрегулирование техническим комитетом 122 (ТК-122)»Стандарты финансовых операций».

Положения стандарта могут использоваться кредитными и некредитными финансовыми организациями, а также субъектами национальной платёжной системы для достижения следующих целей защиты информации:

- определение требований к составу и содержанию организационных и технических мер защиты информации;
- соответствие состава и содержания мер защиты информации актуальным угрозам безопасности информации и уровню принятого организацией операционного риска (риск-аппетиту);
- обеспечение эффективного контроля состояния защиты информации на основе стандартизованного подхода.

Определение требований к составу и содержанию организационных и технических мер защиты информации осуществляется на основании выбранного уровня защиты. Стандартом установлены три уровня защиты: минимальный (третий), стандартный (второй) и усиленный (первый). Причём в финансовой организации могут быть выделены несколько контуров безопасности, каждый из которых может защищаться по своему уровню.

В соответствии с опубликованным *проектом* Положения Банка России «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности» установлены следующие критерии определения необходимого уровня защиты:

- 1-й уровень защиты (усиленный) — для системно значимых кредитных организаций, выполняющих функции оператора услуг платёжной инфраструктуры значимых платёжных систем, кредитных организаций, значимых на рынке платёжных услуг, при осуществлении более 3 млн банковских операций (среднедневной показатель);
- 2-й уровень защиты (стандартный) — для всех остальных кредитных организаций.

Значение 3 млн единиц операций соответствует критерию отнесения объектов критической информационной инфраструктуры Банка к значимым.

Соответствие состава и содержания мер защиты информации актуальным угрозам безопасности информации и уровню принятого организацией операционного риска (риск-аппетиту) должно достигаться путем адаптации, исключения и дополнения базового набора мер по результатам моделирования угроз безопасности информации и оценки рисков с учётом особенностей информационной инфраструктуры и реализуемых бизнес-процессов и/или технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств организации.

ГОСТ Р 57580.1–2017 описывает следующие основные направления в рамках организации системы защиты информации Банка:

- обеспечение защиты информации при управлении доступом;
- обеспечение защиты вычислительных сетей;
- контроль целостности и защищённости информационной инфраструктуры;
- защита от вредоносного кода;
- предотвращение утечек информации;
- управление инцидентами защиты информации;
- защита среды виртуализации;
- защита информации при осуществлении удалённого логического доступа с использованием мобильных (переносных) устройств;
- защита информации на этапах жизненного цикла автоматизированных систем и приложений.

В рамках каждого направления определен перечень мер, необходимых к реализации как в виде организационных мероприятий по защите информации, так и путём применения специализированных средств защиты информации. Если мера защиты информации не может быть реализована, то необходимо рассмотреть возможность (а в отдельных случаях необходимость) применения компенсирующих мер, направленных на обработку рисков, связанных с реализацией тех же угроз безопасности (перечень рассматриваемых угроз должен учитывать положения базовой модели угроз и нарушителей безопасности информации, описанные в Приложении А к ГОСТ Р 57580.1–2017). При этом выбор компенсирующих мер должен быть формализован и закреплён во внутренних нормативных документах организации.

Также стоит обратить внимание, что часть мер, описанных в стандарте, дополняют друг друга и могут быть использованы как компенсирующие.

Обеспечение эффективного контроля состояния защиты информации на основе стандартизованного подхода должно достигаться путём реализации следующих мероприятий:

- осуществление мониторинга и контроля состояния защиты информации;
- проведение оценки эффективности реализованных мер;
- анализа и совершенствования системы защиты информации;
- проведения периодической независимой оценки выполнения установленных требований.

А судьи кто?

Примерно через полгода после принятия ГОСТ Р 57580.1–2017 была принята методика оценки соответствия (ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»). Методика оценки соответствия содержит описание как процесса проведения оценки соответствия, так и требования к формированию отчётных материалов по результатам оценки.

Оценка выбора и реализации финансовой организацией организационных и технических мер ЗИ в соответствии с требованиями ГОСТ Р 57580.1–2017 должна проводиться только независимой организацией: обладающей необходимой компетенцией (порядок оценки такой компетенции не определён) и лицензией на деятельность по технической защите конфиденциальной информации.

Оценка выбора и реализации финансовой организацией организационных и технических мер ЗИ в соответствии с требованиями ГОСТ Р 57580.1–2017 должна проводиться только независимой организацией

И если процесс оценки соответствия требованиям ГОСТ Р 57580.1–2017 не сильно отличается от процесса, описанного в документах стандарта Банка России СТО БР ИББС-1.1, то подход к оценке реализации мер защиты информации кардинально изменён:

1. Из методики убраны оценки, соответствующие состоянию «не в полной мере», «практически полностью», «что-то делается», позволявшие довольно расширенное толкование со стороны проверяющих: все меры, описанные в разделе 7 ГОС Р 57580.1–2017, оцениваются по следующей шкале:
   - 0 — мера не выбрана;
   - 1 — мера выбрана;
2. Процессы управления информационной безопасности (планирование, реализация, контроль и совершенствование) рассматриваются не в разрезе всей организации, а применительно к 8 основным процессам, описанным в разделе 7 ГОСТ Р 57580.1–2017.
3. Перечень мер защиты информации, подлежащих оценке, может быть скорректирован по результатам работ по их адаптации и/или применения компенсирующих мер, направленных на обработку рисков, связанных с реализацией тех же угроз безопасности.
4. Если в организации выделены несколько контуров безопасности, то оценка должна формироваться независимо для каждого контура с общей итоговой оценкой соответствий всей организации.

Другим нововведением, определяемым ГОСТ Р 57580.2–2018, являются детализированные требования к отчётным документам, формируемым по результатам оценки соответствия. К таким требованиям в том числе относятся:

- отчёт по результатам оценки соответствия защиты информации должен быть прошит и скреплён мастичной печатью проверяющей организации с указанием количества листов в заверительной надписи, подписанной руководителем проверяющей группы;
- для каждого электронного документа, файла данных, прилагаемых к отчёту по результатам оценки соответствия ЗИ, должны быть вычислены хэш-функции, реализованной в соответствии с ГОСТ Р 34.11–2012.

* * *

Выпущенные под контролем Банка России национальные стандарты ГОСТ Р 57580.1–2017 и ГОСТ Р 57580.2–2018 несколько нарушают традиции отраслевого стандарта СТО БР ИББС, тем не менее понятно, что это только первые документы в создаваемой экосистеме регулирования информационной безопасности в компаниях, которые подотчётны Центробанку. Аналогичный путь для банков, проделанный стандартом СТО БР ИББС, показывает, что со временем и ГОСТ Р 57580.1 также станет фактически обязательным, причем для значительно большего круга организаций, в частности, некредитных финансовых компаний. Поэтому для таких компаний логично рассмотреть возможность реализации данного стандарта уже сейчас. Пока конкретных сроков перевода требований ГОСТ в разряд обязательных официально не названо, в проектах Положений Банка России указан 2021 год.

ИСТОРИЯ ОДНОГО СЕРВИСА

ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

Алексей МАЛЬНЕВ
руководитель Jet CSIRT, компания «Инфосистемы Джет»

В 2018 году наша компания вывела на рынок новый сервис аутсорсинга информационной безопасности — центр мониторинга и реагирования на инциденты ИБ Jet CSIRT. Сегодня мы приоткроем завесу тайны и поделимся подробностями нашей внутренней кухни. В этой статье я расскажу, какие факторы нас подтолкнули к созданию продукта, почему мы решили двигаться именно в направлении экспертных сервисов, как сформировали структуру услуги, которая оптимально решает задачи заказчиков, и каким образом воплотили идею в реальность.

ЗАЧЕМ РЫНКУ ЕЩЁ ОДИН ЭКСПЕРТНЫЙ СЕРВИС?

Сегодня на рынке представлено довольно много сервисов информационной безопасности, почему мы решили создать ещё один? Первой причиной стало понимание назревшей проблемы: большинство сервисных продуктов покрывает потребности клиентов лишь частично. Так, при выводе новых услуг аутсорсинга ИБ на рынок сервис-провайдеры чаще всего руководствовались двумя принципами: «есть угроза — создадим услугу» и «есть продукт — создадим облачный сервис». При этом они, как правило, не проводили тщательный анализ рынка и запросов типового заказчика, а иногда и вовсе действовали по наитию. В результате многие сервисы не пользовались высоким спросом, были убыточными, вызывали нарекания клиентов и т.д. Косвенно этот факт доказывает очень малое число компаний, действительно сделавших хороший устойчивый бизнес в этом сегменте. В России их можно перечесть по пальцам одной руки, и это при высоких темпах роста рынка! Наша задача заключалась не в создании очередного сервиса «в тренде», а в применении новых подходов, основанных на анализе рынка и клиентов, и создании либо корректировке услуг уже на базе этого фундаментального знания.

Другая причина, которая побудила нас к формированию новой услуги, — высокий потенциал рынка аутсорсинга ИБ. Сегодня мы наблюдаем пять мощных благоприятных факторов для развития экспертных сервисов. Это глобальное развитие аутсорсинга во всех сферах мировой экономики, глобальное повышение значимости информации и её безопасности, рост количества угроз, развитие нормативно-правовой базы в области защиты информации, а также глобальная проблема дефицита высококвалифицированных кадров.

ЭФФЕКТИВНЫЙ СЕРВИС ЗА ТРИ ШАГА

Имея за плечами многолетний опыт аутсорсинга ИБ и сервисного бизнеса в целом, взаимодействуя с десятками действующих и потенциальных клиентов, мы определили для себя три шага, которые должны были помочь нам найти оптимальную концепцию сервиса аутсорсинга Incident Response.

Шаг 1. Изучить уровень зрелости ИБ реальных клиентов и определить их слабые и сильные стороны.

Первым делом мы изучили рынок на основе анализа выборки из 30 уже хорошо известных нам клиентов из основных секторов экономики: ТЭК, промышленность, финансы, госсектор, телеком, транспорт и торговля. В итоге сформировали следующую таблицу:

№ клиента	Уровень зрелости процессов ИБ	Уровень зрелости технологий ИБ	Уровень квалификации ИБ	% процессов In-house	% процессов на аутсорсинге
1					
…					
30					

Для расчёта уровня зрелости мы использовали собственную методику, базирующуюся на методиках Института программной инженерии Карнеги-Меллона и Университета Родса. Если обобщить, то оцениваемые уровни зрелости по разным аспектам, таким как команда, технологии, бизнес и процессы, в итоге суммируются по баллам от 0 до 5. При этом 0 означает полное отсутствие возможностей, 5 говорит о присутствии абсолютно всех возможностей по всем аспектам. В реальном мире оптимальный уровень зрелости большинства организаций составляет около 3. Значения от 4 до 5 могут подразумевать избыточный перекос в сторону ИБ от бизнеса и меньшую гибкость.

Статистика по показателям зрелости у нас вышла следующая (рисунок 1).

Рисунок 1. Статистика по показателям зрелости

Итоговая картина продемонстрировала в среднем довольно низкий уровень зрелости процессов, но чуть больший уровень технологий. Мы пришли к выводу, что экспертная помощь клиентам в среднем нужна больше, нежели инструменты аутсорсинга. Хотя и с инструментами у многих проблемы, учитывая их сложность и стоимость.

Шаг 2. Найти диспропорцию в процессах ИБ клиентов для правильной фокусировки услуги.

Изучив аналогичную выборку клиентов, мы определили, что в подавляющем числе случаев заказчику необходима помощь не только в детектировании атак, но и в реагировании на инциденты.

Дело в том, что процесс Incident Response часто упрощают, в действительности он включает примерно 20 подпроцессов в рамках 4 больших этапов. Детектирование — важный элемент, но без равномерной развитости процессов общая эффективность будет приближаться к самому слабому звену. Оказалось, что 21 из 30 клиентов эту проблему полностью осознают. Практика показала, что подключение зрелого коммерческого SOC вызывает откровенную диспропорцию в процессах Incident Response: достигается приемлемый уровень зрелости процессов детектирования (2–3) при зачаточном уровне развития реагирования на стороне заказчика (0–1).

Стало очевидно, что примерно 70–80% клиентов необходима поддержка в области всех процессов Incident Response. Если отталкиваться от NIST 800–61r2, то она нужна и на следующих этапах:

- подготовка, планирование, выстраивание процессов центров мониторинга ИБ, настройка инструментов;
- детектирование, расследование и анализ инцидентов;
- реагирование в части локализации, нейтрализации и восстановления;
- постинцидентная активность.

То есть большинство однозначно нуждается в комплексной помощи, а не узких сервисах по аналитике. Другими словами, клиентам требуется помощь и по технике, но в первую очередь по процессам и людям. Исключение составляют единицы (<<10%) крупнейших компаний России с развитыми SOC.

Шаг 3. Определить ценности клиента

Как я говорил выше, если сервис-провайдер изначально не понимает ценности клиента, он не может предложить оптимальную услугу по соотношению цена/качество/функции для организации комфортного и эффективного сотрудничества.

Иногда незначительные дополнительные опции могут оказаться крайне важными и полезными, и не нужно выставлять за них счёт. Нередко это напрямую влияет на основные потребности клиента, не требует больших затрат и становится важным условием повышения его лояльности. Эффект аналогичен бесплатному Wi-Fi в ресторане.

Для получения фундаментальной картины и понимания мы искали модель, которая подсказала бы нам:

- как определить главные ценности клиента;
- как определить процессы, которые заказчик хотел бы реализовать самостоятельно (In-house);
- как определить процессы, которые он может легко отдать на аутсорсинг.

Ряд интересных идей и выводов нам помогла сделать методика Wardley Value Chain Mapping. В оригинале она решает задачу выявления ключевых потребностей клиента сервиса и методов их достижения (в любой отрасли).

На первом этапе построения сервиса мы должны определить потребности, причём важно сосредоточиться именно на главной потребности клиента. Если выстраивать услугу вокруг вторичных потребностей или тем более вокруг компонент, возрастает риск упустить что-то важное.

Проводя изучения в области Incident Response, мы получили следующую картину (рисунок 2).

Нетрудно заметить, насколько сложная взаимосвязь между потребностями, обеспечивающими их сервисами и компонентами разных уровней, насколько те либо иные компоненты отличаются по природе, уровню интеграции в готовые продукты, необходимости кастомизации под инфраструктуру клиентов, возможности их масштабирования в сервисной модели.

Методика также показала, что обеспечение основных потребностей клиента в области Incident Response возможно толь-

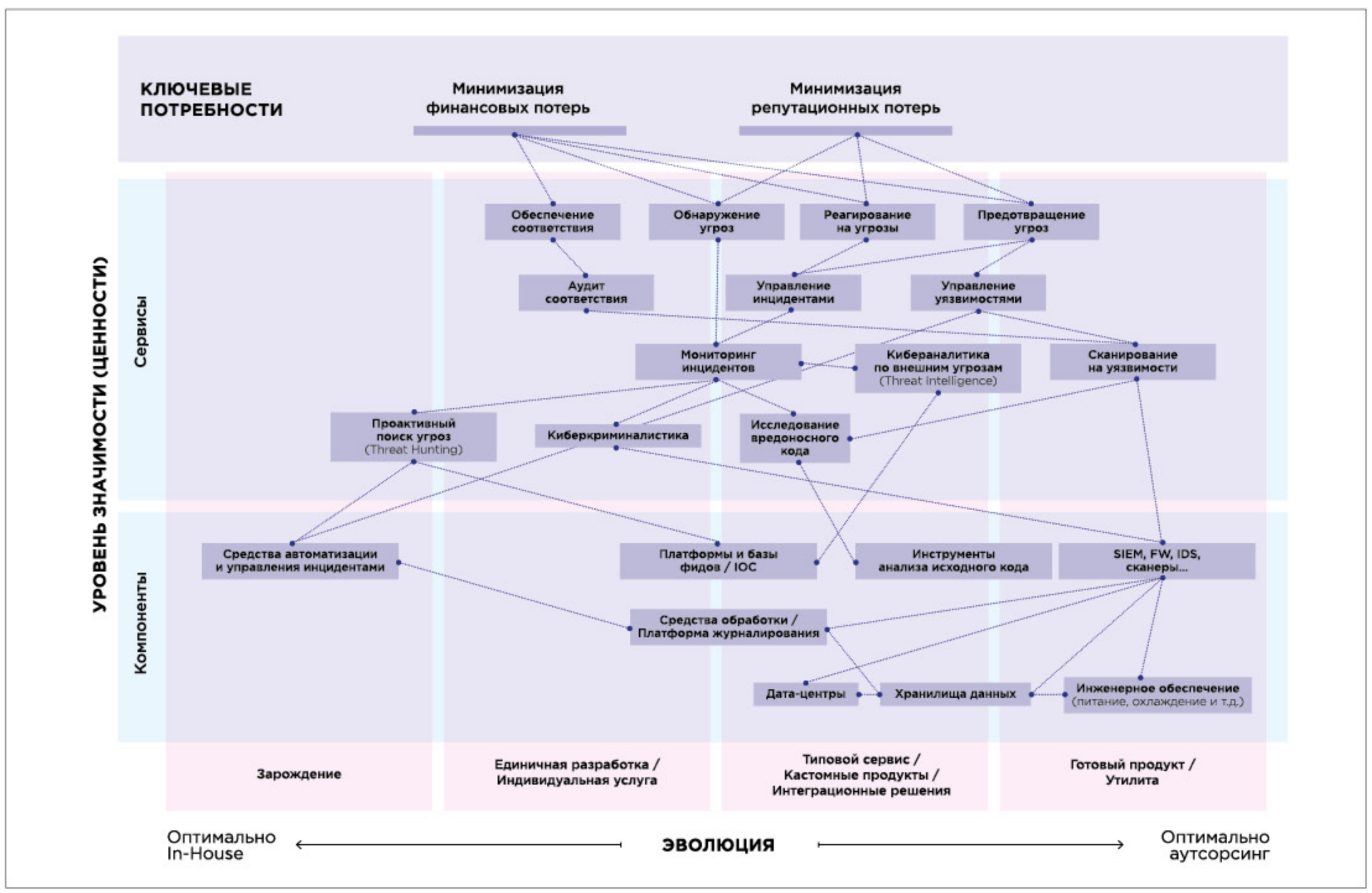


Рисунок 2. Взаимосвязь между потребностями, обеспечивающими их сервисами и компонентами разных уровней

ко через комплексный подход, когда мы берём на поддержку большую или значительную часть процессов. Именно в этом ошибка многих сервисов мониторинга и реагирования на инциденты ИБ — они фокусируются на слишком узкой области, оказывая сервисы уровня компонент.

НОВЫЙ СЕРВИС: ЧТО В РЕЗУЛЬТАТЕ?

Проведя всесторонний анализ рынка под тремя разными углами и отталкиваясь от карты Уордли, мы пришли к выводу, что нам нужно реализовать комплексную услугу по предотвращению, обнаружению и реагированию на угрозы, полностью покрывающую ключевые потребности заказчиков. При этом у нас было чёткое понимание, что на уровне компонент мы должны быть готовы к решению задач по обеспечению соответствия требованиям регуляторов и к предоставлению ряда других дополнительных функций.

Такой подход априори требовал значительных ресурсов, разной специализации и высокой квалификации. Здесь нам способствовало наличие в компании большой и сильной команды экспертов по информационной безопасности, включающей около 200 специалистов различных профилей.

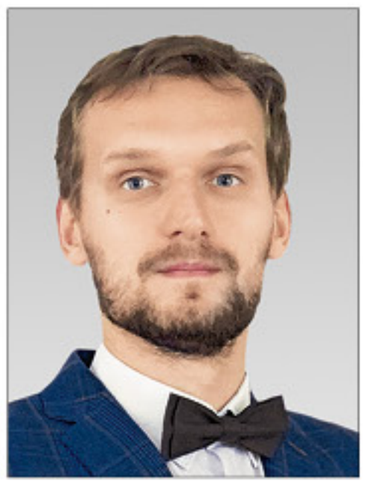
Мы выбрали концепцию центра мониторинга и реагирования на инциденты (CSIRT — Computer Incident Response Team), предполагающую максимально глубокое погружение в инфраструктуру клиента и широкий охват по ИБ-сервисам.

Наш текущий список сервисов Jet CSIRT выглядит следующим образом:

- мониторинг событий ИБ;
- подключение источников событий;
- расследование инцидентов ИБ;
- киберанаалитика по внешним угрозам;
- управление уязвимостями;
- разработка уникальных сценариев выявления инцидентов;
- техническое реагирование, сдерживание и нейтрализация угроз;
- проактивный поиск и обнаружение угроз;
- эксплуатация СЗИ;
- предоставление СЗИ по подписке;
- управление жизненным циклом инцидента;
- изучение вредоносного кода;
- аналитика по открытым данным (OSINT);
- бизнес-ориентированная аналитика;
- взаимодействие с ГосСОПКА;
- комплексное ИБ-консультирование;
- аудит и анализ защищённости;
- форензика.

* * *

Сегодня Jet CSIRT успешно функционирует, помогая заказчикам из самых разных отраслей комплексно решать задачу по обеспечению безопасности ИТ-инфраструктуры. В наших планах — дальнейшее расширение и углубление возможностей в части киберкриминалистики и OSINT-технологий, а также обогащение опыта в части взаимодействия с ГосСОПКА.



Алексей ДАНИЛИН
руководитель направления по развитию бизнеса Positive Technologies

КАК ОБНАРУЖИТЬ ЦЕЛЕВУЮ АТАКУ НА БАНК?

СЛЕДУЕТ ПРИМЕНЯТЬ КОМПЛЕКСНЫЕ ANTI-APT РЕШЕНИЯ

Целевые атаки на банки — прибыльное дело для злоумышленников: создатели WannaCry заполучили всего $140 тыс., а вот Cobalt только в России в прошлом году украла около 1.1 млрд руб., атаковав более 240 организаций (из них 11 — успешно). Всего за несколько лет группировка похитила более €1 млрд у 100 банков из 40 стран мира. Тем не менее обнаружить признаки такого целевого вторжения и предотвратить ущерб от него вполне возможно и помочь в этом призваны специализированные Anti-APT решения.

Cobalt проникали в инфраструктуру банков с помощью фишинговых писем, рассылаемых их сотрудникам. После заражения ПК работника, загрузившего вложение, атакующие искали внутри сети банка узлы, связанные с управлением банкоматами, компрометировали их и заражали ATM вредоносным ПО для манипуляций с диспенсером. Далее происходила управляемая выдача денег подставным лицам — дропам. После проникновения взломщики обычно не торопились, действуя с максимальной осторожностью. Например, атака Cobalt на один из банков в восточной Европе началась с рассылки вредоносных писем в середине лета, а хищение денег произошло только в октябре. Этот промежуток времени может быть короче, но у ИБ-специалистов всё же есть некоторое время для выявления такой активности.

В ОЖИДАНИИ АТАКИ

Для первичного сбора данных об организации злоумышленники используют открытые источники: им нужны имена и e-mail сотрудников. Поэтому для начала необходимо выяснить, какая информация об организации есть в интернете. Например, наличие в сети e-mail сотрудников можно проверить с помощью сервисов типа Hunter и при необходимости присвоить им новые адреса. Важен и регулярный мониторинг даркнета: здесь могут встретиться объявления о покупке/продаже учетных записей сотрудников организации, ее партнеров, подрядчиков, заказчиков и пр. В 59% объявлений о продаже данных в дарквебе речь идет об учетных данных для доступа к различным ресурсам, в т.ч. и к банковским приложениям. Необходимо также проводить аудит периметра, выявляя уязвимые веб-приложения организации, доступные из глобальной сети. Помимо этого, важен комплексный анализ ИТ-инфраструктуры в целом, включая аудит веб-приложений и беспроводных сетей.

ВО ВРЕМЯ ФИШИНГА

Представим, что на банк уже идёт фишинговая атака. Наибольшую угрозу представляет целевой фишинг, т.н. spear phishing, когда письма заточены на конкретного получателя. Именно такой вид фишинга использовала группировка Cobalt, и в 2017 и 2018 гг схема доставки была такова: письма содержали ссылку на вредоносный документ, содержащий эксплойты для удалённого исполнения кода в Microsoft Word и размещённый на ресурсе, подконтрольном Cobalt.

Сотрудник банка переходил по ссылке и, после открытия страницы в браузере, эксплуатировались уязвимости, позволявшие заразить ПК пользователя вредоносным ПО. Корреспонденция имитировала счёта-фактуры, приказы из отдела кадров, сообщения службы ИБ, регулятора, коллег из других компаний и др. В последнее время группировка сначала атаковала контрагентов целевых банков, а потом рассылала фишинговые пись-

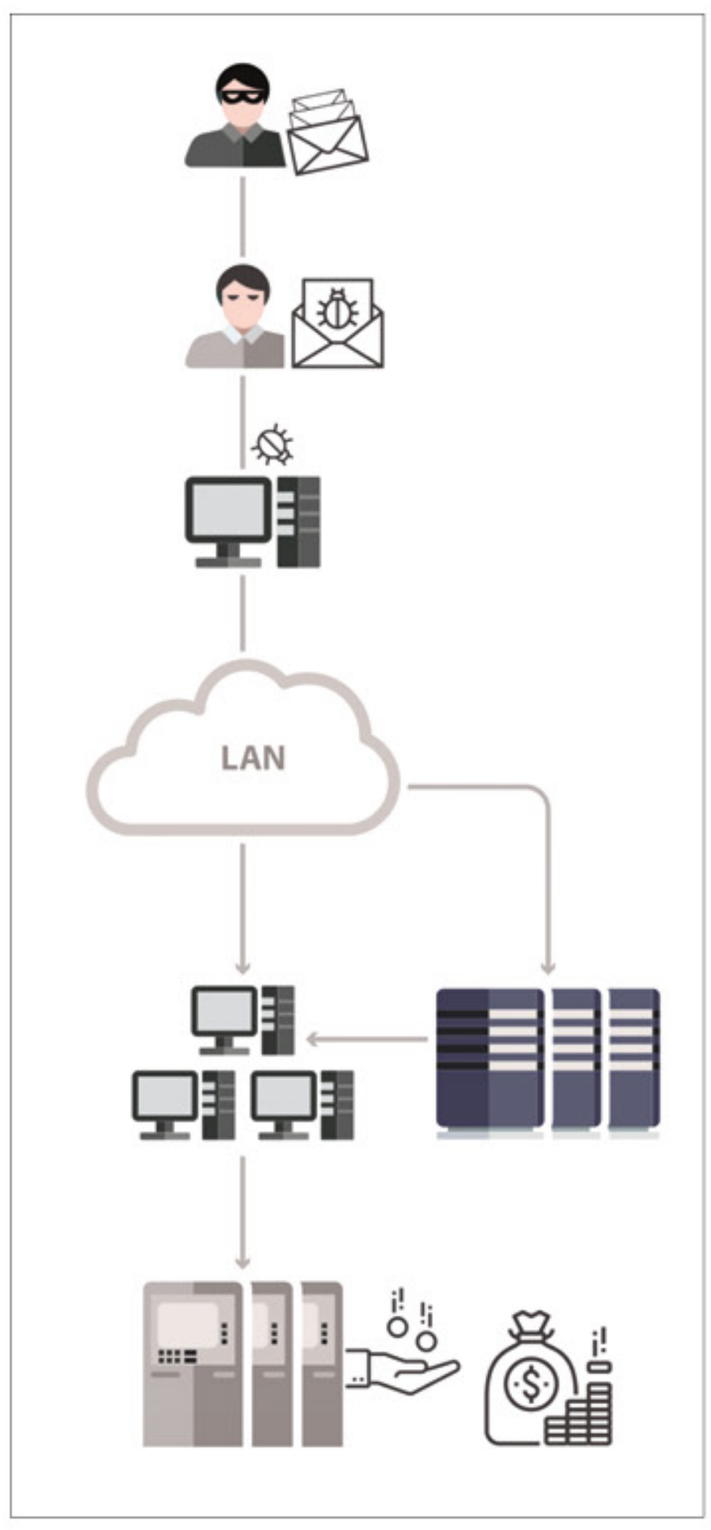


Схема атаки Cobalt на банк

ма с захваченных адресов. В такой ситуации по нашей статистике каждый третий сотрудник (33 %) нажимает на вредоносную ссылку и переходит на вредоносный сайт. Для борьбы с фишинговыми письмами важны регулярное обучение сотрудников и повышение их информированности. Однако 38 % компаний ими пренебрегают, а ещё 37 % делают это формально, не проверяя на эффективность. Также важно предотвратить эксплуатацию уязвимости и вредоносное заражение, для чего необходимо своевременно устанавливать обновления безопасности, в том числе и для прикладного ПО, и, конечно, обновления антивирусной защиты.

Эффективным средством обнаружения и блокировки фишинговых писем может стать многоуровневая система защиты от твредоносного ПО — PT MultiScanner. С помощью набора дополняющих друг друга антивирусных движков, статического анализа, «песочницы» и репутационных списков она позволяет эффективно выявлять и нейтрализовывать попытки доставки вредоносных файлов. Другой её плюс — автоматизация обработки, поступающей от антивирусов информации. В тех случаях, когда вредоносное ПО ещё не известно антивирусам, в игру вступает «песочница», позволяющая анализировать объекты в динамической среде. Это новый модуль проверки, реализованный в PT MultiScanner. Помимо этого, «песочницы» могут использоваться для обнаружения вредоносного ПО, способного мимикрировать, для выявления угроз, скрывающихся за фишинговыми ссылками в письмах. Специальный «кликер» может «прокликать» такие ссылки и выявить опасные файлы, которые скрываются за ними. К пользователю такое письмо не попадёт.

Ещё один способ поймать фишиговую атаку — выявить её прямо в трафике с помощью его глубокого анализа. Например, во время пилотного проекта в одном из российских банков PT Network Attack Discovery (предназначенный для анализа сетевого трафика) зафиксировал несколько десятков классов инцидентов ИБ, которые могли бы повлечь за собой успешные кибератаки со стороны внешнего нарушителя. В частности, сетевые взаимодействия рабочих станций сотрудников с фишинговым доменом. Другими методами аномальные соединения с ресурсами, аффилированными известным группировкам, обнаружить сложно.

Для выявления вредоносного ПО или атак, неизвестных на момент проникновения, может быть использован механизм ретроспективного анализа (реализованный в PT MultiScanner и PT Network Attack Discovery).

В ПОИСКАХ АТАКУЮЩЕГО ВНУТРИ

100% гарантии того, что целевая атака будет остановлена на уровне периметра, нет: группировки уровня Cobalt действуют изощрённо, например, рассылают фишинговые письма не только на корпоративные почтовые адреса сотрудников, но и на личные. Или применяют метод «водопоя» (Watering hole), размещая вредоносные файлы на публичных сайтах, популярных среди потенциальных жертв. Кроме того, не во всех APT-атаках используются вредоносные объекты: в их основе может быть эксплуатация уязвимостей или удалённое выполнение кода. Поэтому главное — своевременно выявить действия злоумышленника во внутренней сети. Например, попытки горизонтального перемещения внутри инфраструктуры с целью добраться до критических элементов, атаки на Active Directory (доменную архитектуру организации) и другие подозрительные события в трафике. В автоматизированном режиме это позволяет сделать PT Network Attack Discovery, благодаря умению строить карту сетевых взаимодействий. Это даёт возможность увидеть пошаговые действия злоумышленников внутри сети и определить все заражённые хосты.

Выявить использование нестандартных портов, попытки эксплуатации уязвимостей или манипуляции с банкоматами на компьютере банковского специалиста во время его отсутствия на рабочем месте позволит и система класса SIEM — MaxPatrol SIEM. Например, в случае с упоминавшейся атакой Cobalt на восточно-европейский банк приоритизация событий из журналов антивирусов с помощью SIEM могла бы помочь обнаружить атаку и предотвратить хищение денег. Но такой приоритизацией, к сожалению, мало кто занимается.

РАБОТА НАД ОШИБКАМИ

Важная часть работы — полноценное расследование произошедшего инцидента и устранение лазеек для его повторения. Например, расследуя одну из атак на банк, в ходе которой злоумышленники подменяли реквизиты платёжного поручения (в этом случае проблематично доказать автора подмены без специальных навыков в области ИБ), эксперты подразделения PT Expert Security Center (PT ESC) Positive Technologies стали свидетелями повторного появления кибервзломщиков. Прямо в ходе анализа инфраструктуры при расследовании был зафиксирован факт «возврата за добавкой»: злоумышленники подключались к тому же самому серверу с помощью приложения для удалённого управления ПК. Это лишь один из многих примеров, демонстрирующий, что все щупальца, оставленные атакующими, надо оперативно выявлять и предотвращать повторение ситуации.

* * *

Целевое вторжение в банк не осуществляется мгновенно: атаку можно выявить на ранней стадии, когда деньги ещё не выведены из банка. Для её обнаружения необходимо применять комплексные Anti-APT решения, включающие в себя и выявление фишинга, и ретроспективный анализ вирусов, и обнаружение подозрительной сетевой активности, и корреляцию событий. Такие решения работают как колокольчики и капканы, размещённые в самых неожиданных местах банковской инфраструктуры, и препятствуют продвижению нарушителя. Безусловно, такая технологическая платформа должна иметь обвязку из регулярного повышения осведомлённости сотрудников в вопросах ИБ, мониторинга открытых данных и расследования инцидентов.

НЕ ОМОЛОГАЦИЯ ПРОДУКТА, А СОЗДАНИЕ НОВЫХ ЦЕННОСТЕЙ!

ОБ ИМПОРТОЗАМЕЩЕНИИ И ШИРЕ

Андрей АКИНИН
генеральный директор компании Вэб Контрол

Сегодня в силу ряда политических и экономических причин, отечественный рынок IT за счет внедрения импортозамещения получил мощный толчок к развитию. При этом сам термин «импортозамещение» имеет скорее политический характер. И по сути представляет собой ряд протекционистских мер, позволяющих отечественным производителям чувствовать себя комфортнее.

Но такая ситуация имеет временный характер, поэтому российские разработчики должны воспользоваться сложившимися условиями, чтобы создать продукты, способные конкурировать на открытом рынке. Каким бы большим ни был наш рынок, его размер ограничен. Соответственно, ограничен и доход, который смогут получить отечественные производители.

В условиях импортозамещения в замкнутом пространстве развитие могут получить лишь несколько компаний — лидеров рынка. Для действительно масштабного развития нашей отрасли необходимо говорить о создании качественных конкурирующих продуктов, то есть о разработке таких продуктов, которые смогут потеснить на мировых рынках решения ведущих зарубежных производителей.

Чтобы такой экспортоориентированный бизнес устойчиво развивался, требуется участие в технологических партнёрствах и активная поддержка государства.

В национальной программе «Цифровая экономика РФ» прописано, что государство планирует вывести отечественное ПО на конкурентный рынок и добиться его преимущественного использования в госорганах. Если речь идет о развитии отрасли IT в целом, такой уровень притязаний мне кажется изначально заниженным. Если планку поставить выше, то по итогам реализации программы наши продукты вполне могут войти в пул лидеров по экспорту информационных технологий.

ВЫБОР ПУТИ

На пути создания своих «бриллиантовых» продуктов перед отечественной отраслью IT открываются разные пути.

Наиболее быстрый и дешёвый — вывод на рынок уже известного зарубежного продукта, но под своей маркой. Это может быть OEM соглашение, White Label или приобретение прав на исходные коды. Такие продукты, как правило, не создают новой ценности, это лишь перенос передовых технологий на локальный рынок. Что в результате имеет заказчик? Не всегда самый свежий продукт, зачастую не отвечающий актуальным потребностям рынка. И тут не стоит забывать, что среди западных вендоров тоже есть продукты, отстающие от отдельных отечественных решений лет на десять.

Другой путь — создавать своё, оригинальное и революционное. Но очевидно, что это требует значительных затрат времени, финансов и человеческих ресурсов. Кроме того, вывод на рынок новых продуктов требует больших маркетинговых вложений. Из отечественных производителей, к сожалению, это мало кому доступно.

Кроме того, помимо денег, для революционных продуктов нужна идея. Именно поэтому, такие продукты — случай, как правило, исключительный. В условиях развитого рынка очень сложно создать то, что никто еще не делал. А инвестировать в создание продуктов, аналогичных решениям от Symantec, Check Point, IBM и т.д., рискованно и неинтересно для самих предпринимателей, тем более в условиях строго ограниченного рынка. Мы не должны быть в роли «догоняющего». У нас должен быть свой уникальный путь.

ИНТЕГРАЦИЯ И ПАРТНЕРСТВО

Кооперация производителей, занимающихся созданием продуктов в смежных областях, становится перспективным трендом на мировом рынке. Каждый разработчик имеет свою специализацию в определенной области. Отечественная ИТ-отрасль может получить пальму первенства, если объединит усилия для достижения заданной цели.

Кроме того, современный потребитель избалован, его уже не устраивает коробочный продукт, он требует индивидуального подхода и разнообразного выбора, и это — большой вызов для разработчиков. Чтобы соответствовать ожиданиям клиентов, логично максимально использовать возможности глобальной цифровой экономики, а для этого необходим переход от конкуренции к технологическому партнёрству.

Смысл интеграции заключается в том, что за счет высокой специализации при создании собственных продуктов, значительно повышается привлекательность конечного продукта. Многие западные международные компании решают вопрос развития продуктов пу-

тем приобретения перспективных стартапов и интеграции их в свою продуктовую линейку.

Для того, чтобы занять свою рыночную нишу, гораздо удобнее уцепиться за кого-то более сильного. Российский рынок пока находится на стадии осознания этого тренда.

Также важно, что технологическое партнёрство, предполагая понимание уникальности и сильных сторон каждого разработчика, ориентируется на развитие и рост всей отрасли, а не своей доли в ней. Такое взаимодействие выводит платформы и продукты на новые рынки и помогает компаниям перепрыгнуть традиционные барьеры при расширении и масштабировании, используя ключевые компетенции своих партнёров. Не нужно продолжать разрабатывать, к примеру, SIEM системы, лучше попытаться развивать собственные сильные стороны, сосредоточиться на удобстве и доступности отдельной разработки.

Чтобы соответствовать международным трендам, отечественным разработчикам IT-систем, нужно активно вступать в партнёрства с ведущими как российскими, так и иностранными вендорами.

ЗАМЕЧАНИЯ ПО ТЕМЕ

IT-отрасль больше, чем любая другая, тяготеет к нестандартным, но простым решениям. Поэтому, не мудрствуя лукаво, делайте просто и удобно для пользователя, но не забывайте о том, куда движется мир. Ориентируясь исключительно на текущие потребности, вы рискуете получить на выходе уже устаревший продукт.

Не надо пытаться создавать универсальные продукты в тех нишах, где много конкурентов. Самостоятельная ценность продуктов сегодня сильно преувеличена. Только создавая продукт, обладающий развитыми средствами автоматизации, открытым интерфейсом, интеграцией со смежными решениями, можно выйти на конкурентный уровень. При этом наличие гибкой и удобной интеграции с другими системами делает такие разработки наиболее привлекательными и для заказчика, и для инвестора.

Кроме того, если ваше решение будет качественным и продуманным, вы можете объединиться с другими вендорами. Очень мало решений живет долго. Большинство разработок, попав к крупному вендору, преобразуется в новые решения, учитывающие опыт, ошибки и требования рынка.

По сути ИБ — сама по себе сфера горизонтальная, она закрывает собой определённый технологический пласт, который используется различными вертикалями

Существует много примеров интегрированных комплексных решений, но ни одно из них не создавалось с нуля, все они в своем большинстве собирались из органически нишевых продуктов крупными вендорами.

ПРО ИБ

Универсальные решения хороши, когда речь идёт об общей безопасности. К примеру, когда крупная компания разворачивает свои CRM-системы внутри облачного сервиса, критически важные данные могут стать неподконтрольными. Невозможно отследить, где проходит граница между личной и корпоративной информацией. На этом этапе и возникает потребность в специализированных решениях, позволяющих защитить конкретные процессы. Большинство западных вендоров предлагает именно такие нишевые решения.

В таком контексте я с осторожностью отношусь к мнению коллег, предлагающих создавать вертикально интегрированные программные решения для определённых областей. IT уже давно не привязаны к вертикалям: и банки, и нефтеперерабатывающая промышленность используют одни и те же технологии. Куда важнее и проще создавать горизонтальные продукты, которые будут хорошо защищать облачные технологии, внутренний информационный обмен, работу на end point, колл-центры, привилегированный доступ и пр.

По сути ИБ — сама по себе сфера горизонтальная, она закрывает собой определённый технологический пласт, который используется различными вертикалями.

На форуме InfoSecurity Russia 2018, который состоится 21–23 ноября в Москве, Web Control проведёт тематическую сессию, где предложит обсудить вопросы интеграции ИБ-продуктов в горизонтальной плоскости. Мы хотим собрать в одном месте отечественных вендоров, которые думают о том, как вместе противостоять крупным западным производителям.

Главная задача для нас — создать группу отечественных разработчиков, основанную на принципах технологической кооперации. Такая команда сможет делать конкурентные продукты, способные выйти на международный рынок или станет основой для создания крупного отечественного консорциума. Подобные структуры уже пытаются создать Ростех, Ростелеком, Infowatch. При этом хочется надеяться, что они не пойдут по пути создания закрытых экосистем, неспособных конкурировать с западными разработчиками.

Специфика IT- и ИБ-отраслей такова, что для их развития не требуется дорогостоящего оборудования, как, например, в автомобилестроении, не нужны крупные капитальные вложения, как в строительстве. Прежде всего, необходимы кадры, но и в этом направление в стране наблюдается безусловный рост. Российские разработки имеют достаточно большой потенциал, чтобы стать крупной и конкурентоспособной экспортной отраслью страны. При этом от государства нужны разумные меры поддержки экспортоориентированных производителей.

* * *

В таком случае, отделив зёрна от плевел и поддерживая не омологацию продуктов, а новые и интересные решения, мы сможем достойно представлять отечество на мировом рынке.

Александр ДОРОФЕЕВ
заместитель генерального директора по продажам АО «Эшелон Технологии», CISSP, CISA, CISM

Алексей ТИТОВ
руководитель направления развития продуктов АО «Эшелон Технологии», кандидат технических наук

САЛЮТ, КОМРАД!

КОРПОРАТИВНЫЕ КИБЕРУЧЕНИЯ КАК СПОСОБ ОПТИМАЛЬНО НАСТРОИТЬ SIEM-СИСТЕМУ

Хорошо настроенная SIEM-система позволяет организации своевременно обнаруживать инциденты информационной безопасности. Сбор и анализ тысяч событий, генерируемых каждую секунду различными элементами ИТ-инфраструктуры, осуществляется быстрым компьютером, а не человеком. Сердцем SIEM-системы, позволяющим автоматизировать анализ событий, является набор правил корреляции, который при каждом внедрении надо «подгонять» под конкретную ИТ-инфраструктуру. Правила можно настраивать на основе интуиции и опыта специалиста по внедрению, но лучше это делать на основе реальных сценариев инцидентов, которые можно сформировать, проведя учебные кибератаки на критичные ресурсы организации, наподобие того, как это делают военные в разных странах [1]. Рассмотрим международный опыт и его применимость к условиям организации.

МЕЖДУНАРОДНЫЕ КИБЕРУЧЕНИЯ

Наиболее масштабными и регулярными киберучениями являются Cyber Guard (U.S. Cyber Command), Crossed Swords, Locked Shields, Cyber Coalition (NATO Cooperative Cyber Defense Centre of Excellence), Cyber Europe (European Union Agency for Network and Information Security). В данных киберучениях участвуют представители государственных и силовых ведомств, а также гражданские специалисты. Киберучения позволяют отточить как навыки организации и взаимодействия, так и технические меры по отражению кибератак.

На примере киберучений Locked Shields 2013 рассмотрим основные моменты их организации. Организаторами учений была создана виртуальная инфраструктура, включающая порядка 400 узлов. Инфраструктура получила название Gamenet. Каждой команде защитников (Blue team) была выделена сеть из 34 машин, включающая маршрутизатор, межсетевые экраны, рабочие станции под управлением Linux и Windows, контроллеры доменов, файловые, почтовые, DNS и web-серверы, а также серверы СУБД.

Стоит отметить, что защищаемые системы были максимально приближены к реальности, и организаторы учений подготовили следующие моменты:

- на операционных системах отсутствовало всего несколько патчей, в основном уязвимым было прикладное программное обеспечение;
- заблаговременно были внедрены два бэкдора, которые в назначенное время начинали обращаться к управляющим серверам;
- в сети имелся подключённый уязвимый ноутбук специалиста подрядчика.

Также к каждой защищаемой инфраструктуре имел доступ представитель команды организаторов (White team), который выполнял роль «blonde», имитирующую любопытного пользователя, который переходит по всем ссылкам в получаемых электронных письмах и открывает все вложения.

Сердцем SIEM-системы, позволяющим автоматизировать анализ событий, является набор правил корреляции, который при каждом внедрении надо «подгонять» под конкретную ИТ-инфраструктуру

Нападающие (Red team) были вооружены полным знанием целевой ИТ-инфраструктуры, а также инструментами, используемыми в ходе кибератак: Kali Linux и Metasploitable [2]. Атакующие были разделены на группы по следующим специализациям: рабочие станции, Web и СУБД, сети и пр. Перед командой «красных» было поставлено 20 задач, которые поэтапно необходимо было выполнять по ходу проведения учений. Примеры задач: изменить содержимое важной Web-страницы, организовать отказ в обслуживании, получить административный доступ, внедрить вредоносный код, получить доступ к определённым письмам электронной почты, получить определённый отчёт, заменить файл с видеозаписью и др. Длительность активной фазы учений составила 3 дня.

Результаты каждой фазы учений, а также подробные рекомендации каждой из команд нашли подробное отражение в 122-страничном отчёте Cyber Defence Exercise Locked Shields 2013 After Action Report, который всё ещё доступен в интернете, в отличие от отчётов более поздних киберучений.

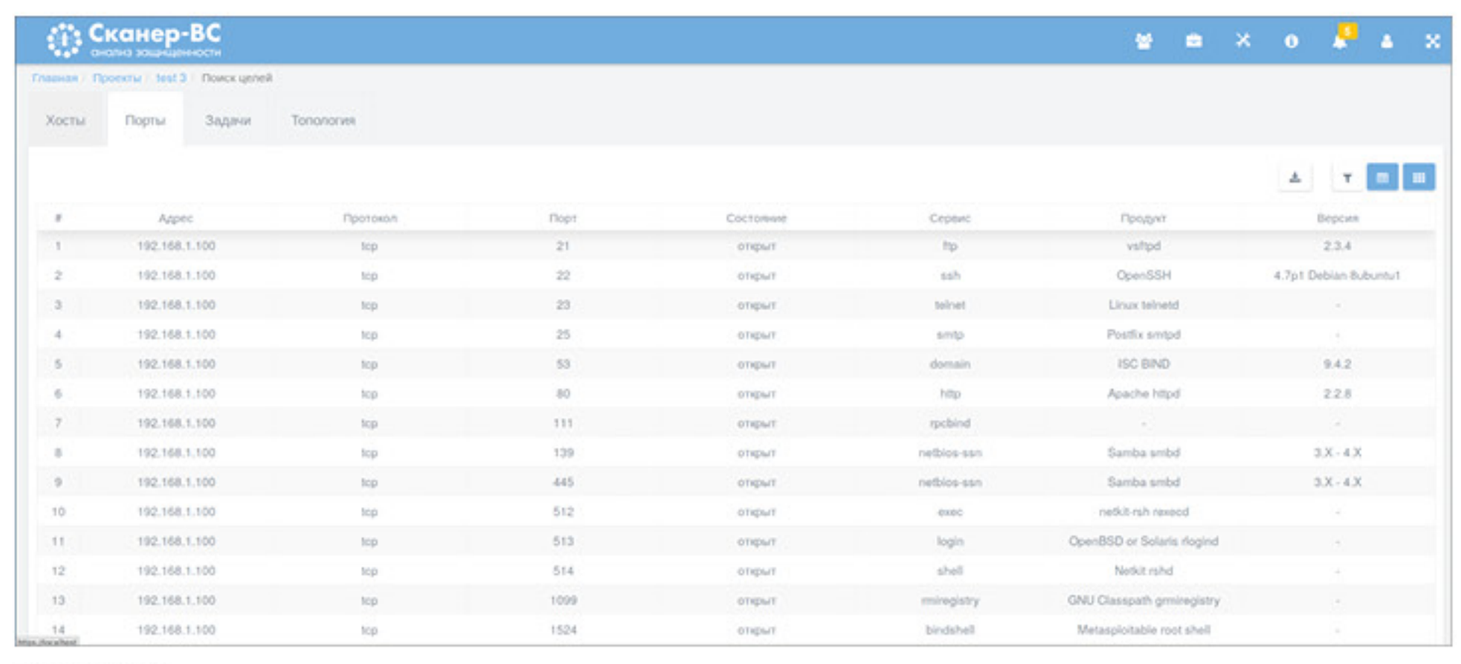


Рисунок 1

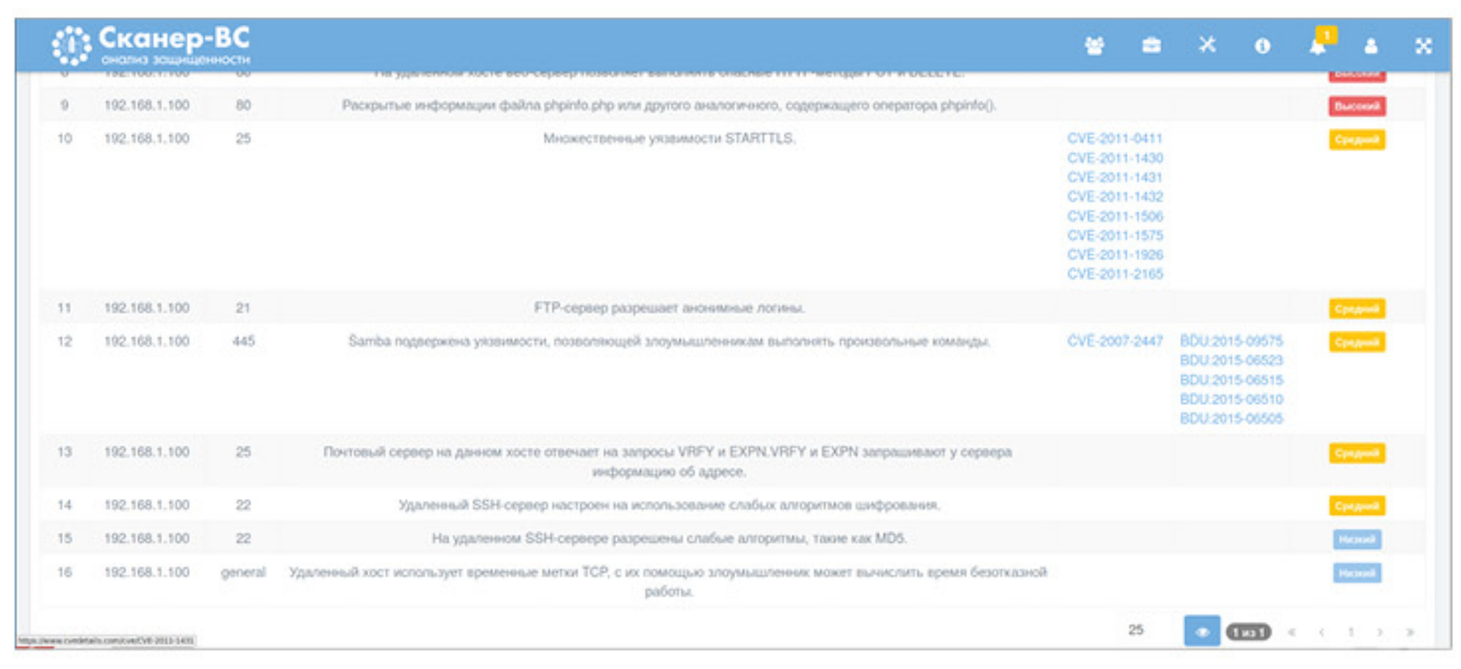


Рисунок 2

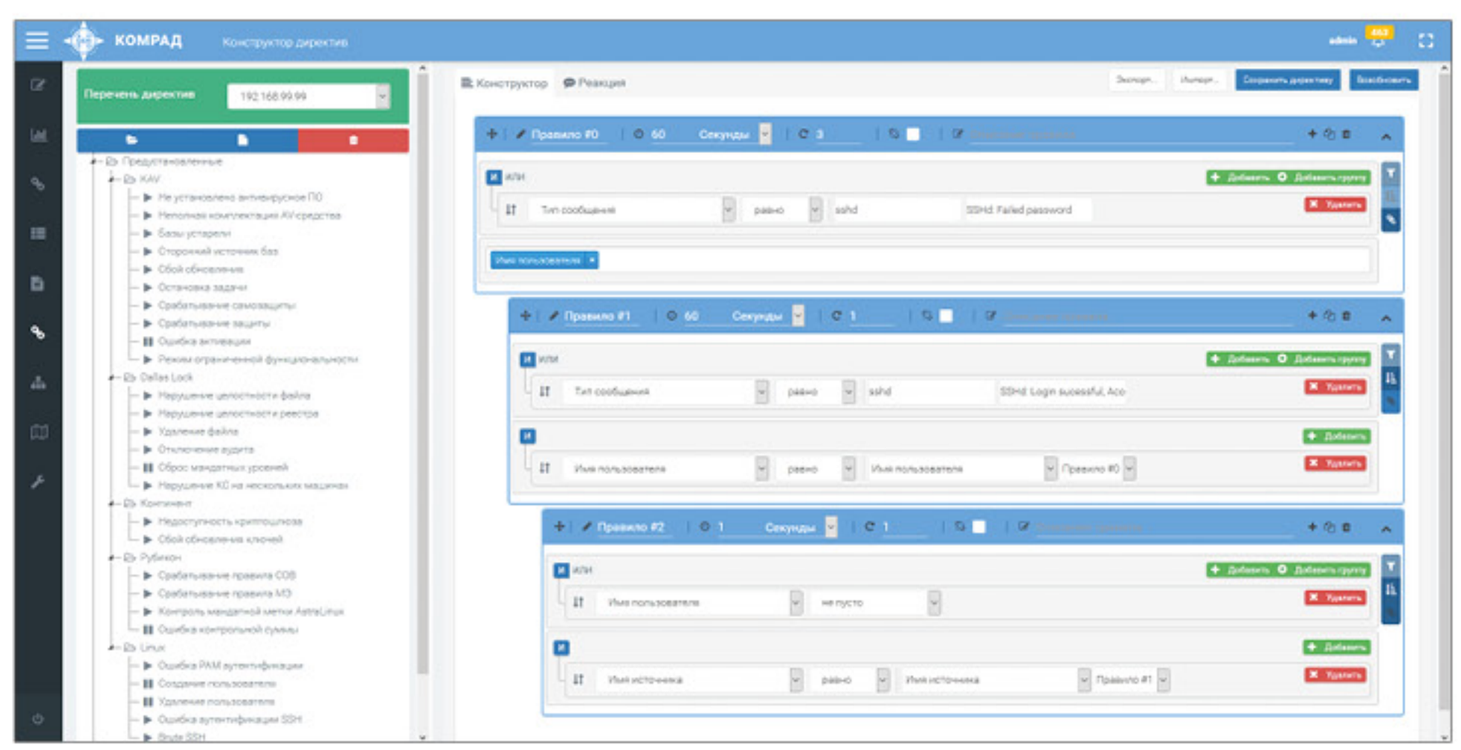


Рисунок 3

ПРЕДЛАГАЕМАЯ МЕТОДОЛОГИЯ

На наш взгляд подобный опыт можно переложить и на практику внедрения SIEM-систем, что мы и предлагаем нашим партнёрам, внедряющим заказчикам SIEM-систему КОМРАД, разрабатываемую группой компаний НПО «Эшелон» [3].

Основные этапы предлагаемого подхода:

- Обследование ИТ-инфраструктуры и выявление потенциальных целей для атак;
- Сканирование на наличие уязвимостей, формирование задач для команды атакующих и определение потенциальных сценариев проникновения;
- Первоначальное формирование правил корреляции;
- Проведение атак, тестирование правил корреляции, обучение специалистов группы реагирования на инциденты;
- Анализ проведённых атак и коррекция правил корреляции.

Разберём некоторые важные моменты. На первом этапе проводится инвентаризация узлов и сервисов, которые могут быть целями атак и источниками событий. Для этого удобно использовать комплекс анализа защищённости «Сканер-ВС» (рис. 1).

Получив текущий срез защищённости узлов (рис. 2), можно сформировать векторы кибератак. Например, обнаружив в DMZ настроенный по умолчанию сервер приложений Apache Tomcat, обращающийся к СУБД в локальной сети, можно сформировать сценарий, предусматривающий установку вредоносных веб-приложений для организации туннеля во внутренний сегмент и атаку на СУБД и другие серверы.

На этапе первоначального формирования правил корреляции включаются собственно правила «из коробки» и добавляются правила на основе предполагаемых векторов атак (рис. 3).

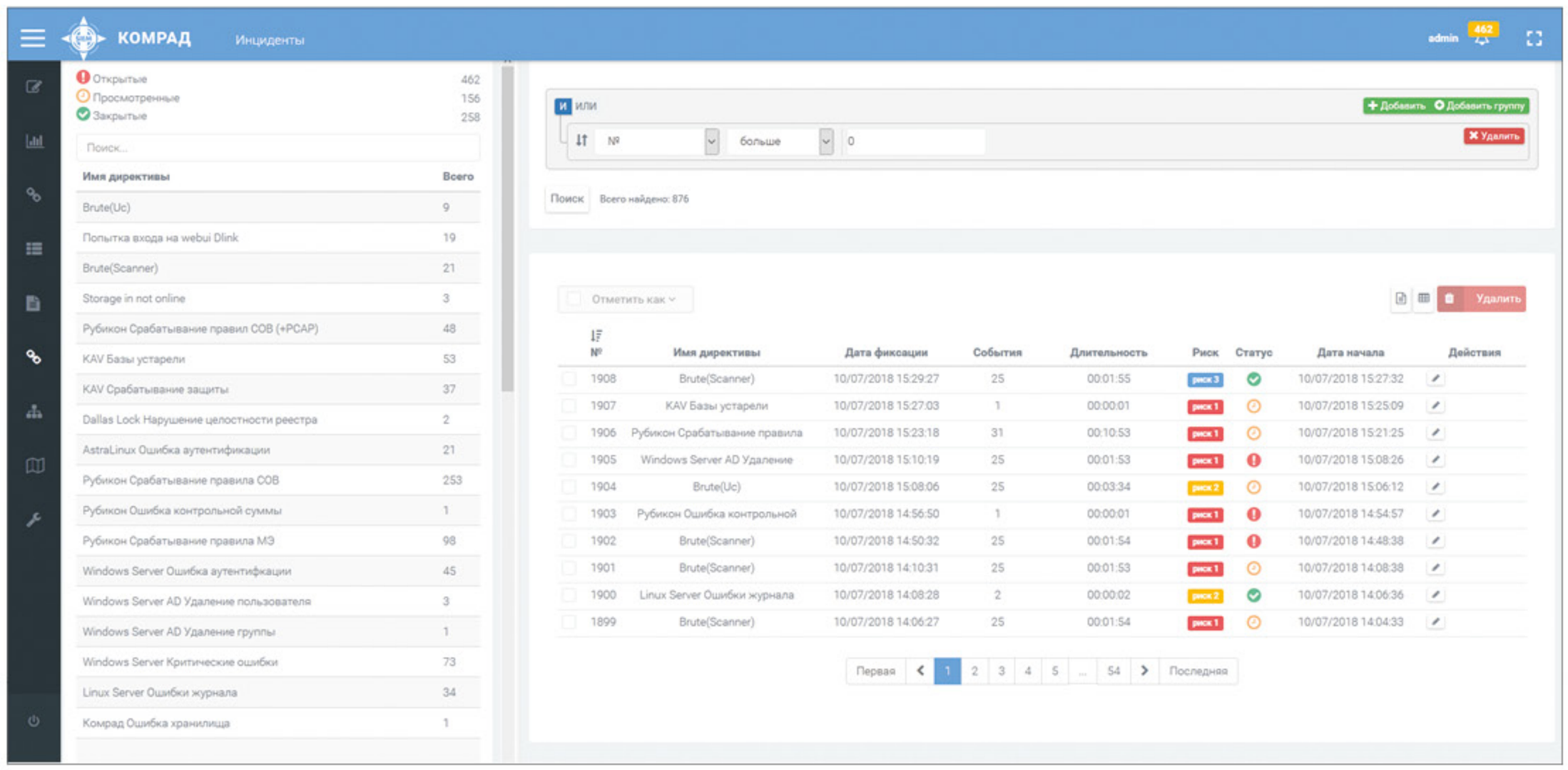


Рисунок 4

В примере с вектором атаки на внутреннюю сеть через сервер приложений SIEM-систему КОМРАД и соответствующие источники можно настроить так, чтобы фиксировались, как минимум, следующие события информационной безопасности:

- попытки подбора к серверу приложений;
- запуск веб-приложений;
- сканирование портов внутри сети;
- попытки подбора паролей к СУБД;
- запрос на выгрузку хешей паролей из системных таблиц СУБД.

Следующим этапом является проведение кибератак по выявленным векторам. В качестве инструмента может опять выступать комплекс анализа защищённости «Сканер-ВС», включающий множество утилит из арсенала этичного хакера. Проверяется срабатывание правил корреляции, а также на практике обучаются специалисты по реагированию на инциденты (рис. 4).

Как и в случае международных киберучений, на наш взгляд, имеет смысл моделировать ситуации наличия любопытных пользователей, а также наличие внутри сети установленного вредоносного ПО.

На заключительном этапе проводится анализ работы SIEM-системы и вносятся необходимые корректировки в правила корреляции.

* * *

Проведение киберучений на этапе внедрения SIEM-системы позволит настроить систему на выявление атак на ключевые узлы имеющейся ИТ-инфраструктуры, а также обучить пользователей системы — специалистов группы реагирования. В результате заказчик получит систему, которая, как минимум, адаптирована под его инфраструктуру и позволяет обнаруживать инциденты по самым распространённым векторам атак.

Конечно же, для поддержания системы в актуальном состоянии правила корреляции должны обновляться по результатам расследования реальных инцидентов, а также регулярных подобных киберучений. Совместное применение SIEM-системы и комплекса средств анализа защищённости обеспечит синергетический эффект в области обеспечения информационной безопасности корпоративной системы.

ЛИТЕРАТУРА

1. *Петренко А.А., Петренко С.А.* Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3 (11). С. 2–14.
2. *Дорофеев А.В.* Подготовка к CISSP: Телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4 (7). С. 69–74.
3. Устройство корреляции событий информационной безопасности / Марков А.С. и др. — патент на полезную модель RUS 166348 01.08.2016. 2016. МПК: G06F 21/55.

Олег ИВАНОВ
генеральный директор
ООО «ЦИБИТ»

Роман КОСИЧКИН
эксперт Департамента комплаенса в кредитно-финансовой сфере ООО «ЦИБИТ»

«БЕЗОПАСНОСТЬ КИИ — НЕ ТОЛЬКО ТЕХНИКА»

РАССКАЗЫВАЮТ ЭКСПЕРТЫ КОМПАНИИ «ЦИБИТ»

С 1 января 2018 года вступил в силу закон № 187 ФЗ «О безопасности критической информационной инфраструктуры». Еще находясь в проекте, этот закон породил много вопросов, касающихся реализации его требований. Теперь, когда эти требования вступили в силу, многие компании столкнулись с необходимостью их выполнения.

Что это за требования и как можно их выполнить? Какими компетенциями должен обладать персонал, строящий и эксплуатирующий системы? На эти и другие вопросы, некоторые из которых до сих пор остаются в «тени» технических решений, отвечают эксперты компании «ЦИБИТ» (Центр исследования безопасности информационных технологий).

— Для начала просьба напомнить, для чего потребовался этот закон и что такое КИИ?

— Новый закон предназначен для регулирования деятельности по обеспечению безопасности объектов информационной инфраструктуры Российской Федерации, функционирование которых критически важно для экономики государства. Такие объекты в законе называются объектами критической информационной инфраструктуры (КИИ). Согласно Закону, к объектам КИИ могут быть отнесены информационные системы и сети, а также автоматизированные системы управления, функционирующие в значимых для государства сферах, таких как, например, финансовый рынок, связь, энергетика.

Объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия между ними, составляют понятие критической информационной инфраструктуры (КИИ).

Организации или индивидуальные предприниматели в определенных отраслях промышленности, обеспечивающие взаимодействие объектов КИИ называются субъектами КИИ.

— Какие действия должны предпринять субъекты КИИ для выполнения Закона?

— Согласно закону, субъекты КИИ должны:

- провести категорирование объектов КИИ;
- обеспечить интеграцию (встраивание) в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА);
- принять организационные и технические меры по обеспечению безопасности объектов КИИ.

— Как протекает процесс категорирования и передачи данных?

— Категорирование объекта КИИ предполагает определение его категории значимости на основе ряда критериев и показателей. Всего устанавливается три категории. Если объект КИИ не соответствует ни одному из установленных критериев, ему не присваивается ни одна категория. Те объекты КИИ, которым была присвоена одна из категорий, называются в законе значимыми объектами КИИ.

По завершению категорирования сведения о его результатах должны направляться субъектом КИИ во ФСТЭК России для ведения реестра значимых объектов КИИ.

Важно отметить, что если в процессе категорирования было определено отсутствие категории значимости у объекта КИИ, результаты категорирования все равно должны быть представлены во ФСТЭК России.

Сам процесс категорирования протекает в три этапа:

- Первый этап. Необходимо создать внутреннюю комиссию по категорированию, включающую наиболее компетентных специалистов по бизнес-процессам, поскольку только «владелец» знает все тонкости бизнес-процесса, которые могут привести к его нарушению и последующим негативным последствиям.

◆ Второй этап. На этом этапе проводится предпроектное обследование и, на основании полученных данных, комиссия принимает решение о наличии перечня объектов КИИ, подлежащих категорированию и присваивает категорию значимости исходя из показателей критериев значимости (социальная, политическая, экономическая, экологическая, значимость для обеспечения обороны страны, безопасности государства и правопорядка).

Результатом второго этапа является «Акт категорирования объекта КИИ», который утверждается руководителем субъекта КИИ. Акт должен содержать полные сведения об объекте КИИ. Субъект КИИ направляет сведения о результатах категорирования в ФСТЭК России, которая проверяет соблюдение порядка и правильности категорирования и вносит сведения в реестр значимых объектов КИИ.

◆ Третий этап. Планомерное выполнение требований по обеспечению безопасности значимых объектов КИИ, включающее разработку ТЗ, модели угроз ИБ, рабочей документации, а также испытания и ввод системы безопасности в действие.

— Что важно при создании систем информационной безопасности для КИИ? На что обращать внимание?

— Система безопасности значимого объекта КИИ представляет собой комплекс организационных и технических мер. Порядок создания системы и требования к принимаемым мерам безопасности определяется ФСТЭК России рядом приказов [1], [2].

Уже довольно много говорилось о технических мерах защиты. Мы же хотели более подробно поговорить об организационных мерах.

Как мы упоминали ранее, одним из пунктов плана мероприятий по обеспечению безопасности значимых объектов КИИ является разработка документации. В рамках данного процесса необходимо создать или модифицировать те нормативные документы организации, в которых бы определялись и излагались процессы обеспечения системы защиты КИИ.

Исходя из текста закона и подзаконных актов, можно составить примерный список данных документов.

Для владельцев значимых объектов КИИ перечень таких документов весьма обширен. Помимо приказов и положений, связанных с категорированием объектов, необходимо согласно [1] и [2] подготовить документы, связанные с:

◆ Проектированием систем безопасности значимых объектов;

◆ Испытаниями и приемом в эксплуатацию систем безопасности;

◆ Контролем за состоянием значимых объектов.

Кроме этого, придется внести ряд изменений в существующие документы по обнаружению и предотвращению вторжений, антивирусной защите, управлению доступом, использованию материальных носителей информацией.

Всего, в случае эксплуатации значимых объектов КИИ, необходимо разработать и изменить несколько десятков организационно-распорядительных документов.

Следует также отметить, что большинство из этих документов являются политиками (т.е. нормативными документами достаточно высокого уровня). Не исключено, что субъекту придется разрабатывать и внедрять документы, конкретизирующие данные политики (процедуры и инструкции).

— Поговорим о владельцах незначимых объектов КИИ. Разве они должны готовить какие-то документы, ведь пункт плана к ним не относится?

— Да, большинство документов, упомянутых нами ранее, для них не требуются. При этом, комиссия по категорированию все равно создается, следовательно, необходимы, как минимум приказ о создании комиссии и документ, определяющий порядок ее деятельности. В ходе своей работы комиссия должна определять критические процессы и объекты, которые обрабатывают критические процессы, разработать модель угроз. По результатам работы комиссии создается перечень объектов КИИ и по всем объектам оформляется акт о категорировании.

Таким образом, даже субъект КИИ, обладающий только незначимыми объектами, должен разработать или модифицировать порядка десяти документов.

— Да, это трудная задача. Справиться с ней могут только подготовленные специалисты. Есть ли в законодательстве требования к кадровому составу субъектов КИИ?

— Согласно приказу ФСТЭК [1] в подразделении организации, ответственном за защиту значимых объектов КИИ, должны работать специалисты по безопасности. Исходя из контекста задач, решаемых ими, данные специалисты обязаны быть компетентны в области ИБ и обладать всеми знаниями и умениями, требующимися от специальности «Информационная безопасность».

— Но ведь с объектами КИИ взаимодействуют не только специалисты по информационной безопасности. Работники, которые участвуют в критических процессах, тоже должны понимать их значимость с точки зрения защиты. Чему и как их надо обучать?

— В вышеупомянутом приказе ФСТЭК явно указывается, что работники субъекта КИИ должны быть обучены правилам безопасности в соответствие с принятыми в организации организационно-распорядительными документами. Не реже одного раза в год следует также проводить организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности КИИ и о возможных угрозах безопасности информации.

— Получается, что процесс категорирования, построения систем

Всего, в случае эксплуатации значимых объектов КИИ, необходимо разработать и изменить несколько десятков организационно-распорядительных документов

защиты и обмена данными весьма трудоемкий и требует высокой квалификации исполнителей. Что же делать, если у предприятия нет опыта построения требуемых систем безопасности?

— Понятно, что не все организации обладают необходимыми ресурсами для создания систем защиты. Например, все банки являются субъектами КИИ. Согласно статье 10 Приказа ФСТЭК [1], руководитель субъекта КИИ создает подразделение или назначает ответственных за обеспечение безопасности значимых объектов КИИ. Как мы уже отмечали, с очень большой долей вероятности это будут сотрудники ИБ. При этом людских ресурсов, ответственных за информационную безопасность, практически всегда недостаточно. Эти сотрудники выполняют массу профильных задач. В их числе — работа с ключевой инфраструктурой, настройка и обслуживание СКЗИ и программного обеспечения по ИБ, организация безопасной разработки, написание нормативной документации, обучение персонала. Очевидно, что при такой большой нагрузке вероятность допустить ошибку или упустить важный момент существенно возрастает. Однако, из данной ситуации есть выход. Тот же Приказ разрешает сторонним организациям, обладающим лицензиями ФСТЭК, осуществлять деятельность по защите значимых объектов КИИ.

«11. Для выполнения функций, предусмотренных пунктом 10 настоящих Требований, субъектами критической информационной инфраструктуры могут привлекаться организации, имеющие в зависимости от информации, обрабатываемой значимым объектом критической информационной инфраструктуры, лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации (далее — лицензии в области защиты информации)».

Согласно статье 10 Приказа ФСТЭК, руководитель субъекта КИИ создает подразделение или назначает ответственных за обеспечение безопасности значимых объектов КИИ. Как мы уже отмечали, с очень большой долей вероятности это будут сотрудники ИБ

Следует при этом отметить, что ответственность за обеспечение безопасности все равно остается на работниках самого субъекта КИИ.

«К силам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся:

- подразделения (работники) субъекта критической информационной инфраструктуры, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры»

— Спасибо! Мы поняли, что помимо технических средства для выполнения требований закона о безопасности КИИ очень большую роль играет работа с организационно-распорядительной документацией, грамотный подбор кадров, обучение работников субъекта КИИ. Скажите, как компания ЦИБИТ может содействовать организациям — субъектам КИИ в решении этой нелегкой задачи?

— Прежде всего, хотим добавить, что даже наличие опытных кадров и обученных работников не исключает помощь лицензированных сторонних организаций при организации системы безопасности значимых объектов КИИ.

Компания «ЦИБИТ» обладает уникальными компетенциями в данных областях.

Имея собственное кадровое агентство, специализирующееся на подборе и трудоустройстве сотрудников в области ИБ, мы всегда готовы предложить организациям нужные кадры с требуемым опытом работы и квалификацией.

Если необходимо, можно обучить работников субъекта КИИ, используя ресурсы учебного центра «ЦИБИТ». Кроме того, учебный центр может содействовать в регулярном повышении осведомленности работников организации по вопросам ИБ.

Наконец, подразделение финансового комплаенса ЦИБИТ всегда готово «подставить плечо», если есть необходимость помочь субъекту КИИ в организации защиты, подготовке системы организационно-распорядительных документов, в проведении проверки соответствия.

— Спасибо.

ЛИТЕРАТУРА

1. Федеральная служба по техническому и экспортному контролю. Приказ от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
2. Федеральная служба по техническому и экспортному контролю. Приказ от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

ТОЛЬКО НАЛИЧНЫЕ!

IV МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ «АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ НДО»

В Ярославле при официальной поддержке Банка России состоялась IV Международная конференция «Актуальные вопросы развития наличного денежного обращения». Участниками мероприятия стали более 200 руководителей и ведущих специалистов в сфере наличного денежного обращения (НДО) из России, стран СНГ, Европы и Азии.

Организатором конференции выступила Ассоциация организаций в сфере наличного денежного обращения, инкассации и перевозки ценностей (АНДО). Генеральные партнёры мероприятия: объединение «РОСИНКАС», компании «Гизеке & Девриент — ЛОМО» и GLORY. Организационная поддержка — Медиа Группа «Авангард».

В работе конференции приняли участие представители Государственной думы, МВД России, крупнейших российских банков, национальных банков и служб инкассации стран СНГ, перевозчиков денежных средств и ценностей, производителей бронированных автомобилей для инкассации, счетно-сортировальной техники и другого оборудования.

Тон конференции задало выступление первого заместителя председателя Банка России Ольги Скоробогатовой. Она рассказала, что при значительном росте числа безналичных операций в розничном товарообороте России (38%), рост числа наличных операций также растет (8%), и сбрасывать старый-добрый НДО на свалку истории никто не собирается. Более того, сфера НДО имеет прогрессивные программы и совершенствуется заметными темпами. Основные направления развития — это диджитализация (внедрение электронного документооборота при совершении операций с наличными); внедрение новой модели кассового обслуживания; мобильное приложение «Банкноты Банка России» (содержит информацию о находящихся в обращении банкнотах); выпуск новых номиналов банкнот и памятных монет; борьба с фальшивомонетничеством.

В обширную деловую программу конференции вошли тематические заседания и дискуссии на следующие темы:

- Наличное и безналичное денежное обращение — единство противоположностей. Повышение доступности, качества и ассортимента финансовых услуг;

Выступление первого заместителя председателя Банка России Ольги Скоробогатовой

Пленарная дискуссия «Наличное и безналичное денежное обращение — единство противоположностей»

- Повышение эффективности в сфере НДО;
- Обеспечение безопасности процессов НДО. Тротуарный риск;
- Инновационные технологии в организации процессов НДО и расчетов;
- Потребности Ритейла в качественном обслуживании в сфере НДО;
- Оптимизация перевозки наличных денег и страхование рисков. Модели инкассации будущего.

Особое внимание привлекла пленарная дискуссия «Наличное и безналичное денежное обращение — единство противоположностей. Повышение доступности, качества и ассортимента финансовых услуг». Модератор дискуссии директор Департамента национальной платежной системы Банка России Алла Бакина сообщила, что по остатку наличных денег в обращении по отношению к ВВП Россия занимает девятое место в мире. Впереди только Швеция, Беларусь, Бразилия, Великобритания, Мексика, США и Китай. В своём выступлении председатель правления ассоциации «НДО», президент-председатель правления объединения «РОСИНКАС» Олег Крылов сделал акцент на том, что сегодня в мире более 2 млрд человек не имеют доступа к банковским услугам, и наличные деньги по-прежнему являются наиболее простым и надежным средством платежей, не требующим специальной инфраструктуры. Вице-президент Банка ВТБ Валерий Чулков, генеральный директор «Гизеке & Девриент — ЛОМО» Ральф Литцке и генеральный менеджер GLORY LTD Ооно Масаюки предложили свои сценарии развития НДО в мире и России.

Руководитель департамента компании «Гизеке & Девриент — ЛОМО» Наталья Ракова рассказала о революции в области решений для кассовых центров, а сотрудники компании GLORY RUS Сергей Кикоть и Ольга Бубнова — о курсе инноваций от Glory, ориентированном на повышение эффективности бизнеса. Директор департамента компании «ГАММА-ЦЕНТР» Дмитрий Муляр сделал квалифицированный обзор передовых решений от мировых лидеров в области приема, хранения, пересчета и инкассации наличности.

Руководитель управления продаж Московского региона «ДИИП 2000» Олег Королев рассказал о современных тенденциях и трендах в налично-денежном обращении. Начальник управления инкассации ЦУНДО Сбербанка Андрей Новиков поделился опытом освоения подразделениями инкассации самых современных технологий. Исполнительный директор Управления продуктов наличного денежного обращения Банка ГПБ Сергей Кулик со своей стороны поведал об опыте внедрения онлайн-инкассации. Президент компании Profindustry Сергей Барсуков провел анализ рынка НДО и сделал ряд предложений по повышению его эффективности.

* * *

На протяжении всех дней конференции работала выставка, на которой демонстрировались образцы современных бронированных автомобилей для инкассации, счётно-сортировальной техники и другого оборудования. На стендах участники получали все необходимые сведения, строили планы сотрудничества и изучали оборудование в действии.

Марк НОВОДАЧНЫЙ
корреспондент BIS Journal

ЦОД-2018

ОТКРЫТИЕ ЦИФРОВЫХ СЕЗОНОВ 2018–2019 НАЧАЛОСЬ С КИИ, БИЗНЕСА И ОБЛАКОВ

«Выбор ЦОД — это так же ответственно, как и выбор спутника жизни. Смена ЦОД — развод и женитьба одновременно: потеря времени и денег неизбежна». Таких откровений на 13-й международной конференции ЦОД-2018 прозвучало немало. Форум оказался полезным как для начинающих, так и для состоявшихся пользователей, таких как Банк ВТБ, имеющий 9(!) собственных ЦОД-площадок, и Ростелеком, предлагающий ЦОД-ресурсы преимущественно госструктурам. Актуальные идеи и предложения были представлены на пленарном заседании и четырех секциях и обсуждены в ходе трех дискуссий: «Как обеспечить безопасность ЦОДа?», «Критерии выбора кЦОДа», «Цифровая экономика (трансформация) и ЦОДы».

ПРОСТО БИЗНЕС

кЦОД — это коммерческий ЦОД. Нынешнее руководство страны мыслит интересами бизнеса, и желание способствовать развитию кЦОДов явно просматривается в программе «Цифровая экономика РФ». Устроители форума предоставили потенциальным потребителям отличную возможность ознакомиться с предложениями в области кЦОД, а также с проблемами, с ними связанными.

Тут полезными оказались не только плановые мероприятия. На каждом из сорока выставочных стендов работали по-настоящему компетентные сотрудники компаний. Секционные заседания позволили собрать ценный технический опыт развёртывания ЦОД и получить рекомендации по поддержке бизнеса. Ряд выступлений был основан на независимой аналитике организаторов мероприятия — ИКС–Медиа и ИКС-Консалтинг, чьи эксперты погружены в тему больше десяти лет.

ПЕРВЫМ ДЕЛОМ БЕЗОПАСНОСТЬ

Как стало понятно из выступлений, специалистов уже немного «достали» маркетинговые спекуляции на темы цифровой экономики. «Хоть горшком назови…», — говорит народная мудрость, только давайте поскорее перейдём к делам! А среди важнейших — постановка безопасности во главу угла «хошь экономики, хошь трансформации».

Часто время на целевых форумах тратится на обмусоливание киберпреступности в виде фельетонных хакеров и «человеческого фактора», сующего какие попало флешки в корпоративные USB-порты. Однако специалистам понятно, что при широкомасштабном внедрении «цифры» имеет смысл обсуждать только КОМПЛЕКСНЫЕ проблемы безопасности.

Иная грань — безопасность и эффективность бизнеса. Некоторые считают: чем бороться с кибербедой, которая всё равно придёт, проще застраховать потенциальные риски. А развитие Больших Данных и ЦОДов поставить в зависимость от недобросовестности поставщиков и прочих ясных для бизнеса проблем. В такой тональности, что удивительно, оказались выдержаны рассуждения представителя организации, входящей в контур Росатома. Похоже, именно в этой ситуации РЕГУЛЯТОР в сфере безопасности должен оказаться тем лекарем, который подкорректирует игривый характер подобного хода мыслей. Хотя бы для того, чтобы поставить цифровой заслон трагедиям, подобным крымскому Армянску.

ОБЛАКО В ДЛИННЫХ ШТАНАХ

Кроме определений «коммерческий» и «безопасный» большой популярностью пользовалось и прилагательное «облачный». Облачные технологии, которые на первом этапе своего развития были средством экономии расходов на базовые ИТ-компоненты для штатных приложений, услуги SaaS и IaaS (ПО как сервис и инфраструктура как сервис), сегодня позволяют сократить затраты на разработку нового прикладного ПО (услуга PaaS, платформа как сервис), упростить создание безопасных ЦОД-решений — на базе гибридных «облаков». В последнем варианте наиболее критичные вопросы ИТ-поддержки решаются «облаком» в корпоративном ЦОД, а менее ответственные задачи переносятся в коммерческие ЦОДы.

Уместно отметить приведённые цифры: даже в западных странах коммерческими являются не более 20% ресурсов ЦОД, остальные — это ЦОД корпоративные. В России доля коммерческих ЦОД — на уровне 10%. И дело не только в посконности и домотканности отечественного консерватизма. На дискуссии «Критерии выбора кЦОДа» приводился пример, когда в ходе первичного отбора кЦОДа на основе 10 требований из 200 кандидатов осталось только 7. В связи с этим можно предположить, что роль регулятора велика не только в обеспечении безопасности, но и в формировании рынка. Что, в свою очередь, повышает актуальность подъёма уровня образования и повышения квалификации кадров для системы технического и правового регулирования рынка ЦОД.

* * *

13-я международная конференция ЦОД очертила круг задач, актуальных для участников рынка. Чем ответит актуализированная программа «Цифровая экономика РФ» и бюджет?

Николай КОЛЬСКИЙ
обозреватель BIS Journal

ДИСТАНЦИОННЫЙ БАНКИНГ 2018

ДБО И ЦИФРОВАЯ ТРАНСФОРМАЦИЯ НА ПРАКТИКЕ

IX Международный Форум «Дистанционный банкинг 2018. Цифровая трансформация на практике» состоялся в конце сентября в конференц-залах отеля Marriott Grand Hotel Moscow. На нём в полной мере проявилось понимание весьма серьёзных обстоятельств. Например, что без отказоустойчивых приложений и быстрых каналов коммуникаций, отвечающих требованиям кибербезопасности, предложения для ДБО спросом подкрепить не удастся.

Отдав дань докладам Банка России и Московской биржи по модной теме маркетплейсов, форум представил далее взгляды и подходы ведущих финансовых организаций к созданию платформ для цифрового банкинга.

ИМПОРТОЗАМЕЩЕНИЕ ПО-ВЗРОСЛОМУ

Слово «импортозамещение» звучало нечасто, однако дух этого явления пронизывал выступления. Накопление и консолидация собственных компетенций и отказ от тотального аутсорсинга ИТ-разработок для «повышения» эффективности — вот приятные впечатления от выступлений Анны Михиной (Тинькофф Банк), Германа Хохлова (Банк ВТБ), Алексея Бородкина (Росбанк). Узловые моменты их докладов: собственные коллективы разработчиков, подкрепление внутренних ИТ-команд экспертными знаниями отечественных партнёров, тщательное документирование и тестирование модулей платформ. В то же время учтён и активно используется и мировой опыт: современные языки программирования, технология контейнеров, подход DevOps… Результат: ПО названных банков не зависит от политических капризов.

В качестве отечественных партнёров для создания платформ цифрового банкинга и ДБО на форуме были представлены компания ФальконФинанс (доклад «MarketPlace. Финансовые продукты в одном окне. Решение ФальконФинанс») и iSimpleLab (доклад «Цифровой банкинг в портале»).

Инновационной «вишенкой на торте» стала технология биометрической идентификации для цифрового банкинга. Технология неоднозначно оценивается участниками рынка. Тем не менее, команда Тинькофф Банк, которая «не внедряет инновации ради инноваций», завершает работу по выпуску соответствующего модуля. Почта Банк уже внедрил биометрическую идентификацию в более чем сотне отделений. Ростелеком несгибаемо уверен в надёжности и безопасности ЕБС, и этот оптимизм разделяет Почта Банк. Как говорится, будем поглядеть.

О. БЕНДЕРУ И НЕ СНИЛОСЬ!

Устроители форума мудро отложили сессию «Безопасность цифрового банкинга и дистанционных каналов» на финал. Потому что, без преувеличения, после доклада Алексея Голенищева (Альфа-Банк) «Социальная инженерия как один из основных трендов «дистанционного» мошенничества. Меры противодействия» в первый момент возникает мысль о необходимости срочно запретить дистанционные операции с деньгами. Число представленных докладчиком вариантов сравнительно честного отъёма средств у населения через ПК и смартфоны уверенно приближается к цифре 400. Присутствующие в зале, конечно же, не поведутся на большинство из представленных уловок. Но люди с улицы! Смогут ли они выделить нюансы текста в адресной строке? Или устоять от соблазна мгновенно, в один клик получить деньги, которые государство «уже перевело» на их фамилии в страховые организации?

А ведь массовому пользователю ДБО угрожают не только «социальные инженеры». Павел Крылов из Group-IB рассказал о свежих кейсах отъёма денег с помощью вирусов. И в выгодном свете представил труд своей компании по выявлению и уничтожению вирусов-клептоманов. Но вот незадача: в ходе последовавшей за этим дискуссии не удалось выявить и описать хотя бы некоторые из органичных недостатков программно-аппаратных платформ, допускающих автоматическую установку зловредов на компьютеры и смартфоны. А ведь бороться надо не с симптомами, а с болезнью!

ЗДРАВСТВУЙ, ГРУСТЬ!

Форум, как обещалось, отличала «продуктивная дискуссионная часть». Но, к сожалению, к финалу ключевые участники дискуссии уже отсутствовали.

Оставшиеся в зале вспоминали «галочки», которые пользователь добровольно проставляет в своём (B)YOD. Но разве пользователю доступна ИСЧЕРПЫВАЮЩАЯ информация об угрозах проставления этих галочек? Давно известны технологии, позволяющие изолировать в смартфонах секретную информацию от бытовой. И тут же вопрос: «А Вы готовы платить за такой смартфон?» Готов, но сколько он будет стоить? А сколько он будет стоить, если интегрировать в него не все функции, нужные, например, военным? А может, следует задуматься о спецсегменте Интернета для ДБО? И т.д. и т.п.

* * *

Вопросов, связанных с кибербезопасностью ДБО, много. Некоторые из них могут быть наивными. Но благодаря форуму стало понятно, что и решение «решаемых вопросов» просто откладывается на потом. А жаль!

Корней РЕУТ
корреспондент BIS Journal

BIS SUMMIT 2018

ОТ НОВЫХ СЛОВ К НОВЫМ ДЕЛАМ?

В сентябре состоялся Business Information Security Summit или в просторечии BISS 2018. В атмосфере праздника, созданной щедрыми организаторами, был продолжен сеанс разоблачения магии цифровой экономики (ЦЭ), начатый на Петербургском цифровом форуме в апреле, а также представлены многоплановые взгляды на тему безопасности сквозь призму представлений об ИТ-культуре. Культуре технологической, правовой и общечеловеческой.

Год назад российский вице-премьер упомянул о поражении вирусом «цифровой экономики» верхов отечественной власти. На ПМЭФ-2018 слухи о такой локальной эпидемии опровергли, увязав российскую цифровизацию с общей мировой «беременностью» этими процессами. В то же время, как показал блиц-опрос Русской Службы BBC, единого понимания в бизнес- и политической элите того, что такое «цифровая экономика» нет. Опытные гибкие респонденты говорили о ней крайне обтекаемо: «то, что связано с цифрой», «есть такая программа», а сам Греф (!) предпочёл попросту уклониться от ответа.

ПОГРУЖЕНИЕ В ГЛУБИНУ

Такая ситуация в верхах только подчёркивает обоснованность и актуальность инициатив Н. И. Касперской по конкретизации первоочерёдных задач ЦЭ. Эти инициативы президента ГК InfoWatch уместно сравнить с айсбергом, верхушка которого была представлена на Петербургском цифровом форуме. На BISS 2018 представление было продолжено вглубь. Возможно, несколько смело сравнивать неформального лидера BISS 2018 с Воландом, а участников первой панельной дискуссии — с его товарищами, но ассоциации напрашиваются.

Тема этой дискуссии была заявлена как «ИБ между Востоком и Западом». Однако, как показало развитие событий, перевод приведенного названия с маркетингового на понятный мог бы звучать как «Возможные подходы к восстановлению и развитию экономики России на инновационных основах в условиях роста противоречий между лидерами, группировками и культурами».

ЭКОНОМИКА БЕЗ ХАЙПА

Особую ценность дискуссии придало участие декана экономического факультета МГУ им. М.В. Ломоносова А.А. Ау-

Декан экономического факультета МГУ им. М.В. Ломоносова А.А. Аузан

зана. Используя понятия «транзакционные расходы» и «сетевые структуры», он представил свой взгляд на «цифровую» экономику и доходчиво разъяснил, почему эффективность ЦЭ запредельно высока для Uber и минимальна для Ростеха.

Его рассуждения и аргументы, кстати, хорошо согласуются с рядом оценок вклада ЦЭ в экономику развитых стран (всего единицы процентов). И с интервью главы Ростеха, озвучившим доли «цифровой экономики» в мировом ВВП, а также в ВВП развивающихся стран и России (5,5%, 4,9% и 2,8% соответственно. Сравнительно немного, если не сказать, мало).

Не отрицая важности этого (ЦЭ) явления, А.А. Аузан совсем не тревожится, что Россия опаздывает вскочить на подножку какого-то уходящего поезда. По его мнению, сегодня важнее сосредоточиться на стратегии выбора партнёров в противовес сиюминутным тактически «пользам» (Китай далеко, и он чужой, а Европа — своя, родная и рядом. Сиюминутные противоречия не должны перечеркнуть долгосрочную перспективу).

Уместно упомянуть также, что декан экономического факультета МГУ, член Экономического совета при Президенте РФ довольно откровенно заметил, что основополагающий закон рынка «Спрос определяет предложение» сегодня извращен, и предложение агрессивно пытается (часто небезуспешно) формировать спрос в своих интересах. По его словам, часть хайпа вокруг ЦЭ — явление того же порядка.

РАСШИРЕНИЕ ИБ-СОЗНАНИЯ

В целом Аузан — это новый камертон, прозвучавший на Business Information Security Summit. Новый, но не единственный новый.

В этом году произошли принципиальные изменения в атмосфере форума. Нишевые цели, задачи и интересы ИБ стали рассматриваться сквозь призму интересов страны и её народа. И это, похоже, сознательный выбор устроителей, предложивших в качестве «инфографики» BISS 2018 слово «конвергенция».

«Конвергенция ИБ-культуры»; «Конвергенция последней линии защиты или единственно нужная защита»; «Конвергенция Compliance, или можно ли забыть про регуляторов и начать жить бизнесом?» — вот темы ещё трёх панельных дискуссий форума.

ПЛЮС КУЛЬТУРА

Годом ранее в этом же зале было предложено рассматривать и внедрять безопасность как иммунную систему ИТ в противовес понятиям «заплатка», «щит» и следующим из них подходам. В этом году понимание ИБ было расширено представлениями о безопасности как о культуре.

Движение в этом направлении видится двусторонним: в людях необходимо развивать культуру безопасного поведения в цифровом обществе (в быту, на работе, при взаимодействии с государством), а цифровая безопасность должна уважать человека. «Как живётся пользователю в безопасной корпоративной среде: смириться или обойти?» (Алексей Белоглазов); «ИБ-перевёртыш, или Влияние культуры на ИБ» (Алексей Лукацкий); «Влияние ИБ на финансовую культуру России» (Артём Сычёв) — темы докладов, как и имена докладчиков, говорят сами за себя.

ФЕДОТ (ТЗ) — ДА НЕ ТОТ

Панельная дискуссия «Конвергенция последней линии защиты или единственно нужная защита» плотно «оседлала» тему перехода от ИБ на основе искусственной интеграции к ИБ как встроенной функции. Поучительную информацию и вопросы для обдумывания представил доклад «Практика обнаружения атак, использующих легальные инструменты» (Сергей Солдатов, «Лаборатория Касперского»). Это выступление, а также доклад «Опыт создания прототипа системы обеспечения безопасности бизнес-процессов» (Вадим Агиевич, Сургутнефтегаз) продемонстрировали важность проблемы несоответствия бизнес-логики, заложенной в ИТ-инфраструктуру, реальному течению бизнеса. Часто реальный бизнес-процесс заметно отличается от представлений руководства, переданных ИТ-разработчикам в качестве ТЗ.

На пленарной дискуссии «ИБ между Востоком и Западом»

На малой сцене во время перерыва рассказывают о новых продуктах и технологиях

НЕДОКОРМ В КОМПЛАЕНС

Последней по времени в очереди «панелей», но не последней по важности оказалась «Конвергенция Compliance, или можно ли забыть про регуляторов и начать жить бизнесом?» Её модератор Михаил Емельянников подготовил констатирующий тревожные тенденции доклад «Комплаенс как средство ограничения конкуренции и заградительный барьер». Далее без перерывов на вопросы-обсуждения выступили и другие: «Управление ИБ-рисками vs Управление требованиями» (Мария Воронова, InfoWatch); «Контроль действий пользователей в информационной среде компании: моральные, юридические и технические аспекты» (Дмитрий Кандыбович, StaffCop); «Обеспечение комплексности нормативно-технического и нормативно-правового регулирования как основа развития безопасного IIoT. Роль отраслевых экспертных объединений» (Владимир Карантаев, Ростелеком-Solar).

Благодаря этим докладам последующая дискуссия о противоречиях между строителями ЦЭ и регуляторами имела прочный фундамент. Получилось, что обильно представленные противоречия — результат финансового недокорма работ в сфере соответствия островков ЦЭ тому, что называют нынче «комплаенс».

* * *

В приветственном/вступительном «слове» форуму Рустэма Хайретдинова, президента ассоциации BISA, отмечалось, что «за 11 лет существования BIS Summit выросло целое поколение специалистов ИБ. ...Ведь это мы стали оцифрованными, они пришли на наш рынок цифровыми!»

Анализируя этот тезис и все, что происходило на форуме, можно утверждать, что на «наш рынок» пришло не только думающее, квалифицированное, но и ответственное «цифровое поколение». В отличие от предыдущего оно теперь понимает необходимость конвергенции слова (регулятора) и дела (ИТ&ИБ).

ИНИЦИАТИВА АРПП «ОТЕЧЕСТВЕННЫЙ СОФТ»

В рамках BIS Summit 2018 председатель правления Ассоциации разработчиков программных продуктов (АРПП) «Отечественный софт», президент ГК InfoWatch Наталья Касперская рассказала об инициативе по вертикальной интеграции российских программных продуктов. Под эгидой Комитета по интеграции российского ПО (создан в рамках АРПП «Отечественный софт») начато формирование стеков отечественных программных продуктов для поддержания типовых задач цифровой трансформации.

На сегодняшний день предлагаются решения «Рабочее место госслужащего», «Ядро корпоративных коммуникаций», «Автоматизация работы МФЦ», «Рабочее место системы управления предприятием», «Платформа серверной виртуализации и распределённого хранения данных».

Упомянутые стеки включают операционные системы линейки АЛЬТ компании «Базальт СПО» или РЕД ОС компании «РЕД СОФТ», используют СУБД Postgres Pro компании Postgres Professional. Прикладной уровень стеков использует приложения компаний «Галактика» (платформа управления корпоративным контентом), «Электронные офисные системы» (системы автоматизации документооборота), «CommuniGate Systems» (платформа объединённых коммуникаций), «Новые облачные технологии» (офисные приложения и сервисы МойОфис), SPIRIT (программный сервер для видеоконференцсвязи VideoMost), InfoWatch (комплексные решения для информационной безопасности), «Росплатформа» (виртуализация ИТ-инфраструктур).

В рамках объявленной инициативы планируется сформировать электронный каталог для подбора готовых стеков. В нём также можно будет находить необходимые продукты и составлять из них полностью отечественные комплексные решения, готовые к внедрению. Заказчик сможет получить полную картину совместимости компонентов такого решения между собой и с другими внешними приложениями, проверить присутствие всех компонентов в Едином реестре российских программ для ЭВМ и БД.

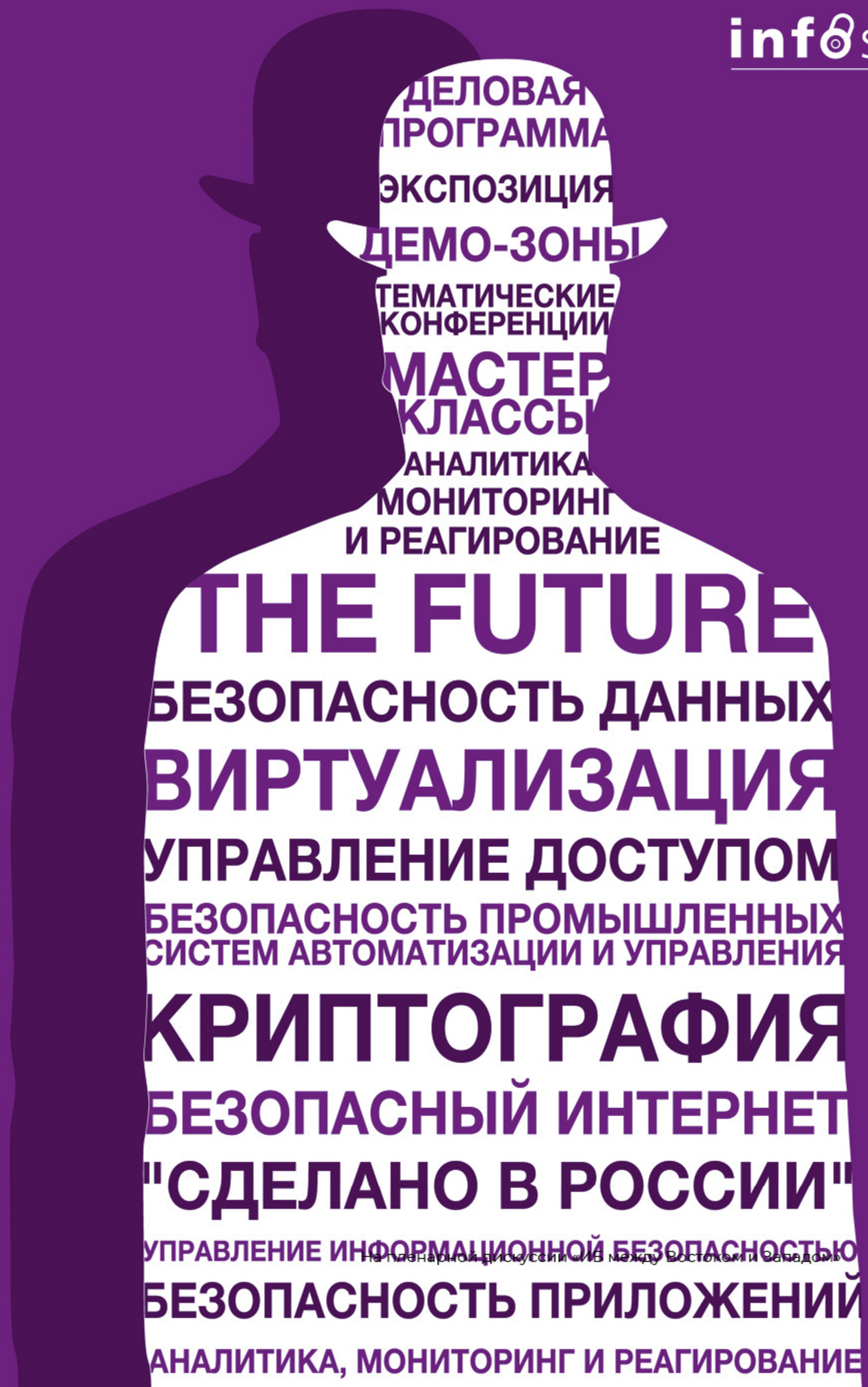
21– 23 ноября 2018

Москва, КВЦ "Сокольники"

itsec®

by Groteck

infosecurity RUSSIA



На пленарной дискуссии «ИБ между Востоком и Западом»

Николай КОЛЬСКИЙ
обозреватель BIS Journal

«ШТАБНЫЕ ЗНАЮТ ШИРЕ!»

КОНФЕРЕНЦИЯ-СЕМИНАР О НОВЫХ ПРАВИЛАХ ДЛЯ УЧАСТНИКОВ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

Банк России совместно с Академией Информационных Систем и Ассоциацией АБИСС провёл конференцию-семинар «Нормативно-правовые изменения в сфере информационной безопасности: новые правила сотрудничества и взаимодействия участников кредитно-финансовой сферы».

Конференциальный уровень мероприятия определили осведомлённость спикеров и переполненность зала — слушатели сидели в проходах. А определение «семинар» подтвердила доступность носителей актуальной информации. Вокруг фигуры Первого заместителя директора Департамента ИБ Банка России А.М. Сычёва во время перерыва случилось столпотворение, которое воскресило в памяти широко известное полотно «Ленин среди делегатов III съезда комсомола».

ИНТЕРЕСНО, ОБОСНОВАННО, НЕ НОВО

Интересными и информативными оказались не только выступления спикеров регулятора. С содержательными докладами выступили, например, компании AKTIV.CONSULTING, чей представитель рассказал о практике реализации требований Положения БР N382-П, и «ДиалогНауки», предъявившей аудитории конкретные цифры по ситуации с выполнением требований того же Положения на основе опыта более чем полусотни аудитов. Правда, выводы, сделанные докладчиками, не блистали новизной. Препятствиями для успешной реализации 382-П являются недостаточность компетенций и остаточный принцип выделения ресурсов на эту работу.

ВИШНИ НА ТОРТЕ

Вишнями на торте стали, несомненно, выступления представителей Банка России.

По итогам сообщений тор-менеджеров регулятора официальная (докулуарная) сессия вопросов и ответов включала 40+ пар вопрос-ответ.

Ключевыми оказались обсуждения противоречий между строгостью, вступающей в силу «нормативки» и следующими обстоятельствами:

- отсутствием чётких определений некоторых понятий;
- отсутствием внятной регламентации практической реализации рамочных нормативных положений;
- пренебрежением учёта:
  - – реальных возможностей немедленного исполнения строгих законов конкретными реализациями ИТ-технологий в финансово-кредитной сфере;
  - – реальных же возможностей модернизации этих технологий для согласия с законодательными требованиями в рамках имеющихся временных, финансовых и кадровых ресурсов.

ЗАКОНОТВОРЧЕСТВО В СТИЛЕ AGILE

Уместно заметить, что описанные выше недостатки законотворчества в финансово-кредитной сфере — это часть базовых пороков нынешней системы права в России. Эксперты конференции-семинара вежливо охарактеризовали ситуацию как *«Законотворчество в стиле agile»*.

Критикуя недостатки законодательной сферы и технологии её внедрения, отметим, впрочем, что А.М. Сычёв попенял в своих комментариях банковскому сообществу, что оно в большинстве своём предпочитает занимать пассивную позицию в процессе создания законов, надеясь на русское «авось» и живя в режиме «пока гром не грянет». К чести присутствующих и самого Первого заместителя директора Департамента ИБ БР никто не оспорил этот упрёк. Хотя… в числе болевых точек внедрения законодательных требований участники называли отсутствие широковещательной «горячей линии» с Банком России. В связи с чем А.М. Сычёв пообещал решить этот вопрос в обновлённой версии сайта регулятора.

ПРО КОЛЛЕКТИВНОЕ БЕССОЗНАТЕЛЬНОЕ

Атмосфера переполненного зала была пропитана духом взаимной заинтересованности в борьбе против всего киберплохого. А также взаимного понимания невозможности ввести

Картина «В. И. Ленин среди делегатов III съезда РКСМ» (художник П. П. Белоусов)

в практику всё хорошее в планируемые сроки.

При этом витала и тревога. Глубоко почвенное, всех примиряющее правило, сформулированное ещё Салтыковым-Щедриным, — «Строгость российских законов смягчается необязательностью их исполнения» — дополняется сегодня ещё одним, пришедшим с Запада: «Своим — всё, для чужих — закон». В связи с чем часть банковского сообщества не по своей вине может оказаться подвешенной на законодательном крючке, что не свидетельствует об абсолютной честности конкуренции.

БРЮЗЖАНИЕ ОБЫВАТЕЛЯ

Продолжая тему обсуждения летних новшеств, видится, что с точки зрения обывателя, нормативные новации Банка России — это лишь реактивное реагирование на вал киберугроз. При этом банки отвлекаются от своей профильной деятельности, тогда как вроде бы тотальный мониторинг кибератак уже ведётся компаниями, подобными «Лаборатории Касперского», и именно они могли бы обслуживать запросы Банка России в части сбора технической информации. Тем не менее по новым правилам ее будут собирать именно банки.

Неоднозначно можно оценить и пользу, причиняемую клиентам банков введением «приостановленных» транзакций.

Лишь с 2020 года внедряется условие об обязательном разделении программных сред подготовки и подтверждения платежей (в том числе при использовании систем ДБО), но уже сегодня вводится обязательность проведения «приостановленной» транзакции через два дня, даже если подтверждения от клиента не получено. И до 2020 года, похоже, остаётся повышенный риск опасности мошенничества, в ходе которого клиент просто отсекается от возможности не то что отказа/подтверждения транзакции, но и от оперативного контакта с банком в течение этих двух дней. Возможность такого отсечения вытекает не только из роста квалификации мошенников, но и из законодательного требования обязательного блокирования «средства проведения» платежа. А если средство проведения платежа и средства коммуникаций с банком — это одно и то же оборудование? Или такого быть не может?

Ну и не выглядит обоснованным фактическое выведение за рамки закона индивидуального опыта антифрод-систем каждого конкретного банка.

Как утверждал Салтыков-Щедрин: «Цель издания законов двоякая: одни издаются для вящего народов и стран устроения, другие — для того, чтобы законодатели не коснели в праздности».

* * *

Хочется верить, что брюзжание в части летних инициатив Банка России — это лишь свидетельство слабой информированности обывателя. А штабные знают больше и мыслят шире. Это уже по мотивам фильма «Рыцари неба». Там крепко наказали пилота, спасшего своего ведомого вопреки приказу «более осведомленного» вышестоящего командования.

ИТ-СОБЫТИЕ ГОДА

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

08/11/2018
отель «Рэдиссон Славянская», Москва

CNews FORUM 2018

16+
Forum* — Форум

БОЛЕЕ 1500 УЧАСТНИКОВ
регистрация на forum.cnews.ru

ДОКЛАДЧИКИ CNEWS FORUM ПРОШЛЫХ ЛЕТ

ЕРМОЛАЕВ АРТЕМ
Министр Правительства Москвы, руководитель Департамента информационных технологий г. Москвы

ЖУКОВ ОЛЕГ
Региональный директор Oracle в России и СНГ

ИВАНОВ АЛЕКСЕЙ
Заместитель Председателя Правления Пенсионного Фонда Российской Федерации

МАЦОЦКИЙ СЕРГЕЙ
Председатель Правления, IBS

ФОМИЧЕВ ОЛЕГ
Статс-секретарь — заместитель Министра экономического развития РФ

ФИЛАТОВ АНДРЕЙ
Генеральный директор IBM в России и СНГ

ЧАРКИН ЕВГЕНИЙ
Директор по ИТ, Российские железные дороги

КАТАМАДЗЕ АННА
Заместитель руководителя Федерального казначейства

БОГДАНОВ КИРИЛЛ
Заместитель генерального директора по ИТ, Аэрофлот

ГИМРАНОВ РИНАТ
Начальник управления ИТ Сургутнефтегаз

PKI-ФОРУМ РОССИЯ

ДЕРЖИТ РУКУ НА ПУЛЬСЕ ВАЖНЕЙШИХ ПРОЦЕССОВ ОТРАСЛИ

В Санкт-Петербурге 25–27 сентября состоялась XVI международная научно-практическая конференция «PKI-Форум Россия 2018». В ней приняли участие 296 представителей из Беларуси, Казахстана, Польши, России. В рамках пяти секций было заслушано 35 докладов, проведено два заседания в формате «круглый стол» и дискуссионная панель «Час эксперта».

По словам председателя программного комитета Владимира Матюхина, рассмотренные на PKI-Форуме вопросы в целом определяют современный этап развития инфраструктуры открытых ключей, электронного юридически значимого документооборота, электронной подписи, сервисов доверия в Российской Федерации и на международном уровне, включая основные трудности, риски и перспективы. Качество деловой программы конференции, её содержание и отличная организация заслуживают общей высокой оценки.

Участие в PKI-Форуме экспертов из четырёх стран, представителей международных организаций и органов государственной власти свидетельствует о важности обсуждения трансграничных сервисов PKI в различных международных форматах (ООН, ЕАЭС, СНГ, АТЭС и др.). На форуме было отмечено, что работа по формированию институциональных основ трансграничного пространства доверия ведётся с активным участием Российской Федерации и имеет положительные результаты.

В то же время у Форума вызвали озабоченность негативные явления, препятствующие эффективному применению технологии электронной подписи и работе удостоверяющих центров. Среди них: отсутствие со стороны регулятора полноценной системы контроля деятельности аккредитованных УЦ; отсутствие диалога между представителями отрасли и Минкомсвязью России, как уполномоченным федеральным органом в области электронной подписи; отсутствие на рынке сервисов проверки электронной подписи, имеющих подтверждение соответствия требованиям ФСБ России.

Важным событием на форуме стало торжественное награждение победителей в номинациях «Стартап года», «Держим марку», «Профессионал года», «Лучший спикер PKI-Форума 2018» и «Лучший модератор PKI-Форума 2018».

* * *

Бессменному организатору конференции Медиа Группе «Авангард» и на этот раз удалось придать форуму завершённую яркую форму и провести незабываемую культурно-развлекательную программу.

Председатель Программного комитета Владимир Матюхин

Сергей Акимов («ИнфоТеКС») и Игорь Качалин (ФСБ России)

Круглый стол «Оценка текущего и перспективного состояния доверия к PKI»

Сергей Кирюшкин («Газинформсервис»)

Иван Аристархов (ФСБ России)

Дискуссионная панель «Час эксперта»

Валентин ПАНОВ
генеральный директор Ассоциации удостоверяющих центров

РЕГИОНАЛЬНЫЕ УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ. БЫТЬ ИЛИ НЕ БЫТЬ?

ВЫТЕСНЕНИЕ С РЫНКА. ГОСУДАРСТВЕННЫЙ УЩЕРБ ОЧЕВИДЕН

Страсти вокруг удостоверяющих центров на PKI-Форуме накалились до предела. На этот раз информационным поводом стал новый законопроект, предусматривающий значительное огосударствление этой сферы. BIS Journal предлагает познакомиться с полноценно изложенной позицией одной из сторон. Надеемся, за ответом Минкомсвязи дело не станет.

СУТЬ ПРОТИВОСТОЯНИЯ

Не подвергается сомнению, что рынок электронных услуг, основанных на юридически значимом электронном документообороте с использованием электронной подписи, получил бурное развитие в России благодаря коммерческим удостоверяющим центрам (УЦ), которые с 2002 года начали «плодиться» в России «как грибы после дождя». За период 2012–2018 гг. Минкомсвязью РФ аккредитованы 486 удостоверяющих центров.

Вот именно это количество — «почти 500!» вызывает сегодня аллергию у некоторых чиновников, хотя УЦ с действующей аккредитацией насчитывается на конец сентября 2018 г. лишь 371. В последние годы в недрах Минкомсвязи один за другим рождаются законопроекты, нацеленные на сокращение количества УЦ до нескольких единиц. И если предыдущие законопроекты предусматривали полное огосударствление этой сферы, то последняя версия такого законопроекта, опубликованная 4 сентября 2018 г. для обсуждения и экспертной оценки, предусматривает возможность существования и нескольких коммерческих УЦ. Заданы такие заградительные барьеры для их аккредитации, после утверждения которых в России, должно остаться не более 10–15 УЦ.

ПРИДУМАННЫЕ БАРЬЕРЫ

Оставим сейчас в стороне вопрос о целесообразности существования более 200 государственных, бюджетных УЦ, остановимся на кластере коммерческих. Основной барьер для них задуман в виде повышения в 143 раза (до 1 млрд рублей) размера собственных средств УЦ. В таком случае в число аккредитованных УЦ войдут 3–4 компании, для которых направление деятельности УЦ является основным, но при этом и те, для кого УЦ — сопутствующее направление, например, операторы сотовой связи, банки, ритейлерские торговые компании и т.п. Остальным действующим сегодня УЦ, которые не сумеют показать наличие собственных средств в указанном размере, уготована судьба лишения аккредитации, по сути — ликвидации.

Вторая новация — повышение в 3 раза — с 30 млн до 100 млн рублей размера финансового обеспечения ответственности аккредитованного УЦ за убытки, причинённые третьим лицам. Она необоснована какими-либо расчётами, фактами, прецедентами недостаточности ранее установленных соответствующих размеров. Не известно ни одного случая, когда страховая компания расплатилась за ущерб, нанесённый в результате дефектов в работе УЦ. Возникает вопрос: разве изменения правил игры, действующего законодательства не должны быть основаны на практике правоприменения, статистике негативных прецедентов, сформулированных и обоснованных предложениях для решения конкретных возникших и систематически повторяющихся проблем? Кто и зачем необоснованно взвинчивает обременения к УЦ?

Наконец, третий удивительный барьер, вызывающий настороженность, с точки зрения потенциальной коррупционной составляющей: новый двухэтапный порядок аккредитации УЦ. После определения Минкомсвязью России соответствия претендующего на аккредитацию УЦ новым требованиям, решение об аккредитации либо отказе в аккредитации будет принимать некий коллегиальный орган, который сформируется из представителей федеральных органов исполнительной власти и представителей экспертного сообщества. Этот же орган будет устанавливать предельное количество аккредитуемых УЦ, принимать на основе заключений Минкомсвязи решения об аккредитации УЦ с позиций оценки деловой репутации руководителя и учредителей УЦ. Можно только предполагать, на основании каких критериев в состав коллегиального органа попадут те или иные эксперты и какими интересами они будут руководствоваться.

Можно напомнить авторам проекта, что любое искусственное ограничение предпринимательской инициативы несёт в себе угрозу конкуренции, национальной и экономической безопасности страны, а такие оценочные понятия как «деловая репутация» являются удобным инструментом для формального отсечения от рынка электронной подписи неугодных конкурентов.

КРУПНЫЕ И МАЛЫЕ УЦ: КТО НУЖНЕЕ И НАДЁЖНЕЕ?

Основная масса коммерческих УЦ (менее 200 действующих) создана 5–15 лет назад. Среди них — менее десятка крупных межрегиональных УЦ с широкой филиальной и агентской сетью во многих субъектах РФ, но основную долю составляют центры, действующие в одном или нескольких регионах. Они успешно конкурируют с крупными УЦ, предоставляя клиентам комплексные услуги, в т.ч. в направлениях программного обеспечения и информационной безопасности. Клиенты зачастую делают выбор в пользу местного УЦ, а не филиала крупного иногороднего УЦ из тех соображений, что в местном УЦ весь персонал — и руководство, и юристы, и бухгалтерия, и квалифицированные специалисты — все рядом, в этом же городе. Проблемы решаются здесь же, очно и быстро.

Можно напомнить авторам проекта, что любое искусственное ограничение предпринимательской инициативы несёт в себе угрозу конкуренции, национальной и экономической безопасности страны

В силу географической близости к местным лицензирующим и контролирующим органам региональные УЦ более осторожны и законопослушны, чем филиалы, и тем более, чем агенты крупных иногородних УЦ. Квалифицированный персонал небольших УЦ стабилен, работает под плотным контролем владельца УЦ, вложившего в этот бизнес значительные личные средства. В то же время, обособленные подразделения крупных УЦ представлены, как правило, мигрирующим персоналом в количестве 4–6 человек, из которых 3–4 менеджеры по продажам. Контроль за обособленными подразделениями со стороны УЦ удалённый, не всегда эффективный, а со стороны Минкомсвязи — никакого. Основная мотивация менеджеров устремлена на объём продаж. Преимущество крупных межрегиональных УЦ перед региональными лишь в налаженной бизнес-схеме, позволяющей минимизировать количество персонала на территориях. Но хорошо ли это с точки зрения информационной безопасности и интересов клиентов? То, что региональные УЦ существуют и развиваются, успешно конкурируя с крупными УЦ, свидетельствует о том, что этот кластер бизнеса УЦ востребован клиентами, он нужен обществу!

Авторы законопроекта обосновывают новые ограничения для аккредитации УЦ «участившимися случаями создания и использования КЭП без ведома владельца». Статистику таких случаев разработчики проекта не приводят, однако известно, что именно ряд крупнейших УЦ оказался замешан в мошеннических действиях по изготовлению квалифицированных сертификатов ключей проверки электронных подписей для перевода граждан из ПФР в негосударственные пенсионные фонды без ведома и заявлений этих граждан. В отношении региональных УЦ такой информации не поступало.

Со стороны представителей ФНС регулярно звучит упрёк в адрес всей массы коммерческих УЦ в том, что они якобы выдают сертификаты ключа проверки электронной подписи с нарушениями, не идентифицируя клиента, в результате чего электронную подпись получили тысячи «фирм-однодневок», нанёсших многомиллиардный ущерб экономике РФ. Очевидно, что УЦ, не обеспечивающие должную идентификацию заявителей, должны нести строжайшую ответственность, вплоть до «пожизненного» запрета работать в качестве аккредитованного УЦ. В то же время, упрекать УЦ за выдачу сертификатов КПЭП фирмам, в дальнейшем признанным «однодневками», совершенно несправедливо. Никакой УЦ, ни коммерческий, ни государственный, не вправе отказать в этой услуге, если заявитель идентифицирован и представил все необходимые достоверные документы. Проблема «фирм-однодневок» не имеет никакого отношения к деятельности УЦ и находится на стороне ФНС.

РЕГУЛЯТОР — КАК ОН РЕГУЛИРУЕТ?

К сожалению, Минкомсвязью до сих пор так и не утверждён Порядок реализации функций аккредитованного УЦ, не конкретизирован алгоритм идентификации пользователей. На запросы УЦ о порядке идентификации пользователей Минкомсвязью даются взаимоисключающие ответы, в т.ч. по вопросу о возможности и правомерности удалённой выдачи сертификата КПЭП при направлении пользователем электронного заявления, подписанного ещё действующей электронной подписью иного УЦ. При этом игнорируются жалобы от УЦ о систематической неработоспособности сервисов СМЭВ, с использованием которых УЦ обязаны проверять паспорта и документацию пользователей. Самые животрепещущие проблемы всех УЦ находятся в плоскости решения перечисленных вопросов, а вовсе не в том, что количество УЦ кажется кому-то избыточным.

Взяв курс на сокращение количества УЦ, с 2017 г. Минкомсвязь в рамках процедуры аккредитации центров ужесточила требования к оформлению представляемой УЦ документации, искусственно затормозив процесс рассмотрения пакетов документов от УЦ, не давая внятных пояснений и не отвечая на звонки, вынуждая подавать заново полные пакеты документов по 3–5 раз и не позволяя осуществлять досылку доработанных документов. Это сильно затормозило процесс переаккредитации, создало колоссальные сложности и нервозную напряжённость для многих УЦ и их пользователей. Нужно ли было их так «кошмарить»? Ведь если не с первого, то с пятого раза практически все УЦ пройдут аккредитацию. По нескольку месяцев значились не аккредитованными УЦ ряда крупных ведомств, в т.ч. ФНС, ПФР, МВД, Минобороны и др., десятки коммерческих УЦ. На конец сентября 2018 г. 86 УЦ «зависли» без аккредитации на период от месяца до года. Кто оценит последствия?

Любопытно, что за 2017 и неполный 2018 годы Минкомсвязь аккредитовала 49 новых УЦ при том, что за все годы прекратили своё существование 19 аккредитованных УЦ. Как можно стенать по поводу «избыточного» количества УЦ и одновременно ежегодно аккредитовывать десятки новых? А ведь экспертами предлагалось Минкомсвязи простое решение: узаконить дополнение к условиям аккредитации — наличие 3-летнего периода работы УЦ в качестве не аккредитованного. Это позволило бы не аккредитовывать «свежеиспечённые» УЦ, свести к минимуму новые аккредитации. Вместо этого Минкомсвязь одной рукой сокращает, а другой — ещё более активно наращивает количество аккредитованных УЦ, доводя ситуацию до абсурда.

Любопытно, что за 2017 и неполный 2018 годы Минкомсвязь аккредитовала 49 новых УЦ при том, что за все годы прекратили своё существование 19 аккредитованных УЦ

ЧТО МОЖЕТ ДАТЬ СОКРАЩЕНИЕ ЧИСЛА УЦ ДО 10–15?

Уход с рынка более 200 коммерческих УЦ, не сумевших показать собственность в заоблачном для них размере, не только разорит их владельцев и усилит недоверие бизнеса к государству, выбросит на улицу тысячи специалистов в этой сфере, но и приведёт к росту цен на услуги УЦ и падению их качества в результате снижения конкуренции, исключению массы организаций из участия в развитии цифровой инфраструктуры страны. Ущерб для пользователей, малого бизнеса, по большому счёту для общества и государства очевиден. О недопустимости необоснованной монополизации рынков неоднократно заявлял Президент РФ. На заседании Госсовета по вопросу развития конкуренции 5 апреля 2018 года В. В. Путин особо отметил: «Государственные структуры, компании с госучастием занимают те ниши, где мог бы работать малый и средний бизнес, фактически вытесняют его с рынков, монополизируют эти рынки. Как следствие, идёт процесс картелизации конкурентных сфер экономики, подрываются предпринимательская инициатива и стимулы к открытию своего дела».

КТО ЖЕ БЕНЕФИЦИАРЫ ПРЕДЛАГАЕМЫХ НОВОВВЕДЕНИЙ И КАКИЕ ЕСТЬ АЛЬТЕРНАТИВЫ?

Несомненно, в выигрыше — крупнейшие УЦ, которые надеются сохранить и даже приумножить свой бизнес путём

скупки за бесценок своих более мелких конкурентов, обречённых на ликвидацию. Достигнет своей цели и Минкомсвязь, стремление которой сократить количество УЦ можно объяснить только невозможностью немногочисленным персоналом Правового департамента обеспечить реальный контроль за сотнями УЦ. Так, может быть, нужно просто расширить штат подразделения Минкомсвязи, добавив туда юристов и специалистов с опытом работы в удостоверяющих центрах, или, что более рационально, законодательно передать функцию контроля за деятельностью УЦ в Роскомнадзор или ФСБ, располагающую территориальными структурами и уже контролирующую УЦ как лицензиатов по криптографии? Совершенно понятно, что невозможно из Москвы, не располагая структурами в территориях, полноценно контролировать УЦ во всех субъектах РФ!

Отдельная тема — это предмет контроля. Вопросы информационной безопасности в УЦ контролирует ФСБ, защиту персональных данных — Роскомнадзор. Минкомсвязь собирает с УЦ пакеты документов, контролирует соответствие документов установленным ею требованиям. Все плановые проверки — документарные. Редкие выездные проверки в составе межведомственных комиссий — только по конкретным заявлениям граждан и организаций.

А ведь контролировать и периодически очно проверять следует не только головные офисы аккредитованных УЦ, а все сотни адресов, где этими УЦ осуществляется деятельность по идентификации пользователей и изготовлению сертификатов. Ибо отдельные или системные недостатки, нарушение процедур идентификации и выдачи криптоключей могут происходить именно в адресах выдачи сертификатов. Формальное сокращение количества УЦ практически не изменит общего количества пунктов деятельности УЦ, но условно уменьшит количество подконтрольных Минкомсвязи субъектов. Что это, как не фикция и самообман? Судя по всему, Минкомсвязь поверхностно подходит к осмыслению этого вопроса, не пытаясь системно взглянуть на проблему, или пытается спрятаться за примитивное, но ничего не меняющее по сути решение. Головные офисы крупных УЦ всегда продемонстрируют полное соответствие требованиям, а что творится в обособленных подразделениях УЦ — Минкомсвязь никогда и не узнает. Как она до сих пор не интересовалась непосредственной практикой обслуживания пользователей в филиалах и агентских структурах УЦ, среди которых немало нелицензированных индивидуальных предпринимателей.

Удостоверяющих центров должно быть столько, сколько востребовано обществом. В режиме конкуренции выживут те, чьи услуги качественнее, дешевле, к кому нет претензий со стороны регуляторов и правоохранителей

ТАК СКОЛЬКО ЖЕ НУЖНО УЦ И КТО ИХ СМОЖЕТ ЭФФЕКТИВНО КОНТРОЛИРОВАТЬ?

Удостоверяющих центров должно быть столько, сколько востребовано обществом. В режиме конкуренции выживут те, чьи услуги качественнее, дешевле, к кому нет претензий со стороны регуляторов и правоохранителей. Остальные утратят клиентов и уйдут. Услуги УЦ должны быть конкурентными — качественными, недорогими и в шаговой доступности. Наиболее близкое направление для сопоставления с УЦ — институт нотариусов, которых в РФ около 8000, определены квоты их количества для населённых пунктов (1 нотариус со своим штатом на 15–25000 жителей). И никому не приходит в голову их сокращать до 10–15 на всю страну, согласившись с обезличенными филиалами в субъектах РФ, устанавливать миллиардный финансовый порог вхождения в статус нотариуса. Однако есть ценз по стажу: чтобы стать нотариусом, необходимо несколько лет поработать помощником.

На сегодняшний день к подавляющему количеству УЦ нет конкретных претензий. Если регуляторам кажется, что их количество великовато, то, усложнив аккредитацию «новорождённым» УЦ, можно постепенно разбираться с качеством оказания услуг существующими. Эффективно задействовать механизмы аудита, иные формы самообеспечения рынком качества услуг. Контроль должен быть не формальным, а действенным и ответственным. Представляется разумным, не взвинчивая требования к финансовым активам УЦ, передать функции контроля за их деятельностью от Минкомсвязи к саморегулируемым организациям удостоверяющих центров (СРО). И пусть финансово своими средствами, или через механизмы страхования за дефекты своих участников отвечают СРО, что вынудит их наладить полноценный контроль за своими членами. Останется лишь законодательно определить формы финансовой ответственности удостоверяющих центров — членов СРО УЦ (индивидуальное, коллективное страхование, компенсационный фонд или их сочетание).

Думается, что это как раз те вопросы, которые Минкомсвязь должна обсуждать публично с экспертным сообществом в рамках существующего, но крайне редко созываемого экспертного совета при Министерстве.

* * *

Во всяком случае, предлагать законодателям проект, несущий в своей основе кардинальное перекраивание и монополизацию рынка услуг УЦ с прогнозируемым ущербом для общества, без достаточного на то обоснования представляется крайне ошибочным и вредным для государства и населения. Хотелось бы, чтобы авторы законопроекта прислушались к изложенным аргументам и приостановили продвижение Законопроекта в его нынешней концепции.

ВИЗИТ МЭРА

В ШТАБ-КВАРТИРЕ ГК INFOWATCH ПРОШЛА ВСТРЕЧА МЭРА МОСКВЫ СЕРГЕЯ СОБЯНИНА И ПРЕЗИДЕНТА КОМПАНИИ НАТАЛЬИ КАСПЕРСКОЙ

Состоялось посещение мэром Москвы Сергеем Собяниным головного офиса группы компаний (ГК) InfoWatch, российского разработчика решений в области информационной безопасности организаций, в рамках которого прошла встреча главы города с президентом ГК InfoWatch Натальей Касперской и трудовым коллективом компании. В мероприятии также приняли участие руководитель Департамента предпринимательства и инновационного развития города Москвы Алексей Фурсин и руководитель Департамента информационных технологий города Москвы Эдуард Лысенко. В ходе визита состоялось обсуждение мер поддержки высокотехнологичных компаний в Москве, в том числе через создание специализированных технопарков.

По решению мэра Москвы Сергея Собянина, в настоящее время прорабатываются предложения о создании технопарка, что позволит его резидентам, включая ГК InfoWatch, получить доступ к налоговым льготам и иным мерам поддержки Правительства Москвы.

По словам Сергея Собянина, наиболее привлекательной площадкой для размещения высокотехнологичного бизнеса сегодня являются московские технопарки, предлагающие качественные площади с доступной арендной платой, благоприятную деловую среду и возможность получения налоговых льгот. Сегодня в 33 московских технопарках работает более 1750 компаний, которые создали 150 тысяч рабочих мест. В том числе, в Москве существуют технопарки, специализирующиеся на размещении ИТ-компаний. В будущем Правительство Москвы готово давать статус технопарка и другим подобным площадкам, например, компании InfoWatch.

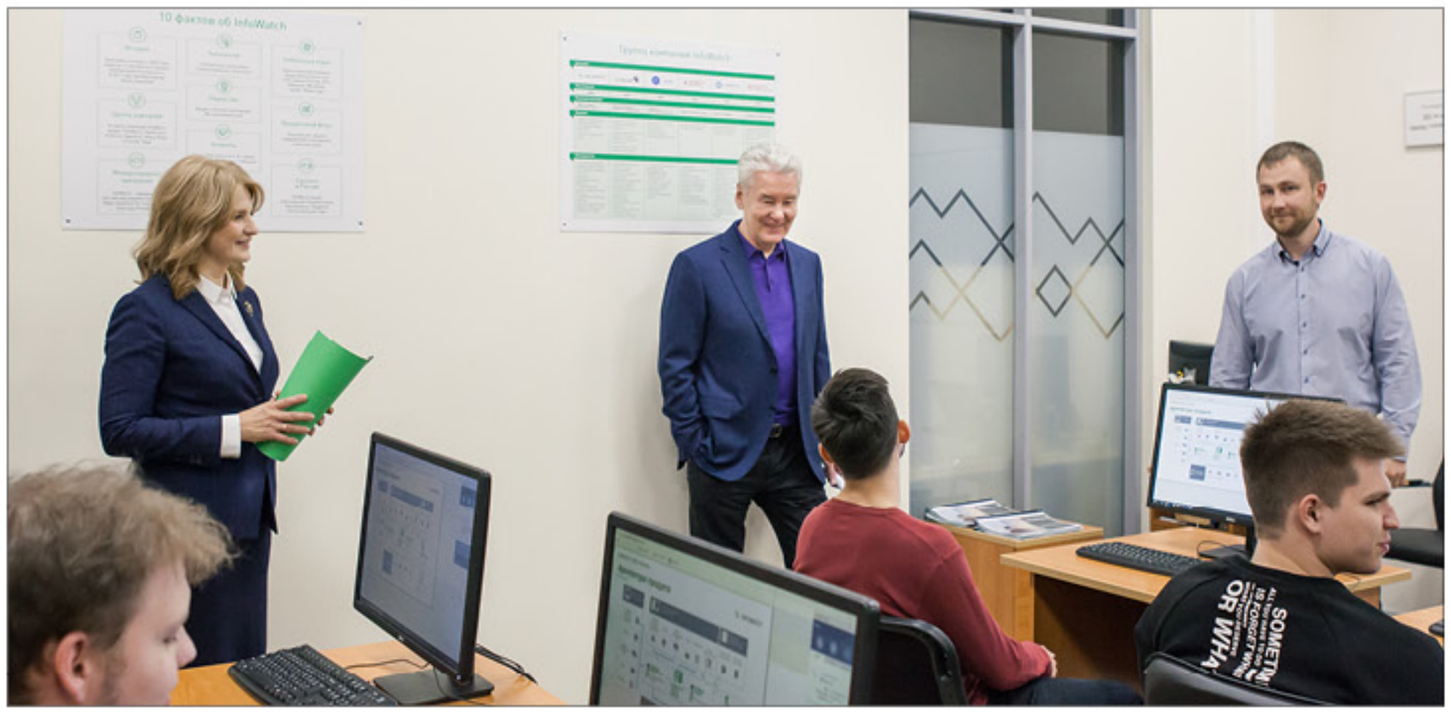
«Москву по праву можно назвать городом программистов, одним из крупных мировых центров ИТ-индустрии. В нашем городе сформировалась полноценная экосистема развития отрасли — начиная со школьного и вузовского образования и заканчивая 15,6 тысячами

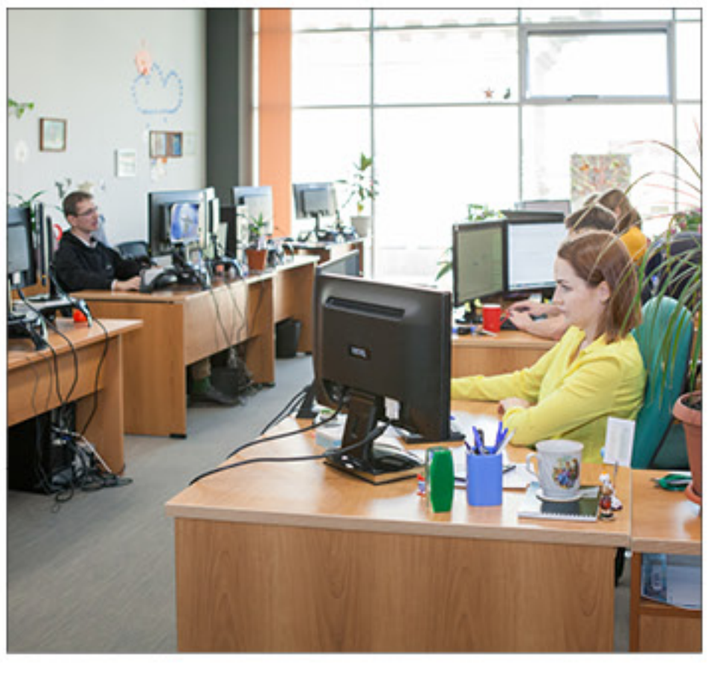
коммерческих ИТ-компаний — от гигантов до небольших стартапов. Я надеюсь, что эта отрасль будет развиваться, потому что у нас есть все: хорошая школа, неплохие колледжи, прекрасные вузы, есть ведущие компании — у нас вся цепочка создана», — сказал Сергей Собянин.

Наталья Касперская рассказала об этапах развития образовательного направления холдинга, включая проект учебного центра «Академия ИнфоВотч». Программы центра нацелены на различные аудитории — госслужащих, руководителей бизнеса, ИТ-специалистов, студентов и школьников.

* * *

Кроме того, глава InfoWatch рассказала мэру об опыте выхода InfoWatch на международные рынки, основных барьерах при экспорте продуктов и решений, с которыми сталкиваются российские ИТ-компании, а также о сотрудничестве с «Московским экспортным центром» по продвижению на рынках стран Ближнего Востока.





СПРАВКА

Группа компаний InfoWatch — российский разработчик комплексных решений для обеспечения информационной безопасности организаций. Продуктовый портфель компании содержит эффективные решения по защите предприятий от наиболее актуальных внутренних и внешних угроз информационной безопасности.

Компания InfoWatch была основана Натальей Касперской в 2003 году в составе «Лаборатории Касперского». С 2007 года является полностью самостоятельной организацией и к настоящему времени объединяет такие бренды как InfoWatch, Kribrum, Attack Killer и Taiga. В компании работают более 400 специалистов, большая часть которых работает в головном офисе в Москве.

Предотвращение утечек конфиденциальной информации (Data Leak Prevention) и защиту организаций от внутренних угроз, связанных с информационной безопасностью, обеспечивает флагманское DLP-решение InfoWatch Traffic Monitor, включая модуль для проведения расследований InfoWatch Vision и программно-аппаратный комплекс InfoWatch Taigaphone для контроля процессов использования смартфонов в рабочей среде, а также система непрерывного мониторинга, диагностики и защиты бизнеса InfoWatch EndPoint Security. Также для предприятий в сегментах малого и среднего бизнеса представлено решение InfoWatch Person Monitor, которое ведет непрерывный мониторинг рабочей активности персонала и использования корпоративных ресурсов.

Защиту предприятий от внешних целенаправленных атак обеспечивают решения компании Attack Killer. Решение позволяет обеспечить автоматизированное и комплексное управление безопасностью веб-ресурса минимизирует риски ошибок, которые могут быть связаны с человеческим фактором, и обеспечивает своевременную защиту прикладных решений и сайтов от появления новых технологий взлома благодаря заложенным на уровне ядра программного продукта принципам машинного обучения. Система автоматизированного контроля исходного кода бизнес-приложений Appercut обеспечивает непрерывную защиту веб-ресурсов благодаря автоматической блокировке ошибок в коде программного приложения еще до их исправления разработчиками такого ПО.

Для защиты промышленных технологических систем был разработан комплекс услуг и решений InfoWatch ASAP, который обеспечивает информационную безопасность автоматизированных систем управления технологическим процессом (АСУТП). Еще одним направлением бизнеса является работа с репутацией заказчика в интернете с помощью платформы комплексного мониторинга и анализа социальных медиа InfoWatch Kribrum.

Компания ежегодно демонстрирует рост продаж своих продуктов и решений, являясь лидером рынка защиты корпоративных данных от утечки в России и странах СНГ. Продукты ГК InfoWatch представлены на рынках Западной Европы, Ближнего Востока, Индии и стран Юго-Восточной Азии.

INFOWATCH®

15 лет защищаем ваши данные

КОМПЛЕКСНЫЕ РЕШЕНИЯ
для обеспечения информационной безопасности организаций

www.infowatch.ru

София СИМОНОВА
обозреватель BIS Journal

AI, ML и ИБ

ЧТО ГОВОРЯТ О НИХ В ИНТЕРНЕТЕ?

Мода, в том числе и на технологии, меняется быстро. Только вчера вкладывались в биткоины и молились на блокчейн, как на панацею от всех бед, а сегодня на пьедестале — Искусственный интеллект (ИИ). С уст не сходит Machine learning, тоже похожее на молитву. Теперь оно, стало быть, всё и решит как на производстве, так и в обслуживании, и, конечно, в сфере ИБ.

Может быть, и решит. Но давайте посмотрим, хватит ли на это денег?

В развитие цифровых технологий вкладываются не только частные компании, но и государство. Так, предварительный бюджет национальной программы «Цифровая экономика РФ» составляет более 3,5 трлн руб. Планируется создание новейшей информационной инфраструктуры: развитие дата-центров и 5G сетей связи, широкое использование платформ для работы с большими данными, развитие направлений искусственного интеллекта, машинного обучения и интернета вещей. По данным из разных источников, на новейшие цифровые технологии из 3,5 трлн руб. будет потрачено 125,3 млрд руб., а на защиту граждан и компаний от угроз со стороны хакеров — всего 18 млрд. ИБ вышла из основного тренда и многие рассматривают защиту информации как одну из областей, где можно успешно применить искусственный интеллект.

По оценкам международной исследовательской компании Markets and Markets, рынок искусственного интеллекта к 2022 г. вырастет многократно — при ежегодных темпах роста совокупного (по разным направлениям ИИ) дохода от 13,9 до 44% в год. Так, мировой рынок распознавания лиц вырас-

тет с $3,37 млрд (2016 г.) до $7,76 млрд (2022 г.). В сфере FinTech совокупный годовой темп роста составит 40,4%, рынок ИИ в этой области на 2022 г. оценивается в $7,305 млрд. Рынок систем машинного обучения в широком спектре областей (банковской, финансовой, здравоохранении, торговле, телекоммуникационных системах, сфере госуправления, обороны, производства, энергетики, а также ЖКХ) вырастет с $1,03 млрд (2016 г.) до $8,81 млрд (2022 г.). Средний годовой темп роста в течение прогнозируемого периода составит 44,1%.

В ЧЕМ ИИ ПОМОГАЕТ ИБ?

В сфере ИБ применение ИИ активно ведётся уже порядка 15 лет: сначала при разработке эвристических модулей антивирусов и при создании защиты веб-серверов, дальше — больше. Сегодня ИИ и технологии машинного обучения помогают отслеживать стабильную работу систем, ищут уязвимости и аномалии, тем самым повышая вероятность обнаружения киберугроз, сокращают время реакции на инциденты в компьютерных сетях, с их использованием работают системы антивирусной защиты. Без новейших систем класса SIEM с использованием технологий машинного обучения и ИИ нельзя представить работу современных SOC. ИИ успешно применяется при сборе и анализе информации для выявления взаимосвязей в случае расследования хакерских атак на объект. Однако решающая роль в паре «машина-человек» пока остаётся за человеком. Тем более что в области ИБ надо смотреть далеко вперёд, а не только изучать уже использованные методы атак.

В РУКАХ КИБЕРПРЕСТУПНИКОВ

Последние достижения в области автоматизации процессов с применением ИИ успешно осваивают киберпреступники. В феврале 2018 г. группа экспертов подготовила 100-страничный отчёт «Злонамеренное использование искусственного интеллекта: прогнозирование, предотвращение и смягчение последствий» (The Malicious Use of Artificial Intelligence Forecasting, Prevention, and Mitigation), в котором проанализированы потенциальные угрозы, которые возникнут при использовании злоумышленниками искусственного интеллекта и систем машинного обучения.

В этом отчёте 26 учёных из 14 ведущих компаний и университетов, в том числе Стэнфорда и Йеля (США), Оксфорда и Кембриджа (Великобритания) вместе с организациями гражданского общества и представителями индустрии ИБ рассматривают ряд злоупотреблений ИИ, фокусируя основное внимание на машинном обучении и вопросах ИБ.

По мнению экспертов, ИИ — это отличное применение компьютеров для выполнения аналитических функций, присущих человеку, исполняемых со скоростью машины. Но компьютер не имеет этической предвзятости, и потому ИИ можно использовать для различных целей как добрых, так и злых. В одних руках обнаруживший уязвимость нулевого дня ИИ нейтрализует её, в других эта «дыра» будет использована как точка проникновения в систему.

В настоящее время алгоритмы ИИ в системе «учатся» на базе миллионов образцов и моделей поведения реаль-

ных вредоносных программ. Обнаружение и изучение нового алгоритма действий, его анализ и оценка потенциальной угрозы происходят за считанные секунды со скоростью и точностью, недоступной для человека. Работа ИИ зависит от качества алгоритма, согласно которому ведётся обучение, и целостности набора исходных данных.

Где возможны потенциальные злоупотребления? В двух областях, говорят эксперты: в неверно написанном алгоритме или неполном наборе исходных данных. Алгоритмы машинного обучения имеют уязвимости как специфичные для этой сферы, так и традиционные, например, переполнение памяти. Поэтому можно говорить о сфере ИБ, пока не привлекавшей внимания специалистов: о кибербезопасности систем машинного обучения и их защите от нападений извне, при которых киберпреступники могут использовать собственные возможности системы для увеличения скорости и точности нападений на оборону системы, поскольку алгоритмы не понимают, с кем и как сражаются.

Для проверки целостности данных возможно применение различных методов, в том числе ограничение взаимодействия ИИ с системой, проверка систем на аномалии и проверка поставщиков данных, например, вредоносного ПО, которое используется при разработке антивирусных программ следующего поколения. Необходимы и исследования построенной с помощью ИИ модели на «мёртвые зоны» или «слепые пятна», чтобы полностью обезопасить систему.

ТРИ НАПРАВЛЕНИЯ

Авторы отчёта выделяют три направления вредоносного использования ИИ — цифровое, физическое и политическое. Они считают, что ИИ в руках злоумышленников позволит проводить широкомасштабные, целевые и высокоэффективные хакерские атаки. Индустрия ИБ уже осознаёт потенциальное злонамеренное использование ИИ и ищет пути реакции на такой сценарий. Как отмечают аналитики, компании, специализирующиеся на безопасности, должны конкурировать не только между собой, но и с хакерами.

Физическое направление использования ИИ несёт значительный этический аспект. Область вредоносного использования ИИ — физическая «идентичность». В последние годы активно развивается индустрия распознавания изображений. Это может иметь как положительные, так и отрицательные последствия. Вычисление преступников в толпе — положительный эффект системы. А, например, алгоритмы определения сексуальных предпочтений людей по фотографиям в соцсетях (их разрабатывали исследователи из Стэнфорда) может негативно отразиться на гражданах, проживающих в странах с авторитарными режимами.

Есть доля негатива в системах распознавания не только лиц, но и речи. С помощью ИИ в сети могут появиться «поддельные» пользователи с синтезированной ИИ речью, может распространяться контент, созданный с помощью ИИ, для дискредитации отдельных лиц и ослабления общественного мнения по отдельным вопросам. В связи с этим появится необходимость адаптации систем аутентификации пользователей как физических лиц, так и системы «человек-машина, имитирующая человека».

К этой же проблеме можно отнести и создание многочисленных фейковых аккаунтов в социальных сетях, распространение фальшивых новостей, целевые фишинговые атаки. И это перево-

НЕЙРОИНФОРМАТИКА-2018

ИИ: МОЗГОВ НЕТ, А АКЦИИ РАСТУТ!

Банковский истеблишмент в борьбе за эффективность всё чаще ставит на искусственный интеллект (ИИ) и, похоже, не без оснований. 8 октября на академической конференции НЕЙРОИНФОРМАТИКА-2018 акции ИИ снова «подросли».

Ученые мужи в очередной раз напомнили, что польза, ожидаемая от ИИ в части оценки рисков, удержания и привлечения клиентов и повышения банковских активов, должна основываться на правильном понимании того, что есть ИИ. В смысле, чего от него можно ожидать и сколько это будет стоить. Не имея возможности обсуждать доклады детально, отметим лишь крупные детали.

Самая крупная. Искусственный интеллект похож на человеческий разум исключительно фонетически. Ничего общего между ИИ и мозгом нет, а фонетическая связь зиждется на постоянном употреблении метафор, незаметно превратившихся в устойчивые термины: «интеллект», «нейрон», «нейронная сеть»…

СРЫВАЯ ПОКРОВЫ

По своей сути ИИ — это несколько типов ИТ-приложений на основе фактически пары разделов математики. Но типов ИТ-приложений в сфере ИИ — несколько, а самих приложений — «тьмы, и тьмы, и тьмы». Желающих отметиться всё больше, и каждый привносит в этот мир приложения со своими «багами».

Добрая старая база приложений ИИ — это математическое моделирование, в основе которого решение уравнений, расчёты по формулам и статанализ. Истоки последнего — в теории вероятностей и матстатистике.

Добрая новая база ИИ — это машинное обучение (ML) и нейронные сети, в коих принято различать два типа: просто «сети» и «глубокие сети».

Суть ML неплохо выразил в своём докладе Алексей Осадчий из ВШЭ. Он отметил, что раньше люди производили

дит использование ИИ в физическом плане в политический аспект проблемы.

Целенаправленная пропаганда и правдоподобные поддельные аккаунты и видеоролики представляют собой мощные инструменты для манипулирования общественным мнением, что уже и было опробовано в ходе предвыборных кампаний в США и Европе. Способность ИИ собирать и анализировать информацию о людях, воздействовать на них, может привести к вторжению государства или иных структур в частную жизнь граждан, угрожать радикальным изменением политических сил между отдельными лицами, корпорациями и государствами.

СПЕЦИАЛИСТЫ ПРОТИВ ЗАКОНОДАТЕЛЕЙ

Среди этических проблем использования ИИ государственными органами встают и вопросы законотворческой деятельности. Часто законодатели не разбираются детально в технических аспектах проблемы, и из-под их пера выходят плохо разработанные нормативные акты. С другой стороны, технические специалисты не хотят заниматься нормативной базой. В то же время многие из них озабочены тем, что раскрытие информации о злонамеренном использовании ИИ может испортить отношение к теме, что приведет к сокращению финансирования или преждевременному регулированию направления.

РЕКОМЕНДАЦИИ

В конце отчёта даётся несколько рекомендаций по смягчению рисков и урегулированию угроз ИБ при массовом использовании искусственного интеллекта. Необходимы:

- переосмысление кибербезопасности и тесное сотрудничество между политиками и исследователями;
- принятие этических норм и практик самими исследователями ИИ;
- определение и методы решений проблем систем двойного назначения с применением ИИ;
- расширение участия заинтересованных сторон и экспертов, участвующих в обсуждении вопросов использования ИИ и машинного обучения. Необходимо изучение различных моделей открытости при обмене информацией, продвижение культуры ответственности и поиск как институциональных, так и технологических решений, позволяющих уравновешивать баланс в пользу специалистов в области ИБ.

КРИТИКА

Критики доклада — эксперты в области защиты данных — не видят серьёзных угроз создания и распространения поддельных новостей, поскольку вместе с усовершенствованием систем машинного обучения и ИИ, генерирующих фейковые новости или аккаунты, одновременно совершенствуются методы и системы их распознавания с использованием того же ИИ.

* * *

Основываясь на отчёте экспертов, можно предположить, что широкое использование систем искусственного интеллекта значительно упростит решение многих проблем, а вопросы этичного использования возможностей искусственного интеллекта зависит от того, в чьих руках он находится. Эти вопросы уже сейчас должны обсуждаться профессиональным экспертным сообществом и представителями органов государственной власти. Тем более что проблем с финансированием направления ИИ в рамках программы «Цифровая экономики» в России не ожидается.

научные знания (законы и формулы, их описывающие), много думая и размышляя. И это очень трудный и затратный во всех отношениях процесс. Сегодня он заменяется ML на основе Больших Данных, т.е. раскалывание «орешка знаний» усилиями разума заменяется перемалыванием больших массивов данных, в ходе которого, выявляются «законы» и «формулы». В результате новую информацию можно предсказывать.

Нейронные сети — это усложнение приложения ML по аналогии с одной из ранних схем работы головного мозга. Тут общего между программой и человеком только то, что программист, реализовавший нейронную сеть, не может объяснить её «поведение». Например, почему после обучения представлениям о внешнем облике кошек, нейронная сеть нарисовала кошку именно так, а не иначе.

ДЕВУШКИ В ХОРОШЕМ НАСТРОЕНИИ

Конкретный пример можно было наблюдать во время доклада руководителя проекта, проводимого в МФТИ при поддержке Сбербанка. Проект был порождён информацией о том, что мессенджеры превращаются в самый удобный канал коммуникаций для населения, и Сбербанк решил вступить в осмысленный диалог на основе собственного ИИ с потенциальными текстовыми сообщениями клиентов. Большая работа, интересные результаты. Обученный ИИ пока еще с разной степенью успеха «беседует» с девушкой в хорошем настроении и с юношей в расстроенных чувствах. С девушкой получается лучше.

Участники конференции единодушно признали, что разные варианты ИИ, понимаемые не как «супермозги», а как несколько типов новых ИТ-приложений, с высокой вероятностью реализуемы. Михаил Лебедев, представлявший на конференции одновременно ВШЭ и штатовский Duke University, а стало быть, весьма информированный эксперт, заявил, что в создание ИИ верит. Но выделка «овчинки» ИИ будет стоить времени и денег. И скорее всего, окупится не «бухгалтерской» эффективностью, но повышением конкурентоспособности и безопасности.

* * *

А одной из уже обозначившихся проблем, связанных с ИИ, является то, что в образовании набирает обороты представление о том, что ментальный анализ и синтез менее эффективны, чем BigData&ML.

Марк НОВОДАЧНЫЙ
корреспондент BIS Journal

Александр БОДРИК
исполнительный директор ANGARA Professional Assistance (MSSP)

КАДРОВЫЕ СТРАТЕГИИ ДЛЯ SOC

ВЫСОКОКЛАССНЫЙ SOC ОРГАНИЧНО СМОГУТ ПОСТРОИТЬ ТОЛЬКО ОРГАНИЗАЦИИ ТОП-50 ЭКОНОМИКИ. ДРУГИМ ПРИДЁТСЯ ИСПОЛЬЗОВАТЬ ГИБРИДНЫЙ ПОДХОД

Банальное определение «Кризис — он в головах» отлично характеризует ситуацию с созданием SOC: часто на первичной стадии создания не определяются цели и задачи, нет понимания целевой процессной модели, люди набираются хаотично — по принципу «как у соседа» или «примерно хватит».

В то же время проблему нехватки кадров в SOC оптимально решать, предварительно определив целевую модель SOC, а именно:

1. Основной сервис (как правило, мониторинг ИБ).
2. Модель нарушителя (для коммерческих структур это в первую очередь киберпреступность и ИТ-администраторы).
3. На основе пункта 2 — перечень сценариев реализации угроз (use cases).
4. Целевая процессная модель.
5. Тип

Перечень сценариев реализации угроз обычно центрирован вокруг Kill Chain и должен покрывать все 6 этапов Kill Chain, а также кейсы отказов в работе Security Controls (встроенные и накладные СЗИ) + кейсы нарушений операционной безопасности службой ИТ (ввода в прод-сегменты непропатченных сервисов и т.п.).

Целевая процессная модель зависит от целевой зоны покрытия — количества объектов под мониторингом, но должна включать как минимум основной операционный процесс из четырёх подпроцессов: Киберразведка, Мониторинг, Расследование и Реагирование (рис. 1). Для внутреннего SOC ключевыми являются процессы Расследование и Реагирование. Грубо говоря, все, что не перерождается в действия процесса Реагирование, представляет собой больше академическую ценность и не помогает снижать ущерб от реальных инцидентов.

Ещё одним крайне ценным для внутреннего SOC процессом является security data management (в более примитивном смысле Управление коннекторами), который позволит упорядочить жизненный цикл подключения к SOC новых ИТ-систем, в том числе предоставить для других корпоративных процессов процессный API, соблюдая который ИТ-проекты смогут и к SOC подключиться и сдать свои проекты вовремя, не тормозя из-за «необоснованных» требований корпоративной кибербезопасности. Классический цикл security data management состоит из пяти стадий:

1. Анализ достаточности данных для use case.
2. Разработка требований к источнику данных.
3. Реализация и тестирование сбора данных.
4. Вывод из эксплуатации источника сбора данных.
5. Управление карточкой источника данных (НСИ).

В результате определения предыдущих четырёх основ (рис. 1) сложится вид SOC — «обычный» SOC (далее SOC), ориентированный на выявление нарушений политик ИБ, утечек и иных технологически простых событий или Managed Detection and Response Provider (далее MDR), способный находить новые угрозы (Threat Hunting).

КАДРОВЫЕ СТРАТЕГИИ ДЛЯ SOC

SOC не очень требователен к ресурсам, но требователен к процессам. Хорошо описанные, отлаженные и внедрённые процессы позволят обойтись привлечением специалистов уровня ИТ-helpdesk, администраторов Windows и администраторов средств сетевой защиты.

Особенных кадровых стратегий для такого уровня не требуется, специалистам нужно всего лишь реагировать на то, что им покажет та или иная аналитическая модель, реализованная на базе решений класса SIEM или data lake.

КАДРОВЫЕ СТРАТЕГИИ ДЛЯ MDR

Однако злоумышленники не планируют подчиняться правилам, поэтому всё больше организаций под SOC подразумевают MDR. От специалистов MDR

Рисунок 1. Основной операционный процесс SOC

уже потребуется глубокое понимание целого ряда сфер (рис. 2).

Готовых специалистов такого профиля на рынке мало, поэтому предлагается использовать одну или микс из следующих стратегий:

1. Развитие существующей команды.
2. Повышение конкурентоспособности оффера работодателя.
3. Селективный аутсорсинг (Hybrid SOC).
4. Поэтапное разворачивание.
5. Привлечение специалистов из смежных областей.
6. Консолидация компетенций за счет уменьшения с трех до двух линий.
7. Формирование регионального центра компетенции.
8. Найм из существующих региональных центров компетенции по SOC.

Стратегии приемлемы и применимы не для всех типов организаций. Например, ориентированные на регионы стратегии 7 и 8 удобны организациям с присутствием в целевом регионе. Разворачивать филиал или обособленное подразделение ради MDR могут себе позволить только игроки рынка, для которых это профильное подразделение.

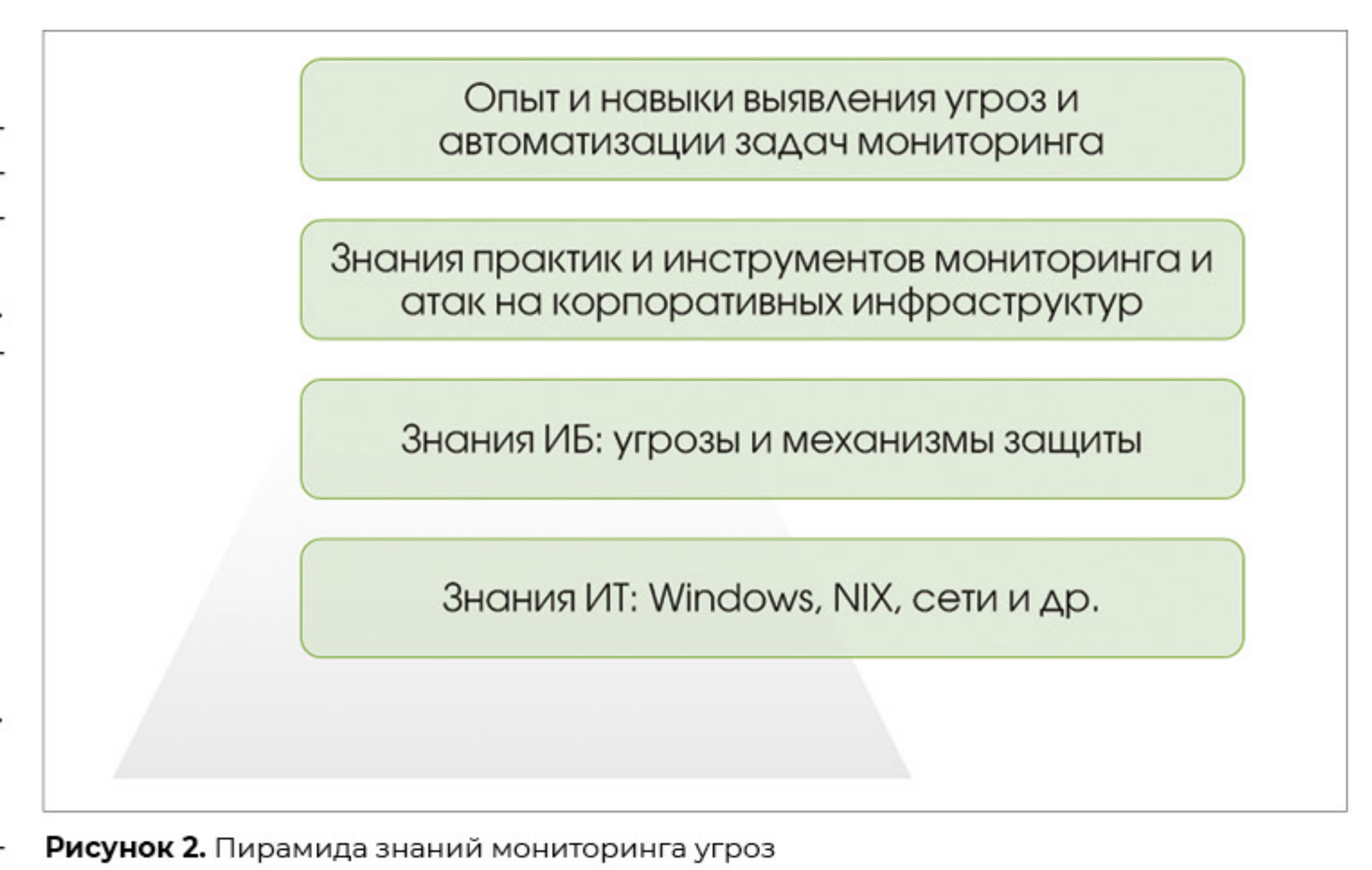


Рисунок 2. Пирамида знаний мониторинга угроз

РАЗВИТИЕ СУЩЕСТВУЮЩЕЙ ИБ-КОМАНДЫ

Прежде чем нанимать новых, ещё не проверенных в бою, специалистов разумно посмотреть на ту команду, что есть. Хорошо, если уже составлены профили (стандарты) компетенций соответствующих должностей, определена их номенклатура и произведены расчёты требуемой численности — иначе потребуется это сделать (самостоятельно или привлечь компетентный внешний SOC, который с этим поможет).

Перед формированием индивидуальных планов развития для членов команды необходимо оценить их навыки — как минимум в форме интервью, задав соответствующие профилям компетенций вопросы. Например, на знание модели OSI, предназначение и типовые особенности работы механизмов аутентификации в Windows и Unix («что делает процесс lsass.exe?»), виды и методы работы средств атаки («как повысить привилегии после получения возможности запуска исполняемых файлов в Windows?»), а также на знание базовых терминов. Увы, многие «специалисты» в SOC даже не знают, что такое IOC.

Повышение навыков происходит как путём киберучений, так и классическими курсами: Администрирование Windows, CCNA, CEH (для изучения методов атаки). Приведены лишь базовые, но, как показывает практика, они же и самые актуальные — пробелов в знаниях специалистов более чем достаточно.

ПОВЫШЕНИЕ РАБОТОСПОСОБНОСТИ ОФФЕРА РАБОТОДАТЕЛЯ

В любой кадровой аналитике первым фактором выбора работодателя соискателем всегда была денежная компенсация. Для внутренних SOC это часто является проблемой, т.к. они затиснуты в рамки корпоративной системы грейдов и окладов. Однако существуют и дополнительные инструменты. Кроме оклада работодатели имеют возможность устанавливать доплату (за коммерческую тайну, за государственную тайну и иные), а также осуществлять разовые выплаты, в том числе и «подъёмные» для переезда кандидатов из регионов. Умелое использование дополнительных инструментов поможет создать особые условия для особых кандидатов, не изменяя всей корпоративной системы мотивации. Но для этого потребуется предварительно выстроить конструктивные отношения с кадровой службой — владельцем HR-бюджета.

Второй по значимости фактор — «интересные задачи». Инструмент этот тяжело управляемый, но очень эффективный. По факту он означает создание нового, а значит, подразумевает возможность решения уникальных проблем. В части технологий это движение в сторону data lake, open source, новых для рынка платформ классов IRP (Incident Response Platform), TIP (Threat Intelligence Platform) и технологий приманок для злоумышленников (Deception Technology) и других. Например, один из банков ТОП-50 тестирует 100% всех новинок на рынке технологий ИБ, в том числе с целью мотивации сотрудников службы ИБ.

СЕЛЕКТИВНЫЙ АУТСОРСИНГ (HYBRID SOC)

Классическим для мировой практики способом снижения нагрузки на штат SOC является привлечение внешнего SOC (сервис-провайдера или MSSP) для выполнения части подпроцессов.

Обычно это процессы мониторинга и расследования, для которых MSSP привносит три ключевые ценности:

1. Быстрый старт за счёт имеющихся людей, технологий и процессов.
2. Предсказание и обход типовых ошибок при создании SOC.
3. Более высокий КПД использования аналитиков.

ПОЭТАПНОЕ РАЗВОРАЧИВАНИЕ SOC

Современные корпорации используют сотни и тысячи ИТ-активов для опера-

Иногда доходит до того, что гиганты забывают, что они уже создали SOC десяток лет назад. Без внимания руководства он успел деградировать, и теперь его строят заново

ционной деятельности. Вместе с тем всегда возможно разделить активы на более и менее важные, как минимум по фактору поддержки ими основных или поддерживающих бизнес-процессов. Совсем не обязательно пытаться объять необъятное и распространить сервис мониторинга сразу на всю компанию, лучше наоборот — подключить базовый объём и плавно тиражировать на процесс за процессом, регион за регионом.

Поэтапный подход позволит снизить одномоментный запрос бюджетных средств, внутренних услуг кадровой службы, давление на рынок труда.

ПРИВЛЕЧЕНИЕ СПЕЦИАЛИСТОВ ИЗ СМЕЖНЫХ ОБЛАСТЕЙ

Декомпозировав для себя, кто такой «аналитик SOC», становится возможным нанимать специалистов из смежных областей. При этом стоит учесть целевую процессную модель, целевую степень использования аутсорсинга и технологические подходы. Например, devops-эксперты будут полезны если строится data lake, но могут быть избыточны, если мы используем много проприетарных «закрытых» технологий.

КОНСОЛИДАЦИЯ КОМПЕТЕНЦИЙ ЗА СЧЕТ УМЕНЬШЕНИЯ С ТРЕХ ДО ДВУХ ЛИНИЙ

MDR подразумевает выявление аномалий через экспертное понимание тонких особенностей работы корпоративной ИТ-инфраструктуры и приложений. В таком случае 1-я линия с ограниченными знаниями и отсутствием реального опыта ИБ-мониторинга лишь пропустит аномалию или, наоборот, замучает аналитиков 2-й линии бесконечными вопросами.

С другой стороны, найти 10+ аналитиков 2-й линии для организации 24×7 сложно и дорого, но будем реалистами: режим 24×7 необходим компаниям, которые живут в таком ритме. Именно в таком режиме они и могут реагировать (рис. 1) на идентифицированные и подтверждённые критичные инциденты. В противном случае потенциальный инцидент подождёт до утра — годами им вообще никто не занимался, и организация не только не прекратила своего существования, но и изыскала деньги на SOC.

Итого. Набор специалистов на 1-ую линию в ряде случаев возможно отменить, ограничившись гораздо более скромным набором на 2-ую и 3-ю линии из расчёта на режим 8×5.

ФОРМИРОВАНИЕ РЕГИОНАЛЬНОГО ЦЕНТРА КОМПЕТЕНЦИИ

После достижения размера ИБ-подразделения в 50+ специалистов в Москве начинают сталкиваться с одними и теми же кандидатами по два и три раза. Московский ИБ-рынок труда «перегрет», и в регионах ситуация в среднем лучше (за вычетом Санкт-Петербурга, Воронежа и Нижнего Новгорода).

При выборе региона для открытия регионального центра компетенции предлагается учесть следующие факторы:

1. Наличие регионального представительства Компании.
2. Баланс спроса и предложения на рынке труда в ИТ (например, в Воронеже кадровая напряжённость больше, чем в Москве за счёт больших региональных центров ATOS и РТЛабс).
3. Размер региона и наличие технических вузов из ТОП-30.
4. Стоимость персонала.
5. Бизнес и политическая среда (например, в Калуге она считается дружественной).
6. Наличие конкурирующих за кадры крупных игроков (особенно активно нанимающих крупных корпораций: Сбербанк, МТС, НЛМК, Газпромнефть).
7. Географическая удалённость (ездить все равно придётся).

НАЙМ ИЗ СУЩЕСТВУЮЩИХ РЕГИОНАЛЬНЫХ ЦЕНТРОВ КОМПЕТЕНЦИИ ПО SOC

Для быстрого укрепления команды возможно нанимать специалистов из существующих региональных центров компетенций. МТС в Краснодаре, Сбербанк в Санкт-Петербурге и Новосибирске являют собой природную цель, благо, компенсации в региональных подразделениях крупных корпораций коррелируют с общим уровнем оплаты труда в регионе.

Многие руководители и акционеры компаний поменьше опасаются «развязать кадровую войну» с компаниями-гигантами (ТОП-30 экономики), но нужно понимать, что службы ИБ как непрофильные подразделения в лучшем случае находятся в конце ТОП-10 внутренних клиентов кадровых служб гигантов, и у них во многом связаны руки корпоративной бюрократией + много других задач, кроме как «воевать» или «мстить».

Иногда доходит до того, что гиганты забывают, что они уже создали SOC десяток лет назад. Без внимания руководства он успел деградировать, и теперь его строят заново. С точки зрения бизнеса, это понятно — SOC для гиганта обычно лишь одно из сотен подразделений средней важности, не более того.

* * *

Построение продвинутого SOC (естественно, со способностью MDR) потребует существенных временных, финансовых и эмоциональных затрат со стороны руководства службы ИБ и кадровой службы организации. Личное мнение автора: высококлассный SOC самостоятельно смогут построить лишь организации ТОП-50 экономики. Другим придётся привлечь внешние SOC для выполнения части подпроцессов — в первую очередь Мониторинга и Расследования, — взяв курс на создание сильной команды, хотя бы для качественного Реагирования.

Анна КАТАНКИНА
обозреватель BIS Journal

АКАДЕМИИ ДЛЯ ГИКОВ[1]

АЛЬТЕРНАТИВНОЕ ОБРАЗОВАНИЕ НАБИРАЕТ ОБОРОТЫ

Информационная безопасность стала модным направлением в образовании не только среди абитуриентов вузов или работодателей, ищущих специалистов. Всё чаще крупные финансовые и IT-компании создают свои академии, открывая в них многочисленные направления в области финансов, искусственного интеллекта, интернета вещей и в том числе в сфере информационной безопасности. Поучиться можно в очной форме (иногда даже за счет организатора или компании-работодателя) или заочно (онлайн). Слушателям, успешно сдавшим выпускные испытания, обещают знания в области ИБ, красивые дипломы и трудоустройство.

ВЗЛОМАЙ СОСЕДА С MAIL.RU!

GeekUniversity. Вместе с Mail.Ru. Онлайн-университет с гарантированным трудоустройством. «Также в разработке и проведении обучения участвуют ведущие технологические компании России», — гласит реклама на сайте Университета.

Как продолжает уверять реклама, главной целью работы учреждения — трудоустройство выпускников, поэтому они «привязали систему мотивации сотрудников и преподавателей к результатам студентов. Мы совершенствуем наше обучение каждый день и сами с удовольствием приглашаем выпускников на работу». За основу обучения взята практика и «подходы ведущих учебных центров США. Вы проведёте 4 аудита информационной безопасности действующих компаний и проектов. Год обучения в GeekUniversity = год реального опыта для вашего резюме».

Что же предлагают для слушателей по направлению ИБ в GeekUniversity? За 4 четверти слушатель получит знания по направлениям:

- Client Side уязвимости (работа веб-протоколов, их уязвимости и методы эксплуатации, защита веб-сервисов от таких уязвимостей; основы БД);
- Server Side уязвимости (server side уязвимостям (RCE, SQLi, IDOR и др.);
- Сети, безопасность сетей (архитектура сетей и обеспечение безопасности проводных и беспроводных сетей. Навыки взлома беспроводных сетей). ОС Linux: Сервер.
- Криптография. Бинарные баги. В этой четверти рассматриваются основные криптографические протоколы, учатся перезаписывать память и загружать свой код в исполнение чужой программы с помощью бинарных уязвимостей. А также изучаются вопросы социальной инженерии и стандарты информационной безопасности.

«После освоения материала первых двух четвертей каждый ученик получит возможность провести аудит веб-сервиса и поучаствовать в реальной Bug Bounty программе, найти уязвимости на сайтах крупных компаний и возможно заработать свои первые деньги за Bug Bounty», — завлекает реклама. По итогам обучения в третьей четверти можно взломать Wi-Fi соседа («о чём вы, конечно же, сразу сообщите ему и объясните, как сделать Wi-Fi сеть безопаснее»). Финалом обучения станет «Подготовка к собеседованию специалиста по ИБ и само собеседование».

Дополнительно Университет предлагает курсы по программированию,

[1] Гик (англ. *geek*) — человек, чрезвычайно увлечённый чем-либо; фанат. Изначально гиками именовали людей, увлечённых высокими технологиями (обычно компьютерами и гаджетами). Слово существует с конца 19 в. Сначала оно применялось к обозначению чего-то странного и необычного. Со временем оттенок с отрицательного (пугающий) сменился на положительный — просто странный.

компьютерным сетям, безопасности мобильных приложений и английскому для IT-специалистов. На их прохождение даётся два года с момента начала обучения. Для поступления необходимо пройти тест и ответить на теоретические вопросы. Зачисление происходит при успешной сдаче (нужно набрать не менее 25 баллов). Если тест не пройден, можно окончить курсы по подготовительной программе, добрать недостающие знания и пройти тест снова. Стоимость обучения в Университете по любой программе — 12500 руб. в месяц. Обучение ведётся на основании государственной лицензии, преподаватели — сотрудники ведущих IT-компаний и специалисты по ИБ. По результатам успешного завершения обучения выпускники получают свидетельство установленного образца о завершении курсов и именной электронный сертификат на портале GeekBrains и Mail.Ru Group.

И ЯНДЕКС СПЕШИТ НА ПОМОЩЬ...

Школа информационной безопасности Яндекса. В начале 2018 г. компания провела набор в Школу информационной безопасности Яндекса, которая прошла в Москве в апреле текущего года. Курсы были ориентированы на студентов и начинающих специалистов. Как описали целевую аудиторию сами представители Яндекса, они хотели видеть на курсах не только студентов и молодых специалистов, но и сисадминов небольших компаний из провинции или сотрудников IT-отделов из НИИ или бюджетных организаций, а также всех интересующихся темой ИБ. От поступающих требовались базовые знания в области IT, теоретические знания по ИБ и правильные ответы на вступительный тест — достаточно было решить половину из предложенных задач. По итогам теста и проводилось зачисление.

Слушателей ждали лекции и практические задания по инфраструктурной и продуктовой безопасности, которые провели специалисты Яндекса. Занятия проходили очно, три раза в неделю, на оставшееся время слушатели получали объёмное домашнее задание. Программа обучения рассчитана на месяц интенсивных занятий, по итогам обучения — экзамен. Все практические задачи, которые рассматриваются в Школе, взяты из жизни и решены сотрудниками компании. По окончании обучения самые успешные слушатели получили предложение пройти стажировку в компании. Обучение проводилось за счёт компании, она же оплачивала проживание и дорогу иногородним слушателям. Все материалы Школы находятся в свободном доступе на сайте Яндекса.

КРИПТОГРАФИЯ? ЭТО МОДНО!

Технологическое сообщество Binary District предлагает одно из модных сегодня направлений обучения. Для слушателей курса «Основы криптографии» не требуется особых знаний в IT-индустрии, хотя желательны базовые знания математики и приветствуется знание языков программирования — курс предназначен для широкого круга лиц, т.е. всех, кто интересуется методами защиты информации. Слушателей познакомят с принципами криптографии и последними достижениями.

«Уникальность курса состоит в том, что помимо знаний классических алгоритмов криптографии он даёт понимание подходов к работе с криптопримитивами и развивает системное мышление. Особенно этот интенсив будет полезен тем, кто хочет в дальнейшем учиться на Blockchain Developer, — завлекают организаторы. — Курс курирует Research Institute — международный научно-исследовательский центр с R&D лабораториями в Москве, Лондоне, Тель-Авиве, Праге и Амстердаме».

Что известно о технологическом сообществе Binary District? Оно «стремится к формированию сильного сообщества исследователей, разработчиков и профессионалов в этих областях. Каждая из программ является результатом сотрудничества Binary District с широким кругом партнёров как российских, так и зарубежных. В Москве Binary District работает в тесном сотрудничестве с Digital October Center — современной площадкой, объединяющей новое поколение разработчиков и инвесторов. Digital October имеет внушительный опыт организации мероприятий, посвящённых новым технологиям».

Цена интенсивного курса из 11 лекций (занятия дважды в неделю) — 55 тыс. руб. Лекции читают кандидаты физ.-мат. наук, специалисты в области ИБ.

СПЕЦИАЛИСТ ИБ ЗА ДВА ДНЯ

Совсем на другую целевую аудиторию ориентируются организаторы тренингов для руководителей и работников предприятий. Курсы проводит международная образовательная компания «Абирой», представительство которой находится в Республике Татарстан. Итогом двухдневного тренинга станут знания по подготовке предприятия к исполнению 187-ФЗ «под ключ» — согласно требованиям Федерального закона № 187 «О безопасности критической информационной инфраструктуры Российской Федерации».

Руководители промышленных предприятий должны не только защищаться от кибератак, создавать системы реагирования на киберинциденты и передавать информацию о них в ГосСОПКА, но и обучать сотрудников и повышать квалификацию персонала в области ИБ. Специалисты «Абирой» помогают компаниям быстро исполнить это требование закона.

Курсы были разработаны «Лабораторией Касперского». В ходе тренинга применяются различные образовательные методики и элементы интерактивного обучения. По окончании курса соблюдение правил кибербезопасности становятся нормой жизни для тех, кто его прошёл и, предположительно, для сотрудников их компаний.

Программа тренинга охватывает различные проблемы ИБ от базовых правил до целевых атак, рассматриваются вопросы утечки данных, безопасного использования соцсетей и пр.

* * *

Курсы включают теоретические, практические и лабораторные занятия. По их завершении участникам выдаются сертификаты от компании «Абирой» и «ЛК», удостоверения о повышении квалификации установленного образца.

«НА ПЕРВОЙ СЕССИИ У НАС «СЛИЛИСЬ» 60% КУРСА»

ВСТУПИТЕЛЬНАЯ КАМПАНИЯ 2018

Марина БРОДСКАЯ
обозреватель
BIS Journal

Жаркая погода, сопровождавшая горячую пору для абитуриентов и их родителей, перешла в тёплую осень. Первокурсники пошли на свои первые лекции, и теперь можно подвести итоги вступительной кампании 2018 г. Она, как и погода, побила собственные достижения прежних лет.

МЫ ПОБИЛИ РЕКОРД!

Новостная лента конца лета полна радостными сообщениями из университетов: «Мы побили рекорд, конкурс составил 70 человек на место!», «Средний балл на экзаменах выше, чем в предыдущие годы!» При этом внимательное изучение условий приёма в вузы в 2018 г., числа бюджетных мест, требований Министерства образования и числа, желающих поступить на конкретную специальность говорит во многом о лукавстве высоких цифр.

Так, по данным всех документов на сайте приёмной комиссии МГТУ им. Баумана, на специальности «Компьютерная безопасность» (10.05.01) открыты 16 бюджетных мест, из которых 2 — целевой приём, 8 — по квотам. Очевидно, что в общем конкурсе на оставшиеся 6 мест победят только сильнейшие, с максимальным числом баллов за ЕГЭ и личные достижения. Для остальных есть 38 мест на платной основе. Ещё интереснее картина на направлении «Информационная безопасность автоматизированных систем» (10.05.03). 30 бюджетных мест включали 3 места по квоте и 26 — по целевому направлению. Какой конкурс был на ОДНО бюджетное место? Да, ещё 51 человек мог пойти на платное обучение. Стоимость года для поступивших в 2018 г. — 284 341 руб.

Число желающих учиться по различным квотам в НИУ МЭИ несколько меньше, но и бюджетных мест немного. Из 20 бюджетных мест по специальности «Безопасность компьютерных систем» (10.03.01) 5 — по квоте, а на 6 из 20 мест на направлении «Организация и технология защиты информации» (10.03.01) будут учиться студенты, поступившие по целевым направлениям. По обеим специальностям также открыты платные места — по 30 на специальность. Стоимость обучения на 1 курсе — 202 тыс. руб.

Интереснее ситуация в ВШЭ. На 30 бюджетных мест подано 412 заявлений. Из 30 мест 7 — по целевой квоте (7 заявлений), ещё 3 — особая квота (17 желающих, у них отдельный конкурс). 30 абитуриентов являлись победителями олимпиад и имели преимущественное право поступления. На 65 платных мест были поданы 253 заявления и к моменту завершения первой волны приёма 56 человек оплатили обучение из расчёта 315 тыс. руб. за год (в прошлом году сумма составляла 260 тыс. руб.).

В МИФИ на 20 бюджетных мест по специальности «Компьютерная безопасность» подано 319 заявлений, 10 человек были зачислены по квотам или вне конкурса, поэтому на оставшиеся 10 мест конкурс превысил 30 человек на место. Минимальный проходной балл на бюджет при прохождении на общих основаниях составил 269. На 4 платных места подали 27 заявлений. Год обучения в МИФИ стоит 250 тыс. руб.

...И АНТИРЕКОРД!

Пользуясь тем, что спрос на IT и ИБ направления из года в год остаётся неизменно высоким, руководители вузов стремятся увеличить число тех, кого можно принять на платное отделение. И никого из этих руководителей не останавливает тот факт, что разница в баллах за ЕГЭ у прошедших на бюджет и оплативших учёбу из своего кармана просто разительная. Конечно, любой экзамен может оказаться лотереей, но факт остаётся фактом — в большинстве случаев база знаний у набравших высокие баллы абсолютно честно основательнее. Отрапортовав об очередном рекорде на вступительных экзаменах, ректоры вузов обычно не рассказывают с высоких трибун, сколько студентов «переживают» первую сессию или переходят на второй курс. Если брать стандартный для технических университетов отсев в 30% в первые два года, то становится очевидным, что кадровый голод в сфере ИБ будет удовлетворён не скоро.

Впрочем, уже трудно скрыть, что университеты не только исполняют запрос на специалистов в сфере ИБ,

Пользуясь тем, что спрос на IT и ИБ направления из года в год остаётся неизменно высоким, руководители вузов стремятся увеличить число тех, кого можно принять на платное отделение

Вопросы о том, стоит ли идти в тот или иной вуз по направлению 10.0.0 часто задают в соцсетях. И ответы на них не прошли бы цензуру пресс-служб университетов

но и решают свои меркантильные вопросы. Этим больше грешат столичные вузы, где стоимость обучения за последние годы (а обзоры мы готовим пять лет) выросла с 120–140 тыс. рублей до 250 тыс., а популярная ВШЭ уже превысила рекордный порог в 300 тыс. руб. за год.

Периферийные университеты не столь жадны, там расценки за обучение в большинстве случаев подняты на величину инфляции. Кое-где за сумму, равную году в ВШЭ, можно успешно прослушать три курса. И, судя по отзывам, полученное образование будет ничуть не хуже, чем в престижном столичном университете. Многие региональные учебные заведения успешно сотрудничают с крупными компаниями, на базе вузов создаются учебные центры, а на семинары и конференции приезжают ведущие столичные специалисты в области ИБ.

ГЛАС НАРОДА (ИЗ СОЦСЕТЕЙ)

Первые государственные образовательные стандарты в области ИБ были приняты в 2010 г., позднее — в 2014–2016 гг. — они были уточнены и дополнены. Выпускники, поступившие в ту пору и получившие знания в соответствии с государственной программой, уже стали молодыми специалистами. Мнения о качестве их подготовки разнятся. Ректоры университетов говорят об отлично подготовленных молодых кадрах, прошедших полную программу в соответствии с требованиями ФГОС, практику в лучших компаниях страны и готовых приступить к обязанностям в своей профессиональной сфере. В то же время профессионалы, месяцами подбирающие кадры в области ИБ, предпочитают брать специалистов из смежных областей и «с нуля» учить их всем тонкостям информационной безопасности.

И тут стоит, наконец, услышать мнение стороны, про которую все почему-то забывают. А именно студентов и выпускников вузов, а также их родителей, на которых собственно и лежит бремя по оплате функционирования университетов. Сделать это сегодня нетрудно.

Вопросы о том, стоит ли идти в тот или иной вуз по направлению 10.0.0 часто задают в соцсетях. И ответы на них не прошли бы цензуру пресс-служб университетов. Эта обратная связь не всегда приятна для них.

Вот типичный диалог в разгар приёмной кампании 2018:

— Подали документы в МЭИ и МИРЭА, подскажите, кто знает, где лучше уровень подготовки по направлениям «компьютерная безопасность»?

— МЭИ, там старый фундаментальный подход к образованию, а вот технологии и оборудование современные.

— Посмотрите на hh.ru вакансии, какой вуз предпочитают работодатели по этой специальности.

— В МЭИ учиться надо самому, ибо знания, которые там дают либо заведомо неверные и на практике не используются, либо устаревшие.

— Закончил МЭИ, в магистратуру не пошёл, много минусов в системе образования и преподавания. Моя кафедра сначала понравилась, было интересно, учили многому по разным предметам в разных областях, но потом всё свелось к одной теме, которую с разных сторон мусолили не один год. Преподаватели хорошо знают свой предмет, но не имеют опыта практической работы и не могут передать студентам свои опыт и знания… Мы учились по книгам, библиотека хорошая, очень выручала.

— Имеющиеся на некоторых кафедрах компьютеры и оборудование морально устарело. На это всегда жаловались не только студенты, но и аспиранты. И можно ли на них преподавать современные предметы — большой вопрос.

— В МЭИ надо выдержать до 3 курса. На первой сессии у нас «слились» 60% курса. Учиться реально сложно и можно забыть про личную жизнь.

— Хороший факультет по информационной безопасности был в МИРЭА.

— Сужу по запросам работодателей и их интересу к студентам. Если университет востребован у работодателей — это лучший признак. Возможно, акценты в обучении связаны именно с запросами потенциальных работодателей. Сильные СПбГУ и Томский университет.

ПРО МАГИСТРАТУРУ

Как отмечают собеседники, продолжать образование после окончания бакалавриата многие не хотят, несмотря на то, что диплом магистра согласно профстандартам нужен для успешного карьерного роста. Но на дипломы больше смотрят в госсекторе, а в коммерческих структурах и зарплата выше, и перспектив роста больше.

Ко всему прочему, у выпускников бакалавриата не так много шансов продолжить образование в магистратуре и по другой причине. Многие университеты, набирающие десятки бакалавров, не имеют магистратур по направлению ИБ. А те вузы, где можно получить диплом магистра, не балуют наличием мест как бюджетных, так и платных. Может быть, поэтому университеты отдают предпочтение направлениям специалитета, а студенты предпочитают учиться 5,5 лет и получать классическое техническое образование в сфере ИБ?

* * *

Завершая краткий ежегодный обзор, замечу, что настала пора вместе или вместо радостных отчётов о прошедшей вступительной кампании обнародовать и реальные цифры выпуска. А также и процент отсева студентов с разбивкой статистики по семестрам, источникам финансирования учёбы и даже баллам ЕГЭ. Ведь если верить преподавателям гуманитарных наук, число безграмотных первокурсников с максимальным баллом по ЕГЭ превышает разумные пределы. Знают ли таблицу умножения и основы алгебры их коллеги — студенты-технари — история умалчивает.

Вуз	Спец. по ИБ	Мест (бюд./пл.)	Заявлений (бюд./пл.)	Квоты на бюджет	Экзамены по ЕГЭ	Мин. прох. балл по приказам	Прох. балл б/пл (2017)	Стоимость уч. года, тыс. руб. (2017 для сравнения)	Магистр	Стоимость
ВШЭ	10.05.01	30/70/ 15 ино	412/253	10	М Р И/ИТК	280	293/нд	315		
НИЯУ МИФИ	10.03.01 10.05.04 10.05.05	20/5 30/15 –/5	319/27 140/26 –/8	5 4	М Ф Р	266/222 270/223 –/203	270 276 278	250,2	10.04.01 75/5	267,6
МФТИ	10.05.01	10/5	31/9	1	М Ф Р	283/221	286/272	250	–	
МВТУ	10.05.01 10.05.03	16/38 30/51	333/нд 281/нд	8 26	Ф М Р	295 298	284/204 цел 270/198 цел	284,341	10.04.01 18/	306, ф156
МАИ	10.03.01 10.05.02	40/40 –/25	1143/101 /25	26	М И/ИКТ Р	245/153 –/171	241/нд 238/нд	193,56 (150,23)		
РГГУ	10.03.01	30/15	568/76	3	М Р И/ИТК	216/138	199/159	217 (208,8)		
МИИТ	10.05.01.65 10.03.01	15/15 17/43	280/38 437/77	5 8	М Ф Р	215/167 217/160	226/149 224/150	206,9 (158,4)		
МИРЭА	10.03.01 10.05.03 10.05.04 10.05.05 10.05.01 10.05.02	40/200 66/140 35/85 35/85 55/140 61/140	Нд	17 30 9 9 19 31	М И Р М Ф Р М И Р	247 233 232 227 226 229	238/нд 224/нд 224/нд 228/нд 220/нд 223/нд	208 (166,4 ск*) (142) 198 (158,5*) (142) (160) 188,5 (150,8*) (160) 188,5 (150,8*) (160) 198 (158,5*) (142) 198 (158,5*) (142)	10.04.01 30 пл	
МГЛУ	10.03.01	17/31	Нд	17	М Иняз Р	нд	–/152	240	10.04.01 1+1	220
СПбПУ	10.03.01 10.05.01 10.05.03 10.05.04	24/25 41/25 41/25 24/25	426/65 519/53 560/112 261/65	4 6 3 2	М Ф Р М Ф Р М И Р М И Р	247/нд 245/нд 248/нд 247/нд	258/нд 235/нд 249/нд 251/нд	180 (153)		
ЛЭТИ	10.05.01	60/15	Нд	10	М Ф Р	249	231/нд	166 (157)		
СПбГУТ	10.03.01	40/70	1356	4	М Р И/ИТК	242/138	238	164 (146)	10.04.01 маг 10/33	
ПГУПС	10.05.03	15/30	245/нд	3	М Ф Р	181/142	215/нд	163,7 (116,2)		
РГГМУ	10.05.02	–/15	Нд	–	М И Р	–	–/128	130 (115)		
СФУ	10.03.01 10.05.01 10.05.03	25/20 20/10 20/10	нд нд нд	3 3 2	М Р И/ИТК	70,33/45,7 70/53 64,33/46	57,67/46,33 72,33/44 58/55,33	154,306 (140,58)	–	
АлтГТУ	10.03.01	33/7	281/нд	6	М Ф Р	198/157	226/нд	96,950 (88,5)		
АГУ	10.03.01 10.04.01	36/10 10/5	414/26 21/1	нд	М Ф Р	нд	173/131	99,5 (92,5)	21 ч на 10 б мест 10/5 пл	101 106380
ДВФУ	10.03.01 10.05.01	23/6 20/9	144/26 /24	2 4	М Ф Р	188/142 189/144	173/нд 156/нд	200 (170)	–	
ВГТУ	10.05.01 10.05.02 10.05.03	16/4 16/7 18/3	198/5 132/4 184/6	10 10 10	М Ф Р	195/140 200/135 199/132	206/нд 201/нд 188/нд	103,8 (95,1)	–	

* предусмотрена скидка для абитуриентов, не добравших баллы по конкурсу

Валерия МЕЩЕРЯКОВА
студентка факультета журналистики
МГУ им. М. В. Ломоносова

КАК Я НАЧАЛ(А) ТРУДОВУЮ ЖИЗНЬ...

СТУДЕНТЫ И ВЫПУСКНИКИ ПО СПЕЦИАЛЬНОСТЯМ ИБ РАССКАЗЫВАЮТ О СВОИХ ПЕРВЫХ ВСТРЕЧАХ С РАБОТОДАТЕЛЯМИ

Продолжаем опрос молодёжи. На этот раз мы попросили студентов и выпускников ИБ рассказать самое интересное: как проходит последний этап выбора профессии. Важнейший как для каждого специалиста в отдельности, так и для отрасли в целом. Оказалось, что часто выбор происходит не в пользу ИБ.

НАТАЛЬЯ ПРЕЛОВСКАЯ, ТОМСК

Помню, когда поступала на кафедру КИБЭВС ТУСУР, не совсем понимала, чего хочу. Тогда меня подкупило звучание слов: «информационная безопасность», «автоматизированные системы» — что-то в душе откликнулось, ну, и подсказало, что это перспективно.

При нашей кафедре работал Центр технологий безопасности. Сначала я проходила там практику, а потом меня взяли на полставки с записью в трудовую книжку. Честно говоря, первое время казалось, что больше отвлекаю других, чем сама работаю, но всё-таки это была моя родная кафедра, и я не боялась, что что-то может не получиться. Работа воспринималась как часть учёбы, как взлётная полоса.

После выпуска оказалось, что в нашем городе не так просто найти работу по защите информации, но я была уверена в своих силах, и успешно прошла несколько собеседований. В итоге попала в одну из крупнейших компаний Томска. Собственно, мне повезло — в меня поверили по одному моему резюме.

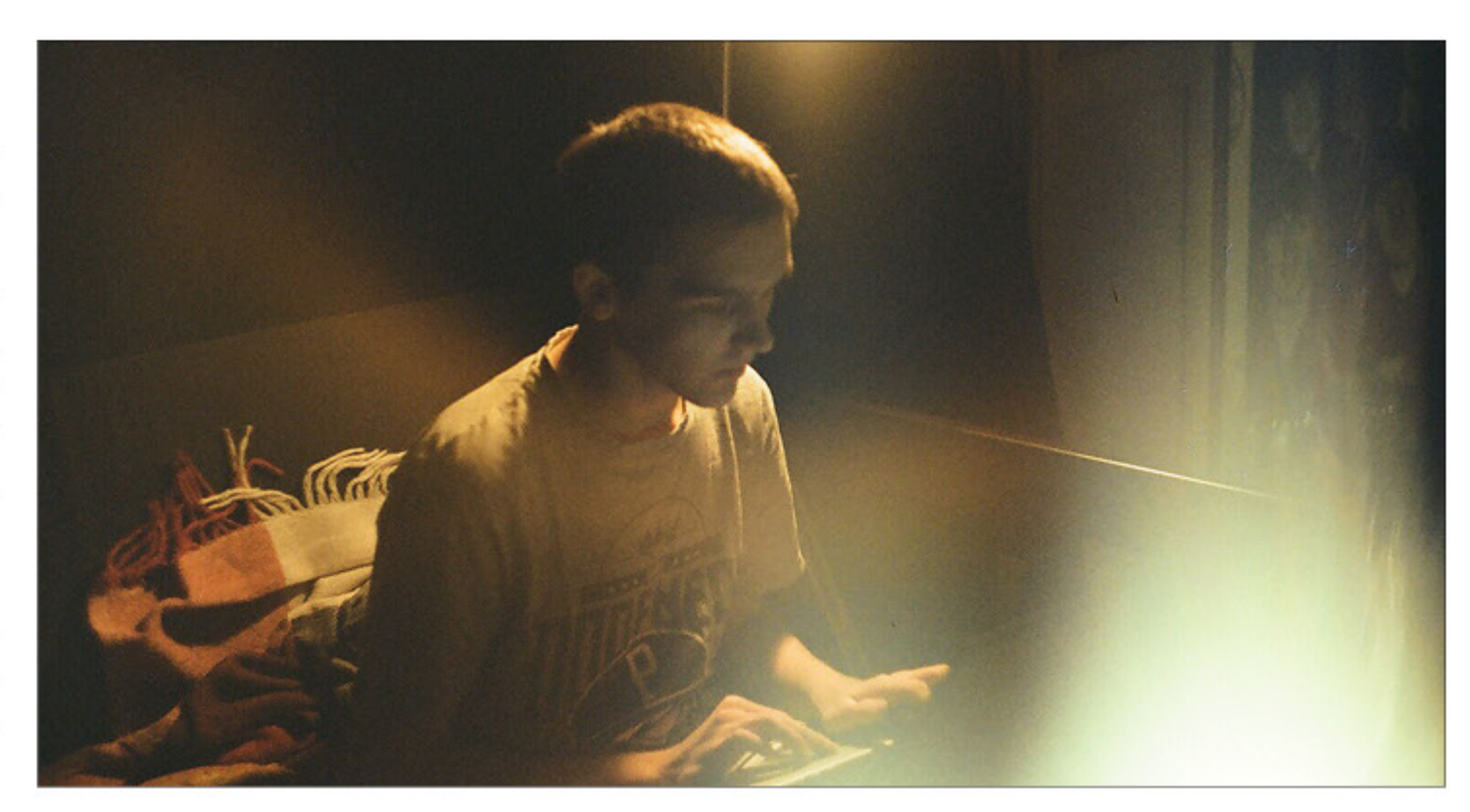
Процесс оформления — проверки, согласования, бумажная волокита… — затягивался, и меня привлекли к новому проекту ещё до трудоустройства. Удивительное ощущение, когда вдруг понимаешь, что те знания, которые ты получила в университете, начинают работать, оказываются необходимыми. Появился азарт, желание во всём разобраться и доказать, что ты и программист, и технический писатель, и системный администратор… Всё это очень пригодилось для развёртывания и настройки автоматизированной системы поддержки пользователей на более чем 3500 АРМ. Система в полном объёме функционирует и сейчас — меняется, развивается, а я продолжаю её администрировать.

Наталья Преловская

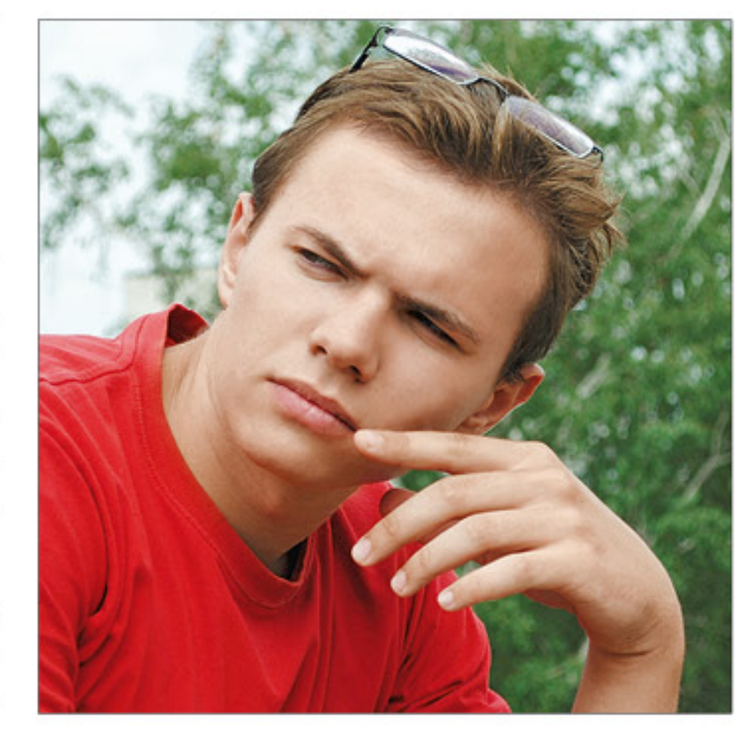
АНТОН ВЛАСОВ, НОВОСИБИРСК

Я не пошёл работать по профилю, потому что такой работы в Новосибирске не было. А если и была, то это скучная работа с документами, актами и всей бумажной чепухой, которая, я считаю, не делает никакого практического вклада в жизнь. По деньгам — в лучшем случае 20–30 тысяч за месяц… Ведь не для этого я четыре года учился и ещё два учусь в магистратуре!

Был вариант работать в Позитив Технолоджис специалистом по ЗИ (классная компания и занимаются они реально интересными проектами), но это предполагало переезд в Москву, а я этот город не люблю, потому и отказался. Учитывая, что я уже имел кое-какой опыт разработки, а душа к ИБ особо не лежала (в университете предметов по профилю было мало, и велись они очень и очень грустно), решил и дальше развивать навыки разработчика. И ни капли не жалею. Сейчас занимаюсь разработкой программ для Android, имею три года опыта разработки в продакшн, а это важно для трудовой книжки, если ты живёшь в России. Писал приложения для Данона, Лореаля, viasat.ru и других чуть менее известных компаний. Нашёл много друзей в этой сфере, все они классные ребята, и я очень рад, что всё повернулось именно так.



Антон Власов



Павел Шабанов

Анатолий Запорожец

ПАВЕЛ ШАБАНОВ, БАРНАУЛ — САНКТ-ПЕТЕРБУРГ

Ещё на третьем курсе в барнаульском АЛГТУ мы с друзьями пытались делать проекты — писали игрушки и продавали на AppStore и GooglePlay. Миллионов мы на этом не заработали — всё как-то внезапно разъехались по разным городам и странам, а опыт-то остался! Один из этих проектов я использовал для дипломной работы и успешно защитился.

После бакалавриата прошёл конкурс на стажировку в СКБ Контур. Отбор был в два тура, на одном из них я спроектировал сервис статистики для многопользовательского шутера. Провёл все лето в Екатеринбурге на стажировке. Но параллельно подал документы в университет в Питере на программную инженерию. В конце лета встал вопрос: идти на работу в компанию (меня позвали по итогам стажировки) или продолжить учёбу? Подумал, что университет важнее и уехал в магистратуру в Петербург. Сейчас учусь и работаю одновременно, пишу кроссплатформенные мобильные приложения.

АНАТОЛИЙ ЗАПОРОЖЕЦ, НОВОСИБИРСК

На первую стажировку я попал на 4 курсе по приглашению знакомого. Собеседование было достаточно комфортным: короткая беседа по общим условиям с HR-ом и разговор с техническим специалистом в основном по нативному JavaScript и его фреймворкам.

Стажировка эта не оплачивалась, так как я делал не реальный проект, а большое тестовое задание, которое только походило на реальный проект. Но после месяца такого тестирования меня взяли в штат. Первый проект, в котором я участвовал, был для заказчика из Новой Зеландии — небольшой веб-интерфейс для удалённого управления серверами, через которые проходит защищённая ip-телефония. Сейчас работаю над проектом для Австралии: социальная сеть для жителей страны, с помощью которой они могут улучшать жизнь вокруг себя, выкладывая свои идеи на всеобщее голосование. Идеи с большим количеством голосов привлекают инвестиции, консулов, волонтёров и так далее.

Совмещать учёбу, даже магистерскую, и работу сложно, хочу договориться на более гибкий рабочий график. Сложно ещё и потому, что в работе и учёбе расходится практически всё. В университете нас учили информационной безопасности в области технической защиты (немного приборостроения, применения технических устройств и т.д.), а программирование было только в начале обучения и только общий курс.

Даниил Бессмертных

Виктория Волкова

ДАНИИЛ БЕССМЕРТНЫХ, КРАСНОГОРСК — ПАРИЖ

Стабильно получать зарплату я начал на третьем курсе. К нам пришёл преподаватель по базам данных и сказал, что есть вариант подработки. Это была небольшая фирма, они хотели развивать проект с обработкой данных форекс-трейдингом. Компания оказалась не очень серьёзной. Я работал там три месяца, потом мы стали расходиться в понимании целей. Я считаю, что в проект нужно вкладываться финансово и морально, а если всё делается на чужом голом энтузиазме, то и винить за ошибки или недоработки, получается, некого. Вот и разошлись.

Летом, устроился на стажировку в компанию Alawar, которая пишет игры на американский рынок. Работал как программист, сидел там с 9:00 до 18:00. И хотя это была неоплачиваемая стажировка — для зачёта университетской практики, — там все было серьезно. На собеседовании давали технические задачи, я их обдумывал и презентовал решения. Более того, на отборе нас было несколько человек, а на каждое задание давали всего пять минут. Когда через несколько дней мне позвонили и сказали, что я принят, я, конечно, был очень рад.

Сейчас я учусь и работаю в Париже, в Университете Пьера и Марии Кюри. А перед самым отъездом из родного города, работал в другой компании разработчиком приложений. Туда тоже было довольно сложное техническое собеседование: так же решал задачи, а потом проходил тесты на стрессоустойчивость и IQ. Моя мама психолог, поэтому, как вы понимаете, я все тесты знал и прошёл их на ура. Работал в этой компании около года, потом получил приглашение из Франции.

Когда уходил, сильно поссорились с начальником: проект был сложный, к тому же в активной стадии. В итоге он сказал: если вернёшься, я тебя никому не порекомендую. Пока что все на моей стороне, да и возвращаться я не собираюсь.

ВИКТОРИЯ ВОЛКОВА, КЕМЕРОВО

На 3 курсе поехала на стажировку в Железногорск, и там у меня появилась трудовая книжка. На самом деле, мне помогли знакомые. Вообще-то я была такая одна в группе — остальные никуда не ездили, проходили практику в технопарке рядом с университетом. Да никто и не хотел большего, зачем утруждаться?

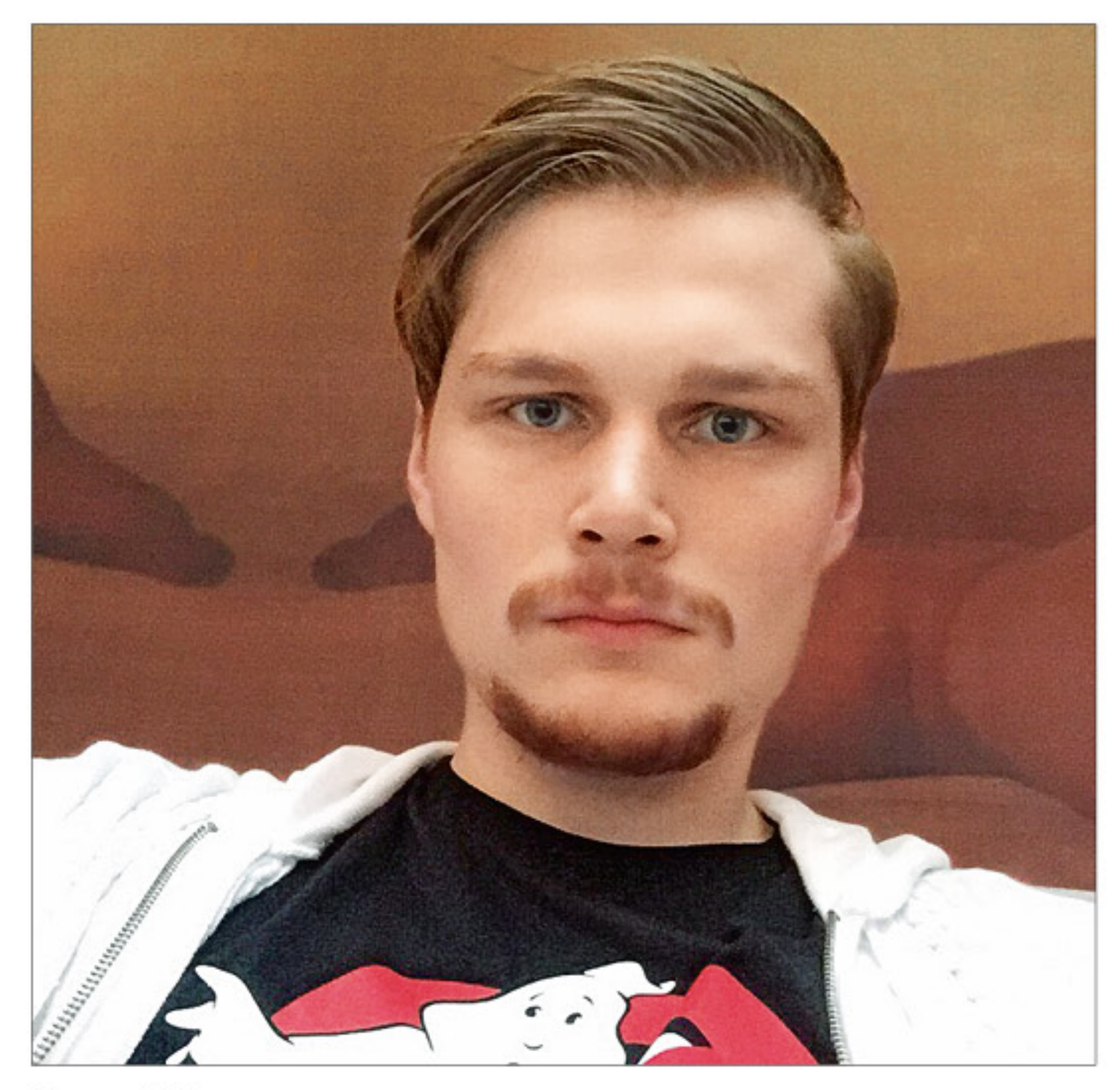
На этой стажировке заработала первые деньги, 20–30 тысяч было вполне: вернулась в свой город и отучилась на эти деньги в автошколе. Потом, курсом позже, выиграла стажировку в Intel — нужно было всего лишь подать своё резюме на программу и ждать возьмут или нет — и несколько месяцев работала в Новосибирске. Мне ужасно понравилось! Это же так приятно, работать в таком комфортном офисе, где есть всё: спортзал, разные игры, хорошая еда и так далее. Человек, работая в таких условиях, становится намного продуктивнее, появляется подъём, больше желания для творчества. Какое-то время очень хотела работать в большой компании, чтобы был большой коллектив и этот желанный офис.

Сейчас ценности поменялись: хочу заниматься наукой. Точно знаю, что это моё. Окончила аспирантуру. Туда я пошла потому, что повезло с научным руководителем, иначе бы не стала подавать документы. Из ближайших планов — дописать и защитить докторскую диссертацию.

ГЕОРГИЙ ДАНИЛОВ, НОВОСИБИРСК — МОСКВА

Первые деньги я получил ещё в школе. Учился в профильном классе и делал ребятам задания по программированию. Своему классу, конечно, бесплатно, а вот другим устанавливал цены.

На I курсе поступил в другой город на ИБ, заехал в общежитие, будучи зелёным абитуриентом. В то время были такие «отработки» для вновь прибыв-



Георгий Данилов

Арина Можейкина

ших — девушки мыли полы и окна, парням доставалась работа потяжелее, но мне повезло. Старшекурсник, который отвечал за интернет во всём здании, оказался земляком и взял меня к себе помощником. Год так и работали вместе. Правда, я только за жилье — у нас была «блатная» комната на двоих, в то время как все жили по четверо. На 3 курсе я уже в одиночку поддерживал сеть общежития, меня приметили и взяли на кафедру на полставки. Выполнял разные задания, от написания программ до анализа определённых устройств на предмет взлома.

Параллельно с учёбой и работой брал на разработку веб-сайты, но нигде не публиковал себя, делал только знакомым и знакомым знакомых. Студентом не мог потребовать за свою работу много: получал от 5 до 50 тысяч за проект. Сейчас работаю программистом в крупной московской фирме.

АРИНА МОЖЕЙКИНА, ЕКАТЕРИНБУРГ — САНКТ-ПЕТЕРБУРГ

В конце учёбы на специалитете разместила своё резюме на каком-то из сайтов по поиску работы. Ни на что не рассчитывала. Резюме моё сложилось благодаря рабочей практике в университете: я занималась криптографией, разрабатывала свою программу, участвовала в проектах, грантах. И именно с этого единственного сайта мне ответили.

Собеседование прошло легко: говорили больше о жизни. Коронный вопрос: как вы видите себя через пять лет? Ответила, что замуж не собираюсь, да и о детях пока не думаю (коронный ответ для молодых девушек, возьмите на заметку, если хотите попасть на работу). Это было моё первое собеседование, и я спросила: а что дальше? Они сказали что-то вроде: всё, приходи во вторник, покажем твоё рабочее место. Я, мягко говоря, удивилась — рассчитывала на жесткую конкуренцию. Так я работала инженером, тестировала программное обеспечение около двух лет, пока не поступило заманчивое предложение из культурной столицы.

Сейчас учусь в аспирантуре в Петербурге. Мне кажется, без процесса обучения я начинаю деградировать. Ведь это скучно, просто так работать и работать. Будто драйв уходит.

* * *

Истории разные и в то же время типичные, и очень лестные, на первый взгляд, для отрасли ИБ. Во-первых, все наши герои — очень инициативные современные ребята, их внутренней свободе и поисковой активности можно только позавидовать. «Смелость города берёт!» — это в прямом смысле слова о них. Один сначала Екатеринбург покорил, потом Питер, другой вообще — Париж! Во-вторых, они все — не ленивые, умные, грамотные, и, что важно, умеющие учиться молодые специалисты. Если бы было не так, они попросту не сделали бы того, что сделали, не добились бы того, чего добились. Причем, судя по их же рассказам, они не считают это великими достижениями. Значит, ещё и скромные! По сути такую молодёжь можно смело записывать в золотой фонд отрасли и быть уверенным: будущее профессии — в надёжных руках!

Только вот вопрос: о какой профессии идёт речь? И о какой отрасли? ИБ или ИТ?

Вы обратили внимание, что только один учащийся благополучно трудится в сфере ИБ? Остальные как-то совершенно естественно соскользнули, утекли в ИТ. Почему? Как такое стало возможным? Государство целевым образом тратит огромные деньги на образование и подготовку кадров в сфере именно ИБ, а получается, что весь этот мощный поток из денег, орг-, обр- и пед-усилий выливается не в тот — в другой! — бассейн.

Вот это — проблема.

Сергей БУЛАЕВ

Сергей ГОЛОВАНОВ

Дмитрий ЛАРИН
историк криптографии, кандидат технических наук

ИНЖЕНЕР, ИЗОБРЕТАТЕЛЬ, ИСТОРИК

К 80-ЛЕТИЮ СО ДНЯ РОЖДЕНИЯ ЛЕОНИДА БУТЫРСКОГО

21 января 2018 года исполнилось 80 лет со дня рождения Леонида Бутырского (21.01.1938–31.01.2015). Леонид Сергеевич Бутырский — советский и российский специалист в области защиты телефонных систем связи — внёс большой вклад в обеспечение безопасности нашей Родины. За достигнутые практические результаты награждён 8 медалями, знаками «80 лет криптографической службе» и «Криптографическая служба России», нагрудным знаком «Почётный радист». Его изобретательская деятельность отмечена нагрудным знаком «Изобретатель СССР».

Бутырский Л. С. является автором уникальной книги [Бутырский, 1978], в которой рассматриваются вопросы, связанные со свойствами речевого сигнала и техническими проблемами восстановления разборчивости речи в условиях глубоководных погружений и полётов в космос, когда требуется применение специальных дыхательных смесей. Изданию этой книги в большой степени способствовал А. И. Берг — советский учёный-радиотехник, военный моряк, адмирал, организатор науки, один из создателей советских радиоэлектронных средств разведки, удостоенный звания Героя Социалистического Труда, награждённый высокими правительственными наградами и Золотой медалью имени А. С. Попова. А. И. Берг внёс огромный вклад в развитие подводной связи и радиолокации. В СССР был одним из пионеров кибернетики и смежных с ней областей знания и техники. Л. С. Бутырский принимал участие в работе конструкторского бюро кибернетики на кафедре автоматики Московского энергетического института, созданного по инициативе А. И. Берга.

Леонид Сергеевич сделал большой вклад в подготовку специалистов в области цифровой обработки речевого сигнала. Он является автором трёх курсов лекций, посвящённых данной проблеме. Л. С. Бутырский щедро делился своим опытом с молодыми сотрудниками и преподавателями. Его заслуги отмечены знаком «За подготовку кадров».

Леонида Сергеевича Бутырского также можно смело назвать одним из ведущих специалистов по истории криптографии. Он является соавтором ряда научных трудов в этой области [Бутырский, 2012], [Бутырский, 2013]. Эти книги посвящены криптографическому противостоянию СССР и нацистской Германии и её союзников в годы Великой Отечественной войны. В первой книге также подробно рассматривается эволюция средств шифрования текстовых сообщений с античных времён до Второй мировой войны, приведены описания советских, немецких, японских, американских, шведских шифрмашин, а также шифраторов производства ряда других стран. Отдельные главы посвящены шифраторам речи, радиостанциям для агентурной разведки и истории стеганографии.

Вторая книга является десятым томом многотомного издания «Великая Победа», подготовленного большим коллективом отечественных историков. В этом томе на основе архивных документов рассматривается деятельность советских криптографических служб в период Великой Отечественной войны, криптографическая деятельность советских разведчиков, контрразведчиков и партизан, а также кратко освещена работа криптографов нашего основного противника — гитлеровской Германии.

Л. С. Бутырский является автором (соавтором) 29 статей и неоднократно выступал с докладами на различных конференциях, посвященных истории криптографии. Тематика работ Леонида Сергеевича охватывает широкий круг вопросов, в первую очередь об истории отечественной криптографии. Среди них есть циклы статей о Спецотделе при ВЧК, от создания которого 5 мая 1921 года ведёт начало новейшая история российской криптографической службы. Ещё один цикл статей рассказывает о работе советских криптографов и связистов в годы Великой Отечественной войны.

Особое место занимают статьи об отечественных криптографах, начиная с Х. Гольдбаха и Ф. Эпинуса до выдающихся деятелей советской криптографии В. А. Котельникова, В. Я. Козлова, Н. Н. Андреева, а также создателей отечественной телефонной аппаратуры защиты речевого сигнала.

Уделял он внимание и истории зарубежной криптографии. Среди его работ есть циклы статей по истории развития криптографии в Швеции, Нидерландах, Германии, а также истории систем защиты речевого сигнала в США.

Присущие Леониду Сергеевичу самоотдача, глубокое чувство личной ответственности всегда являлись надёжным ориентиром и примером, достойным подражания для коллег. Весь свой творческий потенциал он отдавал делу, которому посвятил жизнь. Высочайший профессионализм, поистине энциклопедические знания, всеохватывающая эрудиция, большой жизненный опыт создавали ему непоколебимый авторитет в коллективе. По праву заслуживают восхищения и уважения чёткость и аргументированность занимаемой позиции, бодрость духа, несгибаемый оптимизм, широкий круг интересов, идей и реальных дел. Постоянно находясь в поиске, Леонид Сергеевич беспрестанно поражал коллег новыми идеями, свежестью и нестандартностью взглядов, юношеским азартом, дальновидностью прогнозов.

Леонид Сергеевич Бутырский (21.01.1938–31.01.2015)

Заядлый путешественник, Леонид Сергеевич посетил многие уникальные места нашей Родины: Курильские острова, Долину гейзеров на Камчатке, остров Сахалин, озеро Байкал, исторические города Средней Азии (Ургенч, Хива, Самарканд, Бухара, Ашхабад, Душанбе, Хорог), горнолыжные курорты Кавказа. Ему удалось увлечь интересом к путешествиям многих своих друзей и сослуживцев.

По воспоминаниям Г. В. Емельянова, который считает Леонида Сергеевича одним из своих первых наставников, он был чрезвычайно выдержанным и интеллигентным человеком, никогда не повышал голоса на собеседника, как бы ни расходились их точки зрения.

* * *

Его активный образ жизни и серьёзное увлечение спортом — горными лыжами, спидвеем, большим и настольным теннисом, водно-моторным спортом всегда привлекали к нему молодёжь и делали его душой любого коллектива.

ЛИТЕРАТУРА

1. [Бутырский, 1978] Петленко И. Б., Бутырский Л. С. Речевая связь в искусственных атмосферах. М.: Связь, 1978
2. [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. Гелиос АРВ, 2013. 3 изд. стереотипное М.: Гелиос АРВ, 2017.
3. [Бутырский, 2013] Бутырский Л. С., Ларин Д. А., Шанкин Г. П. «Великая Победа», многотомное продолжающееся издание под общей редакцией С. Е. Нарышкина, А. В. Торкунова, Том X. «Война в эфире». М.: Издательство «МГИМО-Университет», 2013.

Дмитрий ЛАРИН
историк криптографии, кандидат технических наук

XV ВЕК. ВРЕМЯ ЗАМЕНЫ

ПЕРИОДИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В РОССИИ. ЧАСТЬ 3

ТАЙНОПИСЬ ИНОКА ЛУКИ

Мы уже упоминали, что часто шифрование применялось писцами и переписчиками книг религиозного содержания. В основном шифровалось имя автора или переписчика. Характерным примером применения сразу нескольких вариантов шифрования с помощью изменённых знаков служит так называемая «тайнопись инока Луки». Исследователь русской письменности М. Н. Сперанский [Сперанский, 1929] обнаружил её в Смоленской Псалтыри 1395 года. Автор этой Псалтыри, уроженец Смоленска инок Лука, прекрасно владел искусством письма, что в те времена было редкостью.

В этой рукописи Лука применил три вида шифрования: несколько вариантов изменённых начертаний, «цифирь счётную» и систему вязи.

Первый способ — это пропорциональная замена, где некоторым символам открытого текста соответствуют по нескольку символов шифрованного. При этом ряд символов шифрованного текста для одного и того же весьма похожи, а для другого различны. Например, буква а (почти одинаковые), буква в (разные). Вот что начертал Лука на листах 72 и 129 (рис.1).

Рисунок 1. Пропорциональная замена, сделанная при помощи изменённых знаков. Сверху вниз: шифрованный текст, открытый текст и шифрованный текст, ключ.

Вот ещё один ключ шифра пропорциональной замены инока Луки (рис. 2). Тут при создании шифрованного алфавита автор использовал следующие приёмы:

- Перевороты букв. Одни символы он переворачивает вниз головой или в обратную сторону, прибавляя к ним чёрточки (рис. 2 а);
- Деформация букв. Тут Лука затушёвывает обычный облик букв (рис. 2 б);
- Урезка части букв (рис. 2 в);
- Использование особых знаков (рис. 2 г).

На рис. 3 представлен шифр простой замены инока Луки, так же созданный с помощью изменённых знаков. Обратите внимание, что буквы открытого текста идут не в алфавитном порядке.

Теперь кратко рассмотрим другие шифры инока Луки. «Цифирь счётная» подробно описана в предыдущей статье (BIS Journal № 3/2018). Вязь представляет собой фактически ту же систему изменённых знаков. Она образуется путём наложения букв друг на друга, нахлёстывания, зацепления «хвостиков» и т.п. Образец надписи вязью представлен на рис. 4 [Соболева, 2002], [Тайнопись, 2018].

Стоит отметить, что в Европе революционный шаг в развитии криптографии был сделан в 1401 году в Мантуанском герцогстве (Италия). Секретарь герцога Симеон де Крема предложил

ФСРБИТ
Материалы рубрики «История» публикуются при поддержке Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)

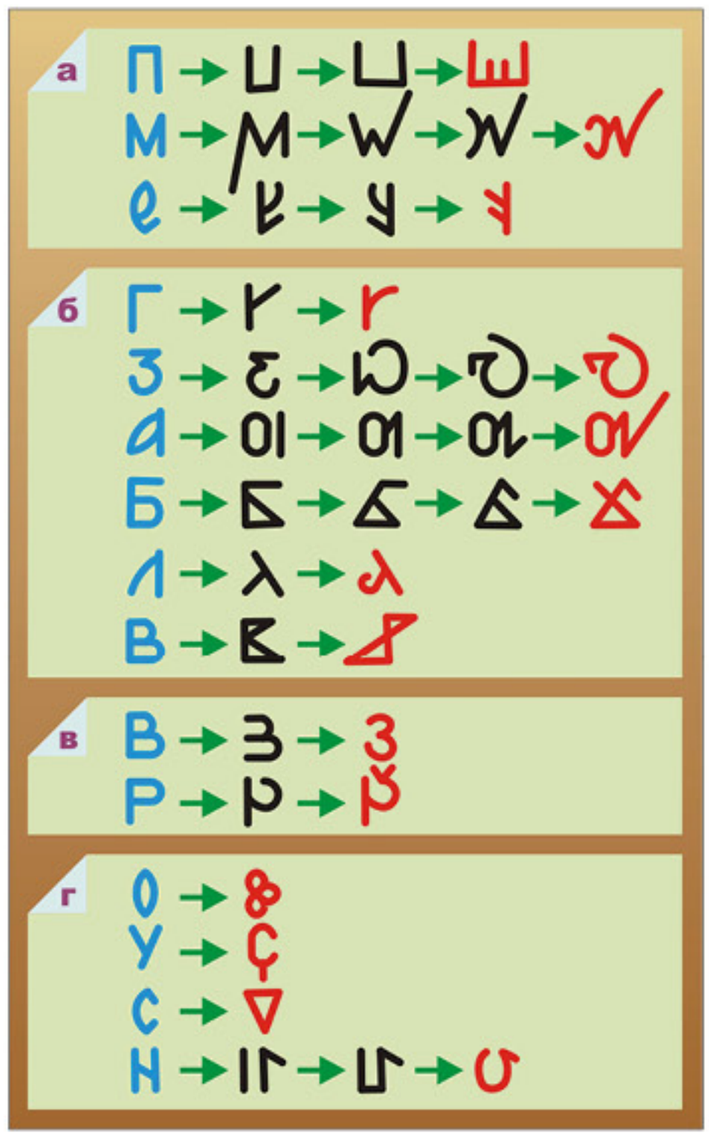


Рисунок 2. Ещё один шифр пропорциональной замены инока Луки

Рисунок 3. Шифр простой замены инока Луки

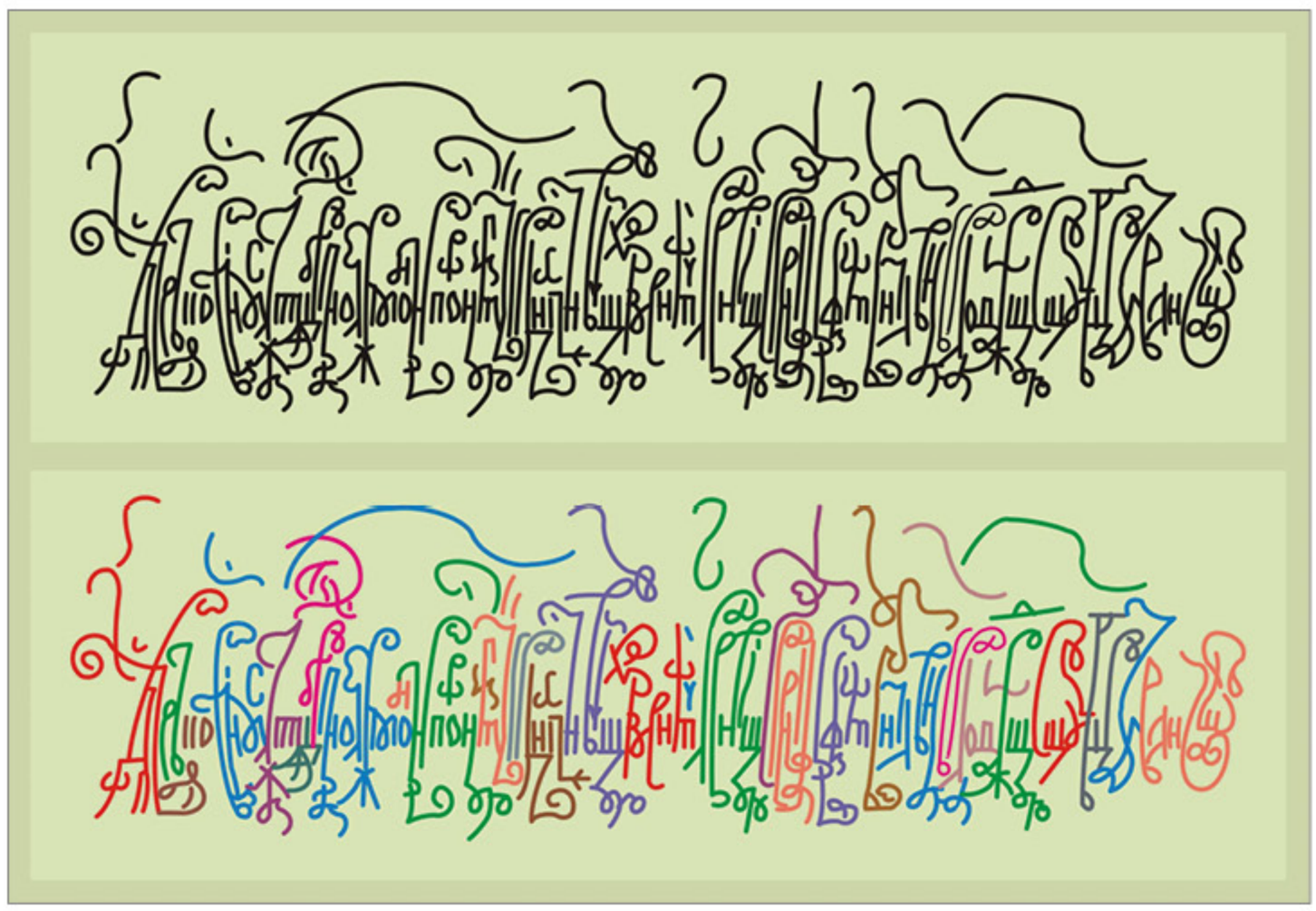


Рисунок 4. Образец надписи вязью

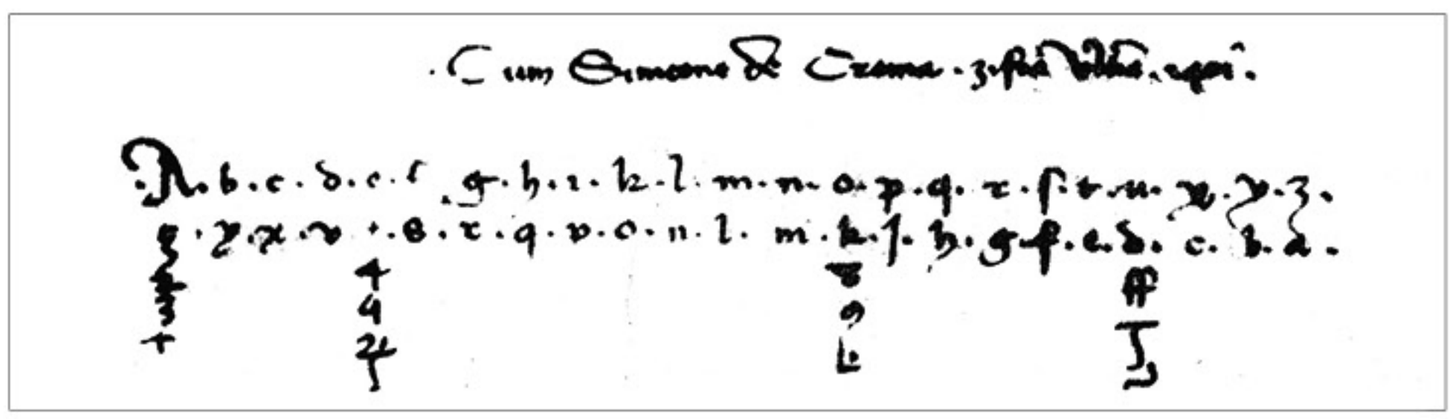


Рисунок 5. Один из первых итальянских шифров пропорциональной замены

шифр, в котором для гласных букв имелись по нескольку шифробозначений. Для одной буквы обычно использовали от 2 до 4 замен (рис. 5). Тот факт, что замена применялась именно для гласных букв, наиболее часто встречающихся, свидетельствует о знании криптоаналитических методов, основанных на частоте встречаемости знаков шифртекста. Это первый подобный шифр, дошедший до нас, хотя, по некоторым сведениям, подобные шифры стали применяться в Италии несколько ранее — с 1390-х годов [Kahn, 1967].

Таким образом, инок Лука использовал, а возможно и разработал прогрессивный для того времени шифр пропорциональной замены, имевший гораздо большую стойкость, чем господствовавшая тогда простая замена, одновременно с итальянцами, а то и раньше. А ведь итальянские города-государства имели на своей службе лучших на тот момент криптографов в Европе, а может быть и в мире[1].

Заканчивая рассказ об иноке Луке, следует отметить, что он в одной книге показал примеры использования различных шифров и первым на Руси опубликовал описание шифра пропорциональной замены. После этого простая замена в различных её вариантах ещё более 300 лет оставалась основным шифром в нашем Отечестве.

ИВАН III ВАСИЛЬЕВИЧ

Одним из великих правителей Московской Руси был Иван III Васильевич, занимавший престол с 1462 по 1505 год. Он первым стал подписываться как Государь и Великий князь всея Руси и именно при нём завершился период татаро-монгольского ига (знаменитое Стояние на реке Угре, 1480 г.).

Иван III проводил активную внешнюю политику. При нем были установлены дипломатические отношения с папской курией, Венгрией, Молдавией, Турцией, Персией, рядом германских государств, Крымским ханством. Эта бурная деятельность сопровождалась обильной перепиской, в том числе и шифрованной. Следует отметить, что

[1] О достижениях криптографов Китая и Индии этого периода известно очень мало. Тема практически не изучена и заслуживает серьёзных исследований.

Рисунок 6. Великий князь Московский с 1462 г. по 1505 г. Иван III Васильевич (22.01.1440–27.10.1505) на Памятнике «1000-летие России» в Великом Новгороде. У его ног побеждённые литовец, татарин и ливонский немец

Рисунок 7. Софья Палеолог

учреждения, координирующего дипломатическую деятельность, тогда ещё не существовало и руководил дипломатами «непосредственно сам государь с думой» [Очерки, 1999. С. 24].

Огромным дипломатическим успехом Московского государства стала свадьба Ивана III с племянницей последнего византийского императора Константина Палеолога — Софией. Сам император погиб при взятии Константинополя турками в 1453 году, но у него остались два брата Димитрий и Фома. Первый стал служить турецкому султану, а второй отправился в Рим, где нашёл покровительство Папы Римского Пия II и кардиналов. У Фомы было трое детей — два сына и дочь, которые после смерти отца, продолжали пользоваться гостеприимством нового Папы Павла II [Карамзин, 2018].

Вскоре Папа стал искать своей подопечной жениха, но это оказалось непросто, царевна категорически отказывалась выходить за католика. В результате «к удивлению многих, Павел обратил взор на Великого Князя Иоанна» [Карамзин, 2018]. В Москву прибыл посол с предложением руки Софии. Предложение было принято, и в январе 1472 года из Москвы выезжает посольство, чтобы привезти невесту на Русь.

Хотя на Руси, а тем более в Риме, уже не только знали, но и применяли шифры, Иван III прибег к более радикальному средству защиты столь важной для него информации — её отсутствию в письменном виде. Послам была дана лишь верительная грамота, а все переговоры должны были вестись исключительно устно.

С грамотой произошёл казус. Пока послы собирались в дорогу, Павел II умер, в Москву поступила информация, что его преемника будут звать Калист, на него и составили грамоту. В пути выяснилось, что новым Папой будет Сикст. В Москву возвращаться не хотелось, и послы просто подчистили имя Калиста, вставили на его место Сикста и поехали дальше. В «окончательном» варианте грамота выглядела так: «Сиксту, Первосвятителю Римскому, Иоанн, Великий Князь Белой Руси, кланяется и просит верить его Послам» [Карамзин, 2018]. Подделку никто не заметил, и 12 ноября 1472 года София прибыла в Москву, где в тот же день была обвенчана с Великим Князем.

Этот брак был крайне полезен для Русского Государства. В частности, за Софией в Москву потянулись византийские греки, многие из которых обладали крайне полезными знаниями и способностями, в том числе в области дипломатии и криптографии [Столпаков, 2016. С. 24]. Из Италии приехали зодчие (построившие впоследствии Кремль и многое другое), пушечных дел мастера и т.п. Кстати в качестве своеобразного «приданного» России достался и её нынешний герб — двуглавый орёл.

Во второй половине XV века Иван III старался установить союзные отношения с Крымским ханством. На то имелся общий противник — Большая Орда, возникшая на обломках Золотой Орды и возглавляемая ханом Ахматом. В Крым отправлялись послы, принимались делегации оттуда. Эта деятельность сопровождалась обильной шифрованной перепиской. Но Иван III оставался верен себе, самая секретная информация передавалась устно, с помощью курьеров.

ПЕРЕХВАТ ИНФОРМАЦИИ

При Иване III зафиксированы и многочисленные факты организации перехвата информации противника. Причём противник этот был внутренний.

В 1470-х годах новгородская знать решила перейти под власть польского короля Казимира IV. Новгородцы и поляки посылали друг к другу гонцов с посланиями для обсуждения вопросов ухода Новгорода под польскую корону. Один из гонцов был перехвачен, и Иван III, узнав о предполагаемой измене, в январе 1480 года двинулся на Новгород с войском. Новгородцы сопротивления не оказали, русские войска заняли город и вернули его под власть Великого Князя [Бабаш, 2002], [Кудрявцев, 2002].

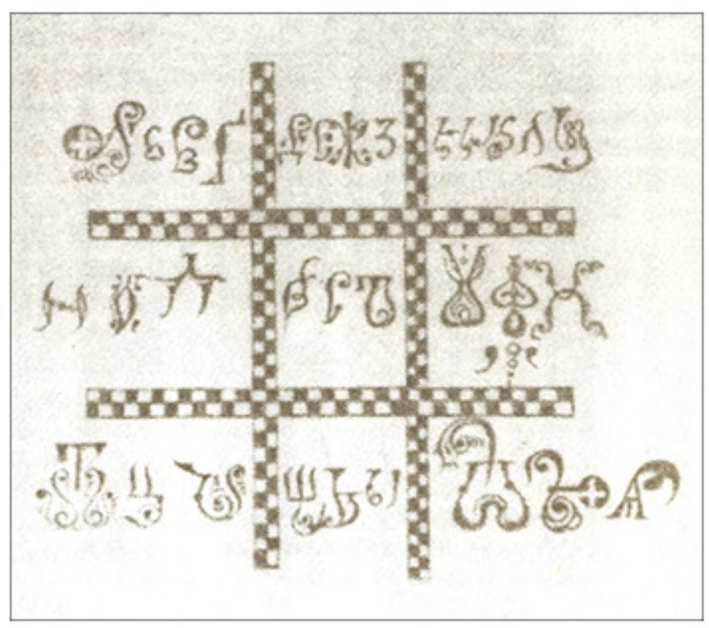


Рисунок 8. Открытый текст геометрической системы простой замены

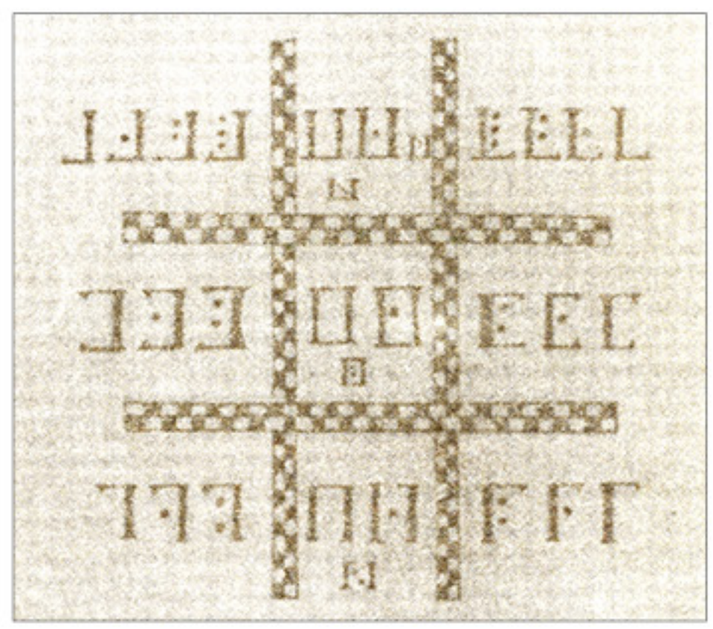


Рисунок 9. Шифрованный текст геометрической системы простой замены

ФЁДОР КУРИЦЫН

Во время правления Ивана III одним из выдающихся дипломатов был посольский дьяк Фёдор Васильевич Курицын. В 1482–1484 гг. он был послан в Молдавию и Венгрию для ведения переговоров с их правителями Стефаном Великим и Матфеем Корвиным о союзе против Польско-Литовского государства. Возвращаясь после выполнения этой миссии, был задержан турками в захваченном ими Белгороде (Днестровском), но благодаря посредничеству крымского хана вернулся в Москву. В 1480–1490-х гг. играл виднейшую роль в политике Ивана III.

Курицын активно поддерживал внука Ивана III Дмитрия (ставшего наследником[2] престола после смерти своего отца, старшего сына Ивана III); в 1497 г. Курицын скрепил грамоту Ивана III и Дмитрия, на которой впервые появился новый герб Русского государства — двуглавый орёл. Когда началась война с Польско-Литовским государством именно Курицын изложил противникам ультимативные требования Ивана III. Но в 1502 г. подверглись опале Дмитрий-внук и его мать Елена Стефановна, после чего был отстранён от дел и Ф. Курицын. В чём причины такого поворота событий?

Дело в том, что Ф. Курицын играл важнейшую роль в истории новгородско-московской ереси; он возглавлял московский еретический кружок, образованный примерно в 1485 г., когда Курицын вернулся из-за границы. Обличитель ереси, архиепископ Геннадий Новгородский, уже в 1480-х гг. именовал его «начальником» еретиков. Тем не менее долгое время московских еретиков не трогали, основные усилия Церкви были направлены на новгородских еретиков. Но в ноябре 1504 г. церковный собор осудил и московских и новгородских еретиков. Иван III решил использовать опыт испанской инквизиции («шпанского короля») и отправил осуждённых на костёр. Среди них был брат Курицына Иван-Волк Курицын, но сам Фёдор Васильевич даже не упоминался в делах собора и остался жив. Тут, видимо, сказались его дипломатические заслуги, однако к государственным делам его больше не допускали. Возможно, он тихо дожил свой век, пребывая в опале.

ГЕОМЕТРИЧЕСКИЕ ШИФРЫ

Ф. Курицын является автором ряда литературных произведений, наиболее известное из которых «Лаодикийское послание» — философско-теологический труд, частично выполненный в стихах. Для нас это произведение интересно тем, что многие страницы в нём зашифрованы шифром простой замены, известным как «литореи в квадратах». В послании же приведён и образец ключа к шифру и инструкция по его использованию.

«Литореи в квадратах», или как ещё называются подобные шифрсистемы — геометрические шифры, представляет собой замену букв открытого текста угольниками и четырёхугольниками, заимствованными из решётки, составленной из двух параллельных линий, пересечённых двумя такими же линиями под прямым углом. В полученных клетках помещено по четыре и по три буквы в порядке азбуки: в тайнописи буквы заменяются, при этом первая — простым угольником, а следующие — тем же угольником с одной, двумя или тремя точками, смотря по месту буквы в нём.

На рис. 8 приведён открытый текст подобной системы, а на рис. 9 — шифрованный. Вместе они составляют ключ к шифру.При этом свою подпись к произведению Фёдор Курицын зашифровал простой литореей. Этот шифр мы описали в предыдущей статье. Очевидно, что, зная вышеупомянутые принципы шифрования, Ф. Курицын использовал их не только в своей литературной, но и в дипломатической деятельности.

Вышеупомянутый брат Ф. Курицына — Иван-Волк Курицын — так же известен как дипломат. В частности, он вёл переговоры о приглашении на русскую службу немецкого печатника В. Готана, не раз ездил за границу и также был еретиком. Он является автором книги «Мерило Праведное», состоящей из поучений о праведных и неправедных судах. Подпись к книге «Иванъ Волкъ Курицинъ» была зашифрована цифровой тайнописью [Словарь, 1988].

Кстати, геометрические шифры впоследствии часто использовались тайными обществами, наиболее известными из которых были масоны. Шифр даже получил название «масонский ключ» или «масонский крест». Считалось, что форма креста придаёт шифру дополнительную стойкость. Интересный факт: подобные шифры использовал Наполеон и его генералы.

[2] Но в конце концов престол занял ещё один сын Ивана III, он стал Великим князем Василием III

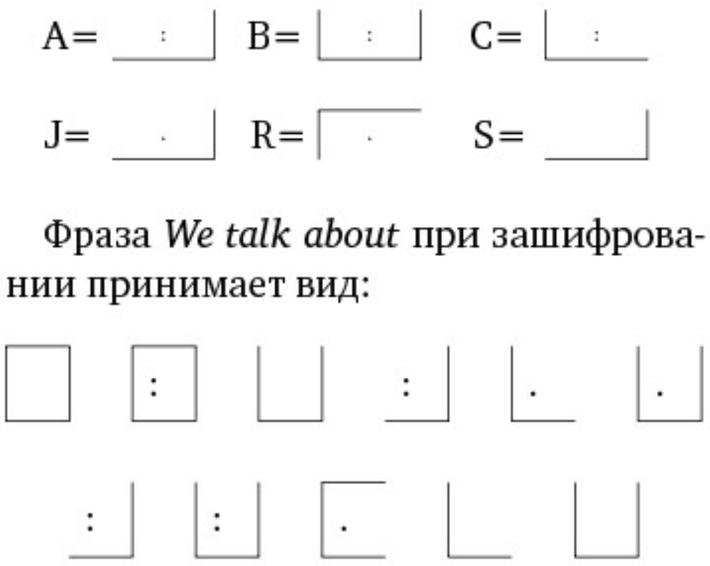
Приведём пример на английском языке. Нарисуем три фигуры [Бабаш 2002, с. 75]:

A:	B:	C:
D:	E:	F:
G:	H:	I:

J.	K.	L.
M.	N.	O.
P.	Q.	R.

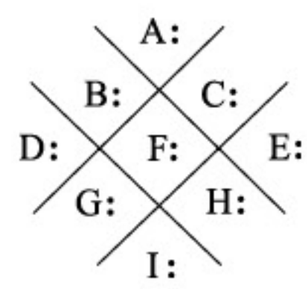
S	T	U
V	W	X
Y	Z	

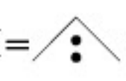
В соответствии с этими фигурами буквы получают следующее геометрическое представление:



Фраза *We talk about* при зашифровании принимает вид:

Геометрическое представление может меняться, например:



Тогда A= , D= , I=  и т.д.

ПРО ДРАКУЛУ

В заключение небольшое отступление. Улыбка истории: Фёдор Курицын остался в веках не как выдающийся дипломат и общественный деятель, а как автор первого на Руси художественного литературного произведения. До него все русские книги были «полезными»: летописями, поучениями, религиозными или философскими трудами… Фёдор Васильевич написал первую «неполезную» книгу — для развлечения. Это был сборник сказок и исторических анекдотов о человеке, о котором Курицын услышал во время своего путешествия в Венгрию и Молдавию. Называется книга «Сказания о Дракуле воеводе». Дракула в ней представлен незаурядной личностью, жестоким, но справедливым правителем. Любопытно, что именно с лёгкой руки нашего соотечественника реальный князь Влад Дракул Цепеш, правивший Валахией в середине XV в., начал своё триумфальное шествие по страницам книг, сценам театров, кино- и телеэкранам.

ЛИТЕРАТУРА

1. [Астрахан, 1996] Астрахан В. И., Гусев В. В., Павлов В. В., Чернявский Б. Г. Становление и развитие правительственной связи в России, Орел: ВИПС, 1996.
2. [Бабаш, 2002] Бабаш А. В., Шанкин Г. П. История криптографии. Часть I. М.: Гелиос, 2002.
3. [Гольев, 2008] Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008.
4. [Гольев, 2009] Гольев Ю. И., Ларин Д. А., Шанкин Г. П. Криптография в эпоху Наполеона // Математика для школьников, № 1, М.: 2009, с. 46–55.
5. [Карамзин, 2018] Карамзин Н. М. История Государства Российского. М.: АСТ, 2018 // magister.msk.ru/library/karamzin/kar606, www.historic.ru, www.spsl.nsc.ru/history/karam/kar06–02.htm 30.08.2018.
6. [Кудрявцев, 2002] Кудрявцев Н. А. Государево Око. Тайная дипломатия и разведка на службе России. М., ОЛМА-ПРЕСС, 2002.
7. [Очерки, 1999] Очерки истории внешней разведки в 5 томах, под ред. Е. М. Примакова и С. Н. Лебедева, М., «Международные отношения», 1999.
8. [Словарь, 1988] Словарь книжников и книжности Древней Руси. Вып. 2 (вторая половина XIV–XVI в.). Часть 1. А-К, Л.: «Наука» 1988.
9. [Соболева, 2002] Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.
10. [Сперанский, 1929] Сперанский М. Н. Тайнопись в юго-славянских и русских памятниках письма. Энциклопедия славянской филологии. Вып. 3–4. Л., 1929.
11. [Столпаков, 2016] Столпаков Б. В., Никонов В. Г. «Чтоб было в тех землях не знатно…». Исторические свидетельства о начале и становлении российской криптографии (XVI–XVII века). Монография. М.: Медиа Группа «Авангард», 2016.
12. [Тайнопись, 2018] Тайнопись инока Луки — Википедия 20.08.2018.
13. [Kahn, 1967] Kahn D. The codebreakers. N- Y: Macmillan Publ. Co., 1967.

Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-математических наук

Александр II в рабочем кабинете. 1880 год

ВРЕМЯ РОСТА

РОССИЙСКАЯ ИМПЕРИЯ ВО ВТОРОЙ ПОЛОВИНЕ XIX ВЕКА. К 200-ЛЕТИЮ СО ДНЯ РОЖДЕНИЯ ИМПЕРАТОРА АЛЕКСАНДРА II

29 апреля исполнилось 200 лет со дня рождения российского императора Александра II, погибшего от рук террористов в 1881 году. В историю он вошёл как Царь-Освободитель. С его именем связана и отмена крепостного права, и освобождение болгарского народа от многовекового владычества Турецкой империи.

ВРЕМЯ ВЕЛИКИХ РЕФОРМ

Александр II начал своё императорское служение в тяжёлые дни Крымской войны, когда решалась судьба обороны Севастополя. Во время его правления подданным пришлось пережить немало драматических моментов и решительных жизненных перемен. Новый император продолжил модернизацию империи, начатую его отцом, Николаем I. Но она была дополнена великими реформами, глубоко затронувшими все стороны жизни государства и общества.

ФСРБИТ

Материалы рубрики «История» публикуются при поддержке Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)

Общество, как известно, реагирует на перемены либо достижениями, либо упадком культуры. С какими именами связано время правления Александра II! Л. Н. Толстой и И. С. Тургенев, ровесник Александра II, у него тоже в нынешнем году 200-летие со дня рождения. Ф. М. Достоевский и П. И. Чайковский, А. П. Бородин и М. П. Мусоргский, В. М. Васнецов и А. К. Саврасов, И. Е. Репин и многие, многие другие.

В числе первых подверглась реформированию финансовая система государства. Государственный коммерческий банк в 1860 г. был реорганизован в первый российский Государственный банк. Санкт-Петербургский частный коммерческий банк стал первым акционерным банком России. Его правление возглавил Г. П. Елисеев, один из основателей торгового дома «Братья Елисеевы». Банк основали в 1864 г. с целью кредитования торговых сделок на Петербургской бирже. А в Москве с 1866 г. начал действовать Купеческий банк. Период с 1862 по 1872 год считается временем непрерывного развития банковского дела в России. В этот период заявили о себе 33 акционерных и 11 акционерно-земельных банков, в 1873 г. действовали уже 222 городских общественных банка.

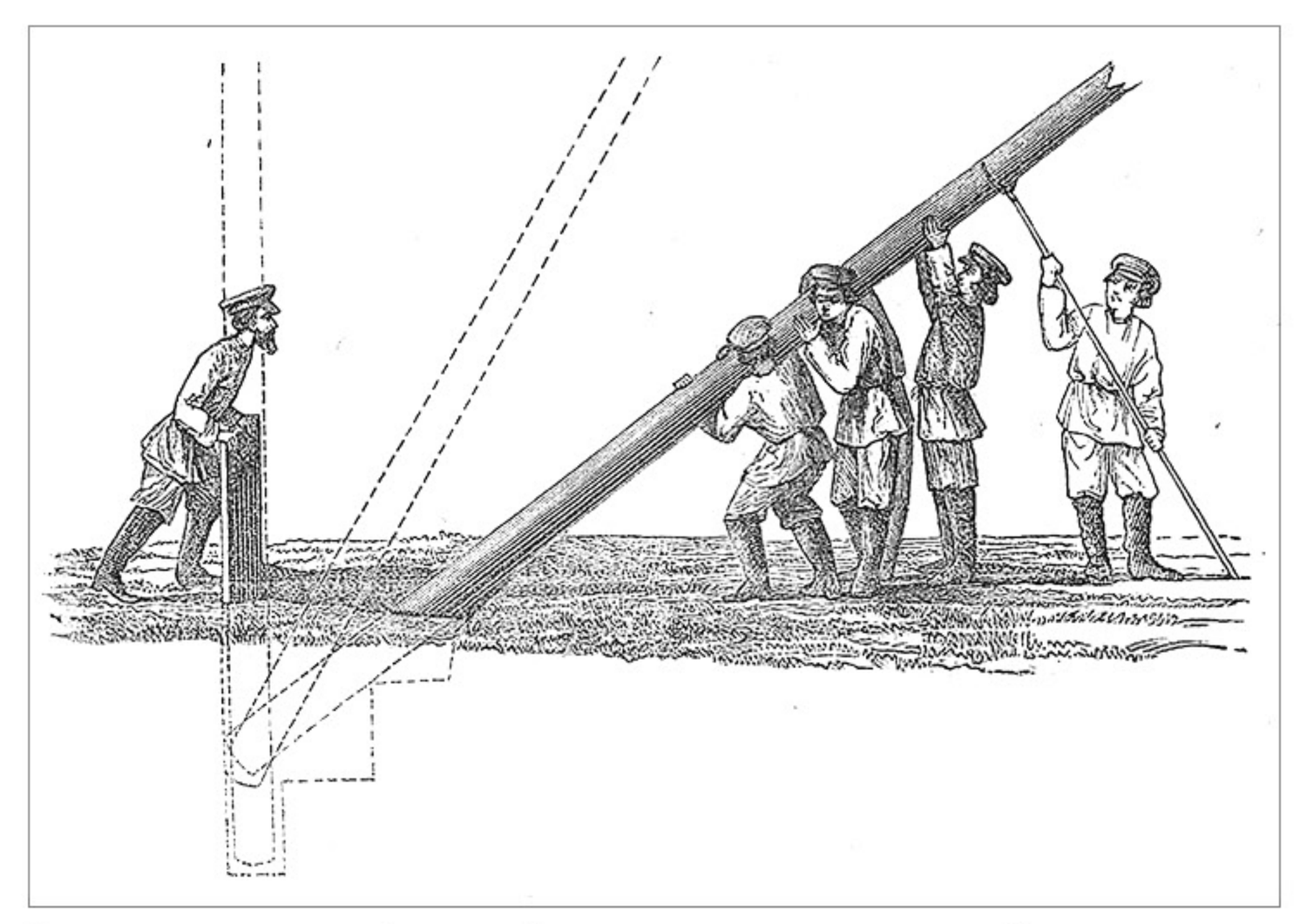


Схема установки телеграфных столбов из технического руководства Сименс

ОСОБОЕ ВНИМАНИЕ РАЗВИТИЮ ТРАНСПОРТА И СВЯЗИ

Реформа банковской системы позволила организовать финансирование развития транспорта и связи. При Александре II в России интенсивно строились железные дороги и телеграфные линии связи. Если к 1860 г. железнодорожная сеть России имела протяжённость около 1600 км, то к 1875 г. было проложено уже свыше 20 тыс. км железных дорог, в год сдавали в использование около 1,25 тыс. км.

Не менее активно велось телеграфное строительство. Сразу после вступления на престол Александр II принял решение о немедленном начале строительства телеграфной линии из Николаева в Крым. В течение лета 1855 г. фирма «Сименс и Гальске» в невероятно сложных условиях организовала работы по сооружению этой линии связи с центром военных действий. «О трудностях, которые нам приходилось преодолевать…, — вспоминал спустя годы В. Сименс, — можно составить себе понятие, если принять в соображение, что все необходимые материалы, исключая деревянных телеграфных столбов, приходилось получать из Германии, что в России тогда не было никаких других железных дорог, кроме линий из Варшавы к прусской границе и из Петербурга в Москву, и что все пути заняты были военными обозами… Доставление нужных материалов из немецких гаваней было чрезвычайно затруднено блокадой русских портов английскими крейсерами».

Симферополь был присоединён к российской телеграфной сети 19 сентября 1855 г. К сожалению, до Севастополя работникам В. Сименса тогда дойти не удалось. 30 августа 1855 г. Александру II доставили только что полученную из Крыма через Николаев телеграмму генерала М. Д. Горчакова: «Войска переходят на Северную сторону… Враг найдёт в Севастополе одни только окровавленные развалины».

Если в конце царствования Николая I, к весне 1855 г., протяжённость телеграфных линий составляла 2 тыс. км, то к 1 января 1857 г. она достигла уже 7,5 тыс. км. К 1870 г. телеграфная линия была проложена до Хабаровска, в 1871 г. — до Владивостока, в 1881 г. — на Сахалин. От этой основной магистрали протянулись местные линии на север и на юг. Всего в течение царствования Александра II в Российской империи было построено более 83 тыс. км телеграфных линий. За это же время было открыто около 1100 правительственных телеграфных станций. Кроме того, приём депеш общей корреспонденции был открыт на почти 1500 телеграфных станциях железных дорог. Для работы на российских телеграфах были подготовлены многие тысячи специалистов. О развитии телеграфа свидетельствуют и данные о росте телеграфных услуг. Так, в 1880 г. во всех телеграфных учреждениях империи было обработано более 33 млн телеграмм. Для сбора и передачи текущей информации о политических событиях и событиях в экономике в 1866 г. в Петербурге было создано «Русское телеграфное агентство», переименованное затем в «Российское телеграфное агентство».

К. В. ЧЕВКИН — ОРГАНИЗАТОР СТРОИТЕЛЬСТВА ЖЕЛЕЗНЫХ ДОРОГ И ТЕЛЕГРАФНЫХ ЛИНИЙ

Создание железнодорожной и телеграфной отраслей народного хозяйства России неразрывно связано с трудами гене-

рала К. В. Чевкина и возглавлявшегося им с октября 1855 г. Главного управления путей сообщения и публичных зданий. Вступив в должность, он обратился к своим подчинённым со словами: «Народный голос, т.е. народная совесть, обвиняет ведомство путей сообщения. Пути сообщения составляют везде коренную потребность жизни государственной и частной; но в России, при значительности её протяжений и суровости климата, потребность эта ощутительнее, и среди нынешних военных обстоятельств она выражается ещё разительнее по тесной связи её с обороною пределов Империи, столь нуждающихся в частых и удобных сношениях с внутренними областями. Поэтому, более чем когда-либо, мы все обязаны усугубить старание ко всемерному улучшению, умножению, упрощению сих сношений. Удобства и дешевизна путей сообщения — вот прямая цель управления оных. Призываю всех чинов сего управления, от старших до младших, сохранять постоянно в виду, при всех служебных действиях, эту главную цель, и стремиться непрестанно к достижению оной» [1].

Сравнительно небольшому штату сотрудников ведомства под руководством Константина Владимировича Чевкина удалось организовать строительство путей и станций часто в труднодоступных местностях, обучить многие тысячи работников новому для них делу, обустроить их труд и быт, обеспечить всем необходимым. При поддержке К. В. Чевкина с 60-х годов в железнодорожное и телеграфное строительство активно включаются российские предприниматели, хотя первоначально это строительство вызывалось прежде всего военно-государственными интересами. К. В. Чевкин добился постепенного освобождения российской телеграфии от полного контроля со стороны фирмы «Сименс и Гальске». Кроме того, он отдал много сил развитию и поддержанию в рабочем состоянии сети внутренних водных путей и шоссейных дорог.

И ещё, казалось бы, неожиданное приложение энергии К. В. Чевкина. Он заведовал сооружением двух замечательных памятников. Открытие первого из них — памятника императору Николаю I по проекту архитектора Монферрана состоялось в Петербурге в июне 1859 г.

Второй памятник был воздвигнут в память исполнившегося в 1862 г. тысячелетия исторического существования России. Ещё в 1860 г. объявили конкурс для проектов памятника. Из 52 соискателей проект скульптора Микешина был удостоен окончательного одобрения. Местом для постановки памятника стала площадь в Новгородском Кремле, перед Софийским собором. Памятник открыли в августе 1862 года.

ТРУД КРИПТОГРАФОВ В ЭПОХУ ТЕЛЕГРАФНОЙ СВЯЗИ

Возвращаясь к телеграфной теме, отметим, что такое замечательное средство связи немедленно стало использоваться для передачи зашифрованных депеш. С развитием средств связи расшифровка посланий, передававшихся по телеграфу, быстро приобрела большое значение. В исследовании известного историка В. С. Измозика «Чёрные кабинеты» [2] содержатся интересные сведения о труде российских криптографов того времени. Так, в докладе императору Александру II министр иностранных дел А. М. Горчаков 29 октября 1856 года отмечал, что распространение телеграфных сообщений «даёт обширное поприще деятельности цифирных экспедиций и уже теперь, удесятерив их работу, может дойти впоследствии до чрезвычайных, ещё невообразимых размеров». В МИДе тогда имелись три отделения (экспедиции), связанные с криптографией: шифровальное, дешифровальное и газетное (перлюстрация). Показатели дешифровального отделения по работе с телеграммами за 1873–1882 годы приведены в Таблице 1.

«Руководитель дешифровального отделения тайный советник Л. П. Иессен, занимавшийся этой работой с 1863 г., писал в январе 1883-го, что обязательной чертой криптографа является «в эпохи критические… непрестанная напряжённость всех умственных сил и способностей, усидчивость вполне антигигиеническая, денно и нощно». И далее вспоминал эпизод из собственной биографии в период франко-прусской войны 1870 года, когда он «с Иванова дня [24 июня] по ноябрь месяц работал… без исключения одного дня, по 14 часов в сутки», что «не преминуло ускорить во мне проявление признаков поколебленного здоровья» [2].

Портрет К. В. Чевкина. Неизвестный художник

Такая работа требовала, безусловно, материальных льгот. Должность старшего чиновника по оплате и пенсионному обеспечению была отнесена ко второму разряду (из девяти) и уступала только высшим должностям империи. Младшие чиновники, составлявшие основной штат, получали обеспечение по третьему разряду.

Количество входящих телеграмм	21107
Количество разобранных телеграмм	8062
Процент разобранных телеграмм	38%
Среднее число служащих	3,3
Среднее число разобранных телеграмм на одного служащего	2442

Таблица 1. Показатели дешифровального отделения по работе с телеграммами за 1873–1882 годы

Кроме того, за каждый отдельно разобранный дипломатический шифр полагалось вознаграждение, которое в 1860–1880-е годы составляло от 200 до 800 р. Сумму вознаграждения определял секретный Цифирный комитет, куда выполненная работа представлялась во всех подробностях. Заметим, что месячный оклад армейского поручика тогда равнялся 45 рублям.

Как правило, чиновники цифирных экспедиций служили там долгие годы. Относительно жилищного вопроса шестой пункт Положения гласил: «Принимая во внимание, что занятия старшего и младших чиновников… требуют уединения и совершенного отвлечения от посторонних влияний, им назначаются квартиры в здании Министерства и, по возможности, всем в одном и том же доме» [2].

НОВЫЙ ВЫЗОВ ДЛЯ РОССИЙСКИХ КРИПТОГРАФОВ

Во второй половине XIX столетия чиновникам дешифровального отделения пришлось отвечать на новый вызов. В ту пору, как мы знаем, по Европе уже бродил «призрак коммунизма», имевший постоянное место жительства в Лондоне. И в России тоже происходил рост антиправительственных настроений, особенно среди молодёжной части интеллигенции, чему способствовала либерализация правил выезда за границу. Члены пока ещё немногочисленных тайных организаций довольно скоро стали использовать шифрованную переписку. Контроль полиции позволял перехватывать значительную её часть. Но далеко не всегда удавалось вскрыть шифр и эффективно использовать письма в следственных действиях. В таких случаях по указанию императора Александра II нерасшифрованные письма могли передавать специалистам МИДа.

Тогда получили распространение так называемые книжные шифры. На рис. 1 приведен пример такого шифра в реальном перехваченном письме 1863 года [3]. По указанию императора письмо с этим шифром было передано в МИД.

10 января 1864 года министр иностранных дел А. М. Горчаков в секретном ответе в МВД указал:

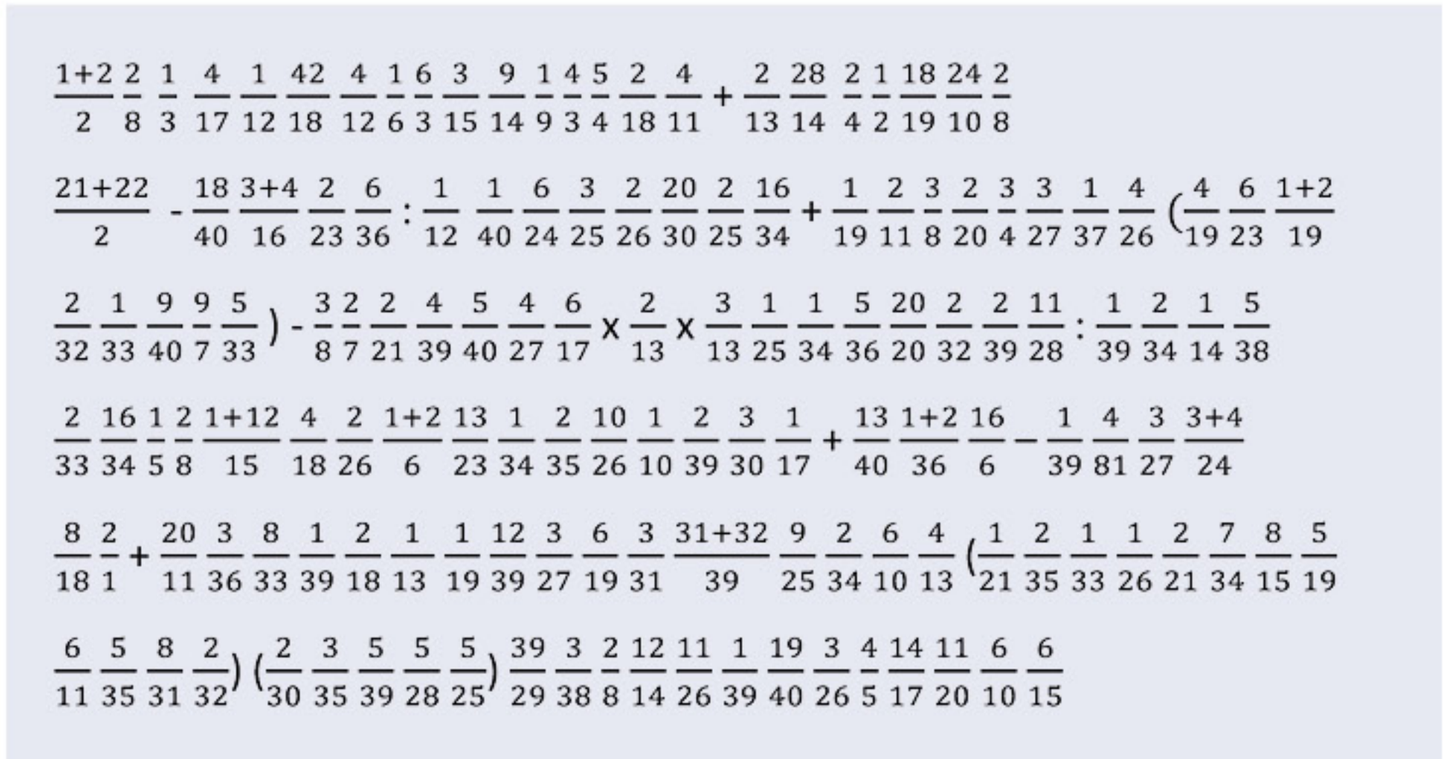


Рисунок 1. Пример книжного шифра

«Я приказал подвергнуть тщательному рассмотрению препровождённое ко мне шифрованное письмо …, но, несмотря на все старания и особенные способности специалистов по этой части, никакого смысла, по недостатку материалов, добиться было невозможно» [3].

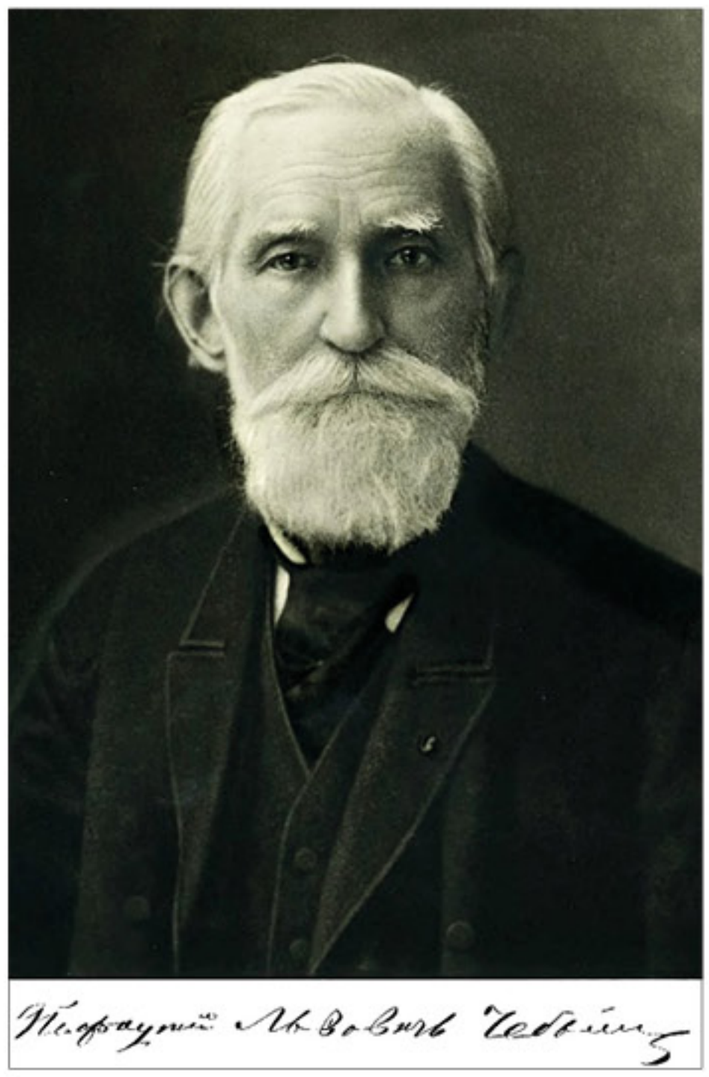
РОСТ АВТОРИТЕТА РОССИЙСКОЙ НАУКИ

Ко второй половине XIX столетия Россия уже давно была интегрирована в культурную жизнь Европы. Достижения в науке, технике и образовании легко преодолевали границы. Пользовались успехом многочисленные научные и отраслевые технические журналы. Если раньше такая литература печаталась на французском и немецком языках, то с середины века в России приступили к изданию научных журналов на русском языке. Активизировались связи между учёными. В 1867 г. в Петербурге собрался Первый Всероссийский съезд естествоиспытателей и врачей, второй съезд состоялся уже через два года в Москве. Подобные и отраслевые форумы стали регулярными. Получившие мировую известность И. М. Сеченов, П. Л. Чебышёв, Д. И. Менделеев и многие другие учёные создавали авторитет российской науке. Общей тенденцией стала организация научных обществ по математике, физике, химии и другим отраслям знания. Московское математическое общество по времени открытия даже опередило такие же общества в Лондоне и Париже.

П. Л. ЧЕБЫШЁВ — НЕУСТАННЫЙ ТРУД НА БЛАГО ОТЕЧЕСТВА И МИРОВОЕ ПРИЗНАНИЕ

Пафнутий Львович Чебышёв деятельно участвовал в создании и стал активным членом Московского математического общества. Именно с П. Л. Чебышёва, как создателя крупной научной школы, началась непрерывная череда выдающихся достижений российских математиков. Выпускник Московского университета, действительный член Петербургской академии наук, он много лет совмещал преподавание математики в Петербургском университете с неустанным трудом на других поприщах.

Великий математик и основоположник современной картографии. Разработчик бронебойных снарядов для крепостной артиллерии Кронштадта и создатель разнообразных механических устройств. Среди них оригинальный арифмометр, инвалидная коляска и стопоходящая машина, представленные на всемирных выставках в Париже и в других городах мира. Государственный деятель, член Военно-учёного комитета и член Учёного комитета Министерства народного просвещения, с чьим именем связана система естественно-научного и инженерного образования, сложившаяся в России во второй половине XIX столетия. Возникшая тогда острейшая потребность в квалифицированных технических кадрах поставила российскую власть перед необходимостью значительного наращивания числа подготавливаемых инженеров.



Пафнутий Чебышёв

Вскоре появилось предложение обучать инженеров на физико-математических факультетах университетов. П. Л. Чебышёв выступил против этого предложения, считая более целесообразным сосредоточить подготовку инженеров в высших технических учебных заведениях, а в университетах готовить специалистов по фундаментальным наукам. По пути создания большого количества технических вузов разного профиля пошла и российская высшая школа. В нынешнем году отмечается 150-летие создания Московского высшего технического училища — одного из признанных лидеров отечественного инженерного образования. Занимаясь народным просвещением, Пафнутий Львович добивался увеличения окладов преподавателей, разрабатывал программы математического образования для средних и высших учебных заведений. Он обосновывал и отстаивал необходимость знакомства старшеклассников с понятиями комбинаторики, дифференциального исчисления и аналитической геометрии.

Научные труды Чебышёва ещё при его жизни получили широкое признание как в России, так и за границей. Он получил много наград. Повсюду, в академиях наук, научных обществах, университетах он был избран почётным членом. В 1874 году его избрали действительным членом Парижской академии наук — первым из российских учёных в XIX столетии. Ему писали из Парижа, что французские математики считают его величайшим аналитиком столетия и преемником К. Гаусса. В 1890 г. по предложению Парижской академии наук президент Франции наградил Чебышёва командорским крестом ордена Почётного легиона. По поводу этой награды президент Парижской АН Шарль Эрмит написал в письме к Чебышёву следующее:

«Мой дорогой собрат и друг! Командорский крест Почётного легиона, который был Вам пожалован президентом республики является лишь небольшой наградой за великие и прекрасные открытия, с которыми навсегда связано Ваше имя и которые давно уже выдвинули Вас в первые ряды математической науки нашей эпохи. Все члены Академии воспользовались случаем засвидетельствовать ту горячую симпатию, которую Вы им внушаете. Все они присоединились ко мне, заверяя, что Вы являетесь гордостью науки в России, одним из первых геометров Европы, одним из величайших геометров всех времён».

Заметим, здесь Чебышёв именуется выдающимся геометром ещё и в согласии с древней традицией, когда то, что мы сейчас именуем математикой, связывалось прежде всего с геометрией. А под математикой понимали учение, включающее в себя магическую астрологию. Современники отмечали высокие человеческие достоинства П. Л. Чебышёва. В памяти учеников сохранились его слова, которым он сам неизменно следовал: «Честь дороже прибытка». Через три года, в 2021 году, исполнится 200 лет со дня рождения этого великого сына России.

А в нынешнем году, вспоминая, в связи с юбилеем императора Александра II, достижения России, мы должны отметить, что достигнутый в годы его правления рост культуры, образования и науки не ослабевал и при императорах Александре III и Николае II. Российские учёные и инженеры прочно утвердились на передовых позициях в мире. Общеизвестны российские корни самых громких достижений в области электротехники, радио, телевидения, авиации. Это следствие больших государственных вложений в образование. Так, расходы на народное образование составили в 1913 году почти 19% от всех расходов государства. Начальное образование было бесплатным и с 1908 года стало обязательным. Число студентов за 20 лет выросло в 3 раза и составило в 1913 году 80 тысяч человек.

* * *

Упомянем ещё одно важное событие. В 1896 году в Нижнем Новгороде была проведена Всероссийская выставка. Для рабочих и учащейся молодёжи не только вход на неё был бесплатным, но и проезд по железной дороге от места жительства и обратно. Такой льготой воспользовались 282 тысячи человек. Все эти действия, начавшиеся с реформ императора Александра II, позволили значительно расширить социальную базу грамотности и образованности в России. Показательно, что уже в конце 1915 года контингент краткосрочных офицерских курсов, призванных восполнить убыль фронтовых командиров, на 80% состоял из лиц крестьянского происхождения [4].

ЛИТЕРАТУРА

1. Русский биографический словарь А. А. Половцова. Чевкин К. В. Спб., 1912.
2. *Измозик В. С.* Чёрные кабинеты. НЛО. М., 2015.
3. РГВИА, ф.801.
4. *Головин Н. Н.* Военные усилия России в мировой войне. М., 2001.

Александр БОДРИК
вице-президент по ИБ ISACA Moscow, CISA, ITIL Expert

УРОКИ УПРАВЛЕНИЯ СТРАТЕГИЧЕСКИМИ ПРОЕКТАМИ

ЗАМЕТКИ БЕЗОПАСНИКА

Классическое китайское проклятье «Чтоб Вам жить в эпоху перемен!» актуально и по сей день. Иногда, казалось бы, и перемены позитивные, а новые проекты приносят больше проблем, чем пользы. К числу таких проектов относятся так называемые «стратегические проекты», которыми руководят члены правления и курируют руководители организаций.

Примером такого проекта для информационной безопасности может служить аудит информационной безопасности при поглощениях и слияниях (M&A). В таких проектах нет ни чёткого ТЗ (задачу ставит бизнес, мало понимающий в ИБ), ни строгих стандартов, а значит, присутствует весь спектр проектных рисков: объём, сроки, ресурсы и качество. За проектом также следит правление организации, и любой косяк может стать поводом для кадрового решения.

ПРОЕКТНЫЕ РИСКИ

Объём. Отсутствие ТЗ означает возможность бесконечного раздувания объёма работ, а через них — требуемых ресурсов и качества проекта. Противостоять этому можно с помощью формирования т.н. «экспертной позиции» — организация и внутренний заказчик должны принимать изначальное превосходство специалиста по ИБ в своей теме. Помогают утвердить экспертную позицию участие в профессиональных ассоциациях, публикации в СМИ, наличие профессиональных сертификатов (ISACA, ISC 2, ITIL) и сильные soft skills.

Проектные сроки. В стратегических проектах желательно установить рабочий ритм — регулярные встречи по проекту + иные регулярные проектные действия. Например, сбор обратной связи от клиента, подготовка и отправка отчётности по проекту с чёткими этапами, плановыми, фактическими и прогнозными сроками, перечнем проектных рисков и проблем (реализовавшихся рисков).

Желательно использовать и современные инструменты коммуникации: выделенные чаты в мессенджерах (WhatsApp, Slack и т.п.), постановщики задач («тудушники»).

В случае отсутствия члена команды более чем на день-два, необходимо передать задачи по стратегическому проекту другому участнику. В частности, объяснить задачи (провести инструктаж), передать проектные артефакты (документы) и познакомить с ключевыми участниками проекта. Ещё лучше — изначально назначить каждому участнику проекта заместителя (back-up).

Ресурсы. Разнообразие технологий, подходов и практик в ИБ сказывается на разнообразии необходимых ресурсов. Ресурсов постоянно не хватает, а когда они есть, частенько под сомнением оказывается надёжность исполнителей (в разрезе выполнения проектных задач). Ведь именно в стратегическом проекте исполнители должны работать компетентно и ответственно: выдерживать дедлайны и не допускать грубых ошибок («косячить»).

Для выбора исполнителей нужно регулярно измерять их надёжность, и еще до начала стратегического проекта иметь длинную «скамейку запасных» с неким рейтингом по итогам ранее реализованных проектов.

В целях измерения надёжности мы определим её как произведение Компетентности на Ответственность. Для оценки Компетентности и Ответственности применим старую-добрую матрицу (как в анализе рисков ИБ), и используем качественный подход — оценки от 1 до 5. Имея такую матрицу 5×5, мы сможем распределить по ней наших исполнителей. Каждый из них получит числовой вес Надёжности, например, 20 (4 Компетентность × 5 Ответственности). Соответственно мы сможем выбрать для нашего проекта самых надёжных (например, 20% исполнителей с лучшим рейтингом).

ПРОЕКТНЫЕ ВОЗМОЖНОСТИ

Финансовые рынки учат нас, что высокие риски соответствуют более высокому потенциалу доходности, и в стратегических проектах это именно так. Во многих компаниях функция ИБ имеет мало шансов быть упомянутой на уровне правления, и только стратегический проект даёт ей и ее руководителю возможность быть замеченными.

В стратегических проектах жёсткий рабочий ритм и сложные задачи сближают членов команды: завязываются новые полезные знакомства с людьми высокого уровня, сглаживаются старые конфликты и т.д. По итогам завершения такого проекта возможна и выплата отдельной премии, например, из фонда генерального директора.

* * *

Стратегические проекты имеют две стороны. Во-первых, это возможность показать свою эффективность и зрелость как управленца. Во-вторых, продемонстрировать недостаточную для занимаемой должности компетентность. Используя приведённые выше практики, можно повысить вероятность более приятного для профессионалов исхода, и подняться на новый уровень, как минимум с точки зрения профессиональной компетенции и политического влияния в организации.

Международный форум

21-23.11.2018

ALL-OVER-IP

ТОЛЬКО БИЗНЕС - НИЧЕГО ЛИШНЕГО

Генеральный спонсор:

axxonsoft

MEMBER OF ITVGROUP

www.all-over-ip.ru

ИГРАЮТ ВСЕ!

СВОЯ АТМОСФЕРА И «НАША ИГРА»

Медиа Группа «Авангард» запустила новый проект: первое интеллектуальное ТВ-шоу по информационной безопасности «Наша игра». Формат и правила игры хорошо знакомы поклонникам Анатолия Вассермана и передачи «Своя игра». Выпуски «Нашей игры» будут регулярно выходить на Youtube-канале BIS TV. Первую игру можно увидеть уже 15 ноября.

«Наша игра» — это не индивидуальное, а командное соревнование. По правилам, в каждой игре участвуют 3 команды по 5 человек. Команда-победитель выходит в следующую игру серии. Команда, занявшая 2-е место, пропускает 1 игру и затем может вернуться, а проигравшая команда, увы, завершает борьбу. Однако игроки могут снова принять участие в будущих играх в составе новых команд. В 5-й — финальной — игре серии примут участие команды, набравшие больше всего баллов по итогам всех игр.

Если говорить о ходе игры, то особых сюрпризов здесь нет: 2 раунда и финальный вопрос. В каждом раунде разыгрывается 6 категорий по 5 вопросов разной стоимости. В финал выходят команды, имеющие положительный баланс на счете. Особенностью «Нашей» станет тематический фокус каждой игры. Так, например, первая прошла под эгидой темы SOC.

В первой игре сыграли команды «Слонята и мамонты», «Steak holders» и «неSOCрушимые». К всеобщему сожалению и некоторому удивлению, команда «Слонята и мамонты» хоть и боролась до последнего, но не смогла преодолеть отметку в 0 и завершила игру с отрицательным балансом, а вместе с тем и гонку к чемпионскому титулу. Но коллеги не расстроились, а признались, что чувствовали настоящий азарт во время игры. Так что, возможно, некоторых из них мы встретим в составе новых команд на ближайших играх.

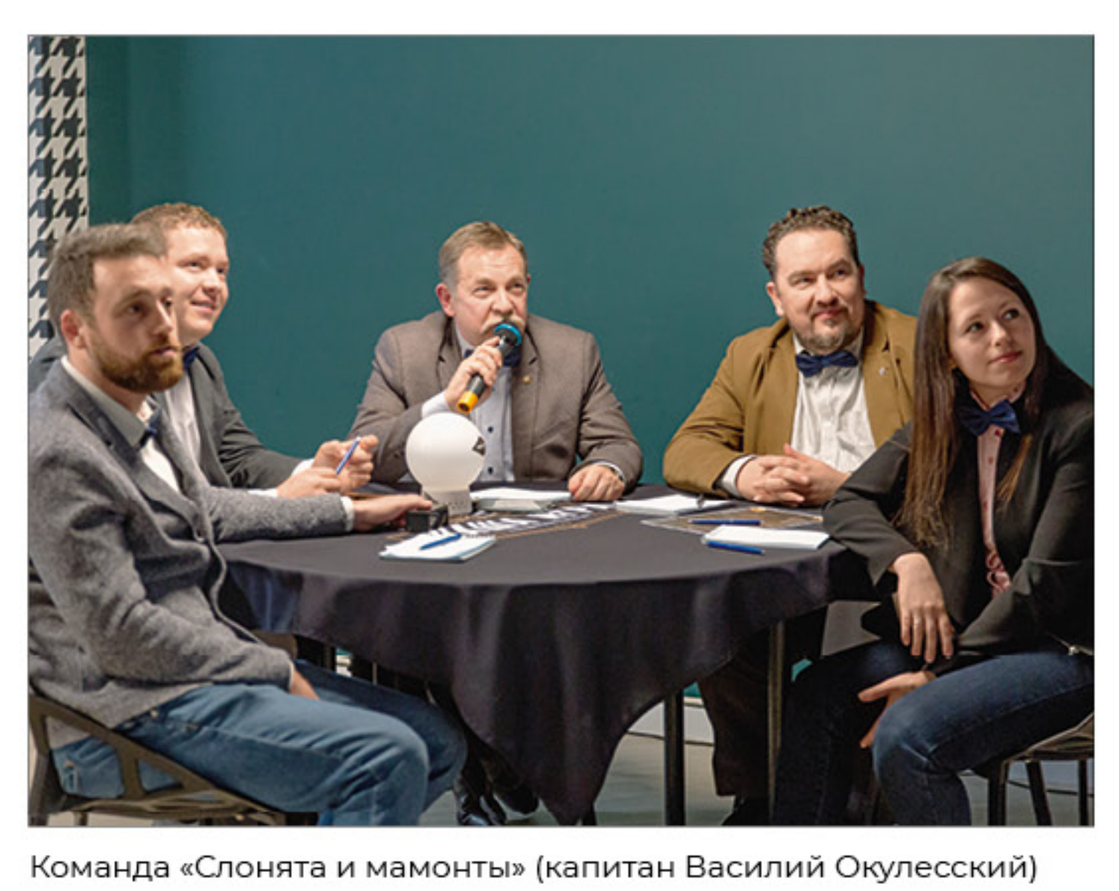
По словам Льва Шумского, капитана команды-победительницы, «силой» его команды являются люди. Сомнений в победе капитан команды в своих рядах и не допускал. Выбрав стратегию «тихой сапой», «Steak holders» провели игру с уверенным отрывом от остальных команд. Отметим, что Лев является победителем со стажем: его команда выиграла «Свою ИБ-игру» на VIII Уральском форуме.

Татьяна Станкевич изначально хоть и не была уверена, что ее команде удастся обыграть настоящих мамонтов отрасли, тем не менее выбрала для своих «скромное» название «неSOCрушимые». Сокрушить эту команду в самом деле не удалось, коллеги заняли 2-е место и получили возможность продол-

Победители «Нашей игры» — команда Steak holders (капитан Лев Шумский)

Ведущий игры Алексей Лукацкий

Команда «неSOCрушимые» (капитан Татьяна Станкевич)



Команда «Слонята и мамонты» (капитан Василий Окулесский)

жить борьбу в прежнем составе, пропустив одну игру.

Роль ведущего взял на себя Алексей Лукацкий, известный последователь темы геймификации в информационной безопасности. Алексей провел титаническую работу и подготовил все вопросы для игры и, что называется, правил бал. По правилам, все спорные моменты, касательно вопросов, ответов, зачисления или списания баллов, в узурпаторском порядке решает ведущий.

— Это совершенно новый формат и для нас, и для сообщества, — рассказывает Артем Зубков, генеральный директор Медиа Группы «Авангард». — И у нас есть планы и задумки, как сделать так, чтобы формат стал популярным среди широкой публики: специалистов, регуляторов, вендоров, студентов и всех, кто интересуется или связан с темой информационной безопасности.

Съемки игры проходили в пространстве «Весна», где собрались как специалисты по информационной безопасности, так и представители вендоров, интеграторов и дистрибуторов в роли игроков, гостей и болельщиков. Мероприятие объединило около 50 участников и в будущем предполагает быть регулярным местом встречи и проведения интеллектуального досуга представителей отрасли ИБ.

* * *

Организаторы приглашают к участию специалистов по информационной безопасности принять участие в будущих играх сезона, оставить заявку можно на сайте игры *igra.ib-bank.ru*. Организаторы также приглашают к партнерскому участию вендоров, интеграторов, дистрибуторов, учебные центры, профессиональные клубы, ассоциации и всех желающих.

ТРОЕ И ПИПЕЦ

Пьеса Рустэма Хайретдинова
Посвящается годовщине WannaCry

СЦЕНА ПЕРВАЯ

Бизнес пересчитывает купюры. Входит ИБ.

ИБ. Привет, я по делу, срочно.

Бизнес. Опять бабки клянчить будешь? Знаешь, гад, когда зайти. Через камеру за мной подглядывал небось?

ИБ. Не, денег просить не буду, потом попрошу. Просто патч надо накатить. Бесплатно. Слежу, конечно.

Бизнес. Вот ведь гад, надо бы камеру заклеить. Бесплатно — валяй.

СЦЕНА ВТОРАЯ

Бизнес пересчитывает деньги. Входит ИТ.

ИТ. Там этот параноик из ИБ со своим патчем… Говорит, с вами договорился. Если так патчи накатывать, всё остановится. Нужно аккуратненько, а то системы встанут.

Бизнес. Ну договоритесь уже как-нибудь сами, что вы за каждым чихом ко мне бегаете.

СЦЕНА ТРЕТЬЯ

Все трое совещаются.

Бизнес. Не смогли опять за два месяца договориться, за что я вам только зарплату плачу! Ставить стрёмно и не ставить стрёмно. Дилемма… Давайте мне после праздников все аргументы за и против, и я, так и быть, приму личное взвешенное решение: ставить или не ставить. *(В сторону)* А там, глядишь, и само рассосётся.

СЦЕНА ЧЕТВЕРТАЯ

Те же и Пипец. Незаметно входит Пипец с большим чемоданом на колёсиках. Покашливает, чтобы привлечь внимание.

Пипец. Здравствуйте, извините, что без приглашения. Я — Пипец.

Бизнес. Почему с вещами?

Пипец. Я надолго.

ИБ. А я говорил!

ИТ. Ты всё время только говоришь. Сделал бы что-нибудь хоть раз!

Бизнес. За что я вам только деньги плачу?

Немая сцена.
Только слышно, как Пипец достает одежду из чемодана и развешивает на плечики в шкафу у Бизнеса.

(Занавес)

КОММЕНТАРИЙ АВТОРА

Эта «пьеса» — реакция на первый «громкий» шифровальщик WannaCry, попытка визуализировать проблему, по причине которой он стал таким разрушительным. Разговоры с пострадавшими заказчиками показали, что эта проблема — не техническая: об уязвимости, которую использовали атакующие, знали давно, и патч выпустили еще за три месяца до атаки. Пожалуй, это первый выпуклый пример того, что безопасность сегодня — это именно бизнес-проблема цифровых компаний, когда скорости изменения систем отстают от нужд безопасности.

Рустэм Хайретдинов, *драматург*

НАША ИГРА

ГИЛЬДИЯ МАСТЕРОВ ИБ

Первое интеллектуальное шоу по информационной безопасности

Премьера на BIS TV 15 ноября

Смотри новые выпуски
и становись участником игры:
igra.ib-bank.ru

Полетели на Урал!

18–22 февраля 2019 года
Республика Башкортостан

ural.ib-bank.ru

УРАЛЬСКИЙ ФОРУМ
XI
информационная безопасность финансовой сферы