



24> Анатолий АКСАКОВ
(Государственная Дума РФ)
**Долгожданные перемены
к лучшему**

28> Андрей ВЫБОРНОВ
(Банк России)
**Стандарт СТО БР ИББС-1.4
актуален и востребован**



32> Сергей ВАЛУЙСКИХ
(Сбербанк)
**Второй SOC: тюнинг
или новая модель?**

38> Андрей БАЖИН
(ВТБ Капитал)
Защита премиум-класса

88> Артем ЗУБКОВ
(ФСРБИТ)
**Система стабильна,
но неповоротлива**

ФЗ-187: СОХРАНИТЬ ПЕРО ЖАР-ПТИЦЫ



САМАЯ МАСШТАБНАЯ КОНФЕРЕНЦИЯ В ОТРАСЛИ



SOC-ФОРУМ 2018

**ПРАКТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ
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

Лето-2018. Опаленная низким и жарким солнцем, Россия смотрит на мир сквозь сетку футбольных ворот. И конечно, дружно возмущается по поводу пенальти (в виде пенсионной реформы) со стороны правительства. Будет гол? Или, все-таки, не будет?

А мы, тем временем, готовим сани, в которых ИБ предстоит ездить не одну зиму. Обсуждаем ФЗ-187 «О безопасности критической информационной инфраструктуры РФ». А как иначе, ведь под его действие попала вся финансовая сфера целиком. Поэтому пришлось собрать кворум: регулятор, специалисты, эксперты и, куда ж без них, непосредственные исполнители этого самого закона.

Сани в работе у нас не одни. Есть и модернизированные, повышенной комфортности — это принятый Госдумой в июне ФЗ-167 «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств». Он на радость всем расширяет полномочия не только Банка России (что было бы не удивительно), но и операторов платежей, в частности, банков.

Есть и экспериментальные сани, не совсем пока понятные — это Стандарт СТО БР ИББС-1.4–2018 «Управление риском нарушения ИБ при аутсорсинге». Про него член нашей редколлегии Сергей Вихорев, с сомнением покачав головой, сказал: «Лиха беда начало».

Есть и совсем дикие, заморские — закон Европейского союза о защите данных — GDPR. Его еще на русский язык официально не перевели, а он уже многих напугал своими штрафными санкциями (до 20 млн евро). Но так ли страшен черт? Читайте — узнаете.

Можно было бы как сенсацию представить розвальни от вновь испеченного Минцифра — решение радикально переписать программу «Цифровая экономика РФ», но это пока только слова, идеи, соображения... Когда появится реальное средство передвижения, тогда и обсудим предметно. В качестве компенсации предлагаем международный обзор «Цифровая гонка. Никто в мире не хочет стать аутсайдером...» Полезно вспомнить, что ты на планете не единственный.

А пока сенсаций только две: в Сбербанке новый SOC! Сами создатели называют его крупнейшим в России и (тсс! Хотя, чего мелочиться?), может быть, даже и в Европе. Вторая: Ростелеком купил Solar Security и собирается отхватить кусок в 70–80 % рынка услуг по ИБ в отчизне. Об этом и поговорим.

Вообще-то, в номере много чего любопытного — не только выставка саний. Даже больше, номер получился настолько разнообразным, что другой член нашей редколлегии Василий Окулесский потерял ориентацию и сильно встревожился. «Безопасность — это что вообще такое!?» — хватается он за голову на последней странице. И не удивительно.

Вы сами-то сможете ответить на этот вопрос без сомнений?

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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

Сычев А.М. — и.о. 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 ИТЦ «Вулкан»

Дзержинский Ф.Я. — главный эксперт — координатор

системной экспертизы блока «информационные

технологии» ООО «ТехноСофт», CS DP

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. — руководитель проекта ИБ АО «РЭЦ»

Некрасов И.В. — главный редактор журнала

Окулесский В.А. — руководитель департамента

ООО «ЦИБИТ», кандидат технических наук

Пазизин С.В. — начальник Управления по обеспечению

информационной безопасности ОАО Банк ВТБ, кандидат

физико-математических наук

Шумский Л.С. — руководитель направления ИБ

АО «Альфа-Банк»

Янсон И.А. — бизнес-партнер по информационной

безопасности, Департамент безопасности ПАО «Сбербанк

России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Одувалов М.В. — эксперт BIS Journal

Филипчук А.А. — технический директор ГК ЦРТ

Калашникова Е.В. — Банк ВТБ (ПАО)

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**

Шеф-редактор: **Былевский П.Г.**

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

Арт-директор: **Мельников Н.С.**

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

Северный В.П., Хвастунова О.Н., Бродская М.А., к.т.н.

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

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

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

Цветокорректор: **Науменко М.Б.**

Корректор: **Бальтерманц Л.Ф.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»

Адрес: 127473, Россия, Москва, 3-й Самотечный переулок,

д.21 (м. «Достоевская»)

Координаты: 55.779380, 37.61150

Тел./факс: +7 499 271-70-85

Интернет-версия: journalib-bank.ru

E-mail: bis@ib-bank.ru

Отдел рекламы: reklama@ib-bank.ru

Отдел распространения: tirazh@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (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 6.07.2018. Тираж 7000 экз.

Заказ № 240554. Цена договорная.

Отпечатан в «Типографии на Угрешской»

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

Тел.+7 495 720-62-28

© BIS Journal, 2018



НОВОСТИ

5 В мире, в России, криминал

ТЕМА НОМЕРА

- 10 КИИ**
Андрей ВЫБОРНОВ (Банк России)
Лучшие оказались готовы
- 12 КИИ**
Александр КУЗНЕЦОВ (НТЦ «Вулкан»)
До развилки и дальше
- 17 КИИ**
Анна ВОРОБЬЕВА (BIS Journal)
Работаем на перспективу
- 20 КИИ**
Павел КОРОСТЕЛЕВ (Код безопасности)
Может ли выполнение требований по защите КИИ повысить риски ИБ?

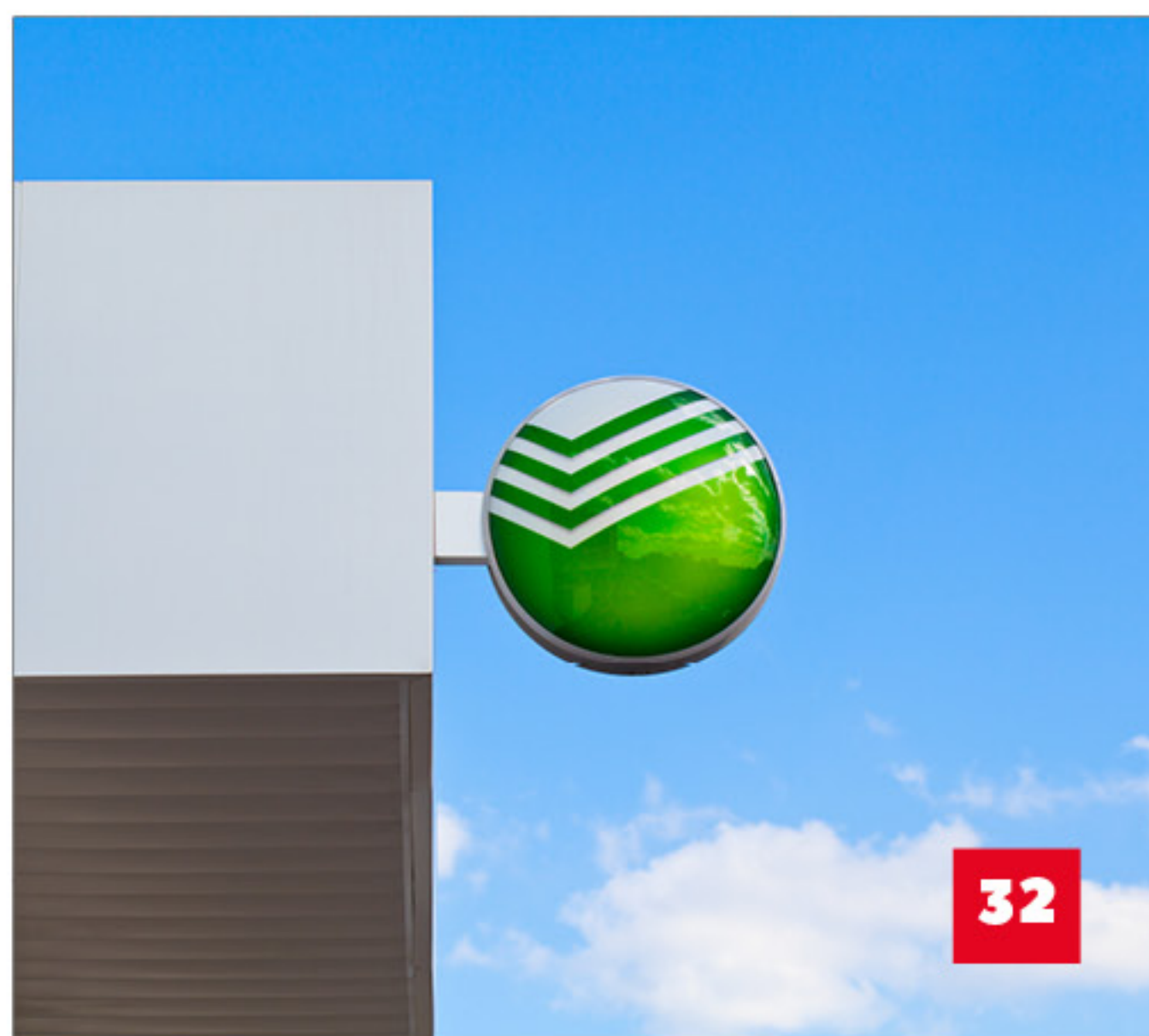
РЕГУЛЯТОРЫ

- 24 Законодательство**
Анатолий АКСАКОВ (Государственная Дума РФ)
Долгожданные перемены к лучшему
- 28 Стандарты**
Андрей ВЫБОРНОВ (Банк России)
Оцени киберриски при аутсорсинге, прими оптимальное решение

БАНКИ

- 32 СОСи России**
Сергей ВАЛУЙСКИХ (Сбербанк)
Второй СОС Сбербанка
- 36 Рынок ИБ**
Анна ВОРОБЬЕВА (BIS Journal)
Solar Security в новой роли... сталкера





БАНКИ

- 38 Специфика ИБ**
Андрей БАЖИН (ВТБ Капитал)
Защита премиум-класса
- 41 Финтех**
Валерия МЕЩЕРЯКОВА (BIS Journal)
В один клик
- 42 Законодательство**
Кристина БОРОВИКОВА, Андрей ДРОЗДОВ (KPMG)
GDPR. А так ли страшен черт?



УГРОЗЫ И РЕШЕНИЯ

- 48 SWIFT**
Антон СВИНЦИЦКИЙ (АО «ДиалогНаука»)
SWIFT в стране безопасности
- 50 Блокчейн**
Марат РАХИМОВ (ООО «Газинформсервис»)
Безопасность блокчейна
- 52 Практика ИБ**
Дмитрий МИХЕЕВ (АйТи БАСТИОН)
Страх и ненависть при удаленном доступе
- 54 Инструментарий**
Леонид БОНДАРЕНКО (АО «Кросс технолоджис»)
Утечки данных
- 56 ГосСОПКА**
Георгий КАРАЕВ (Перспективный мониторинг)
Проводник для восхождения на ГосСОПКА
- 58 Облачные технологии**
Денис КАЛЕМБЕРГ (SafeTech)
Облачная подпись на смартфоне
- 60 IDM**
Александр МАХНОВСКИЙ (Аванпост)
Топ-5 вызовов для системы IGA



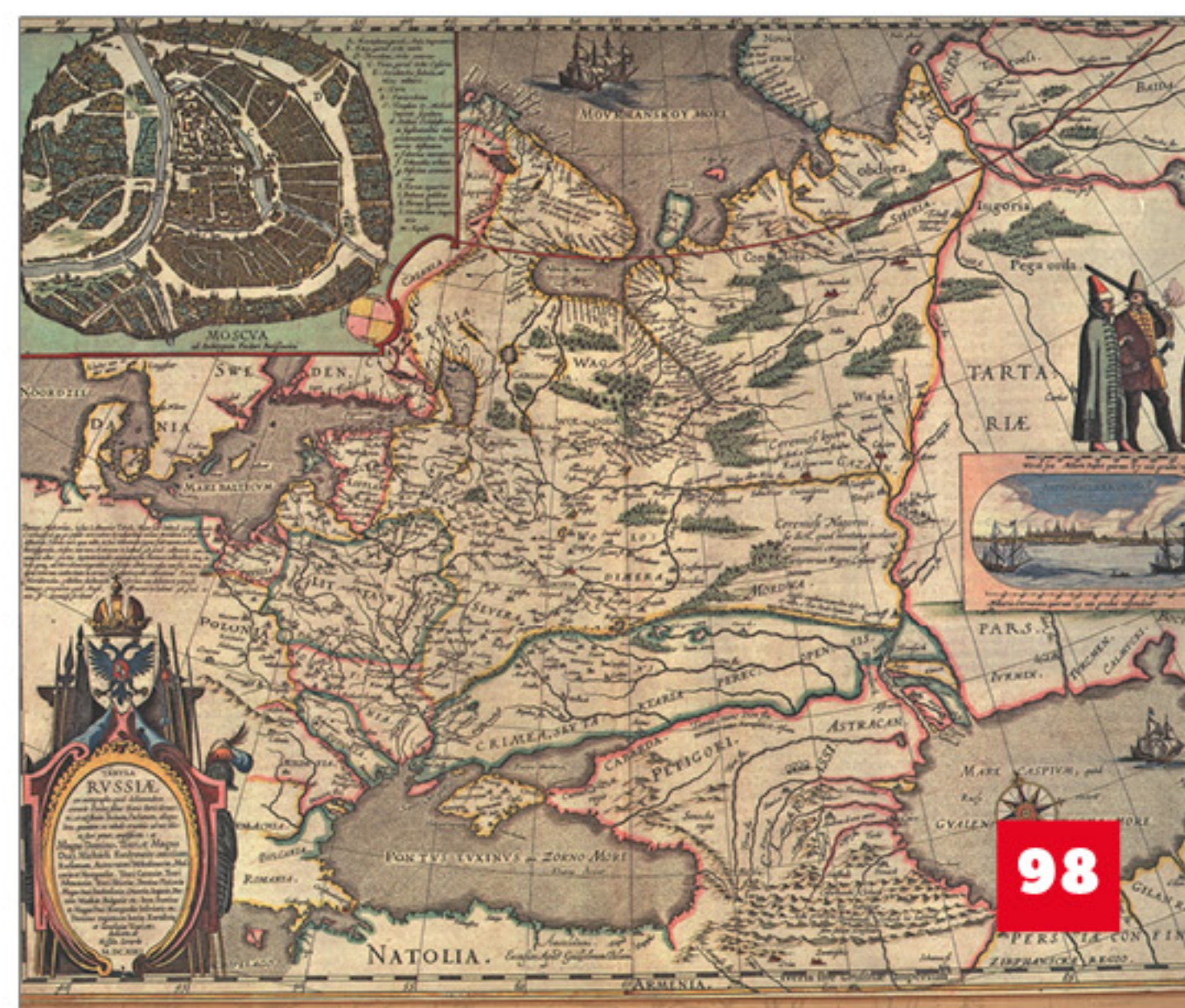
ИНФРАСТРУКТУРА

- 64** **Деловые мероприятия**
Марк НОВОДАЧНЫЙ (BIS Journal)
VII Форум АЗИ
- 66** **Деловые мероприятия**
Николай КОЛЬСКИЙ (BIS Journal)
Positive Hack Days 2018
- 68** **Деловые мероприятия**
Валерия МЕЩЕРЯКОВА (BIS Journal)
CTCrypt 2018. DLTReg 2018
- 72** **Деловые мероприятия**
Валерий КУЛИКОВ (BIS Journal)
Между Сциллой и Харибдой
- 74** **Обзор**
Анна КАТАНКИНА (BIS Journal)
Цифровая гонка



ОБРАЗОВАНИЕ И КАРЬЕРА

- 80** **Карьера**
Александр БОДРИК (ISACA Moscow)
ТОП-работодатели для ТОП-карьер
- 83** **Обзор**
Марина БРОДСКАЯ (BIS Journal)
Олимпиады по ИБ 2018
- 86** **Кадры**
Евгения КОЛОДИНА (ЦИБИТ)
Закрыв глаза, любовь не повстречать
- 88** **Доклад**
Артем ЗУБКОВ (ФСРБИТ)
Система стабильна, но неповоротлива
- 92** **Обзор**
София СИМОНОВА (BIS Journal)
Кто делится знаниями?



СУБЪЕКТЫ

- 94** **История**
Дмитрий ЛАРИН (АО «Лаборатория «СКАТ»)
Древнерусские шифры
- 98** **История**
Борис СТОЛПАКОВ (историк криптографии)
«Дмитрий Франзбеков челом бьёт...»
- 104** **Молодой специалист**
Валерия МЕЩЕРЯКОВА (BIS Journal)
Студенты в области ИБ: кто они?
- 108** **Мысли вслух**
Василий ОКУЛЕССКИЙ (BIS Journal)
Безопасность — это что?

БОЕВЫЕ УЧЕНИЯ ЕЦБ

Европейский Центробанк проверит кибербезопасность финсектора подведомственных организаций. Тестировать системы на прочность будут штатные сотрудники и нанятые команды хакеров, которые попытаются обнаружить недочеты, моделируя реальные попытки взлома.

Проект называется «Европейская программа по отражению угроз с использованием специальных экспертов, атакующих систему извне» (European Framework for Threat Intelligence-based Ethical Red Teaming — TIBER-EU). Программа носит рекомендательный характер для стран-членов ЕС.

В ходе тестов предлагается использовать «полный спектр приемов, которые применяют реальные хакеры». В частности, предлагается подвергнуть условным кибератакам критически важные системы финансовых учреждений.

По итогам проверок будут даны рекомендации по совершенствованию конкретной системы безопасно-

сти того или иного финансового учреждения, уточнили в ЕЦБ. При этом «...власти будут признавать прохождение тестов только в том случае, если в них будут участвовать не только внутренние специалисты, но и внешние стороны».



ПО \$142 С НОСА — ВСЕГО \$172 МЛРД

Опубликован доклад о кибербезопасности Norton Cyber Security Insights за 2017 год. По представленным данным в прошлом году жертвами интернет-мошенников в 20 странах мира стали 978 млн пользователей, а общая сумма хищений составила 172 млрд долларов. В среднем каждая зафиксированная (!) жертва преступлений в Сети потеряла около 142 долларов.



К сожалению, данные о киберпреступлениях приведены только по 20 странам мира, среди которых нет России: Австралия, Бразилия, Великобритания, Германия, Гонконг, Индия, Индонезия, Испания, Италия, Канада, Китай, Мексика, Нидерланды, Новая Зеландия, ОАЭ, Сингапур, США, Швеция, Франция и Япония.

Больше всего от киберпреступлений пострадали пользователи в Китае — почти 353 млн человек в совокупности потеряли 66 млрд долларов. На втором месте оказалась Индия, где в 2017 году в результате таких преступлений 186 млн человек потеряли 18,5 млрд долларов. На третьей позиции США — там с киберпреступлениями столкнулись 143 млн потребителей — больше половины взрослого населения страны.

УКРАИНСКИЕ ХАКЕРЫ НАПАЛИ НА ГЕРМАНИЮ

Киберпреступники проникли во внутренние сети двух крупнейших немецких поставщиков электроэнергии.

Служба безопасности Германии зафиксировала атаки на ранних стадиях и успешно их отразила. Хакеры могли нарушить подачу электричества потребителям и даже избирательно повредить энергосистемы компаний.

Нападение было организовано группой хакеров, которые в декабре 2016 г. проникли в сети энергетических компаний на Украине. По крайней мере, так утверждают эксперты. Тогда на Украине из-за хакерской атаки были зафиксированы масштабные перебои с электроэнергией.



МЕКСИКАНСКИЕ УМЕЛЬЦЫ

Впервые у ряда мексиканских банков хакеры похитили огромную сумму — примерно \$15,4 млн. Через поддельные запросы они перевели средства на подставные счета, а затем быстро обналичили их.

Всего было отправлено около сотни поддельных запросов на перевод сумм от десятков тысяч до сотен тысяч песо. Тем не менее пока неясно, какую сумму злоумышленникам удалось обналичить, поскольку некоторые мошеннические транзакции были заблокированы.

По мнению специалистов, перевод таких крупных сумм не мог обойтись без инсайдеров. Межбанковская система обмена сообщениями SPEI осталась нетронутой, а хакеры, вероятно, атаковали банковское ПО, разработанное самими организациями или местными подрядчиками.

ВОЛЖАНЕ УКРАЛИ МИЛЛИОН

Житель Волжского задержан по подозрению в хищении денег с банковских счетов жителей десятка регионов страны.

Судимый безработный 32-летний волжанин вместе с еще несколькими участниками преступной группы в течение двух лет рассылал потенциальным жертвам смс-сообщения со ссылками. Затем с электронных карт тех, кто переходил по этим ссылкам, списывались деньги.

Похищенное мошенники вкладывали в криптовалюту. При обыске в квартире подозреваемого волжанина оперативники нашли более трех десятков сим-карт разных операторов, банковские карты, мобильные телефоны. Также были изъяты наличные деньги в объеме около 130 тысяч рублей. По имеющимся сведениям, доход преступной группы составил около миллиона рублей.

ЗАПУЩЕНА ПЛАТФОРМА ОБМЕНА ДАННЫМИ

Ассоциация банков России запустила пилотную версию платформы обмена данными о киберугрозах. Главная задача платформы, разработанной компанией BI.ZONE, — предоставить банковскому сообществу, прежде всего малым и средним региональным банкам, возможность обмениваться информацией о возникающих угрозах и возможных атаках.

В настоящее время такие данные поступают в платформу в рамках сотрудничества между Сбербанком и

компанией Мегафон, последняя предоставляет информацию по электронным кошелькам. Сейчас насчитывается 17 участников пилотного проекта, в перспективе к ним присоединятся еще 20. Первыми участниками и партнерами новой платформы стали Сбербанк, УРАЛСИБ, ЮниКредитБанк, РОСБАНК, Тинькофф Банк, НСПК и другие.

Пилотирование платформы будет длиться три месяца, а после подведения итогов проект ждет масштабирование.



СПОНСОРЫ



10-11 октября
2018 года

Москва, ЦВК "Экспоцентр"
Павильон № 7



V МЕЖДУНАРОДНЫЙ ФОРУМ
ВБА-2018

ОРГАНИЗАТОРЫ



10-11 октября 2018 года на Форуме "ВСЯ БАНКОВСКАЯ АВТОМАТИЗАЦИЯ 2018" / ВБА-2018 в Москве (ЦВК "Экспоцентр", Павильон № 7) будут представлены:

- Автоматизированные банковские системы (АБС, ИБС, core banking)
- Автоматизация фронт-офиса, филиальной сети, розничного и корпоративного бизнеса
- Электронный и мобильный банкинг, системы ДБО
- Банковские карты, платежные системы, процессинг, бесконтактные платежи, NFC
- Системы самообслуживания, банкоматы, платежные терминалы
- Управление продажами и банковским обслуживанием, CRM-системы, call-центры
- Управление эффективностью и бизнес-аналитика, BPM и BI системы, управление рисками
- Банковская ИТ-инфраструктура, ЦОД, оборудование, сети и телекоммуникации
- Управление ИТ-активами, сервисами, изменениями, ITSM
- ИТ-аутсорсинг и облачные технологии для банков
- Информационная безопасность банков
- Электронный документооборот, ЕСМ-системы, электронные архивы
- ЭДО с государственными органами (ГИС ГМП ФК, ФНС, ФССП, ФМС и др.)
- Управление ресурсами, управление персоналом (HRM-системы), АХД, закупки
- Интеграционные решения для банков

Оргкомитет Форума "ВСЯ БАНКОВСКАЯ АВТОМАТИЗАЦИЯ 2018" / ВБА-2018
Тел.: +7 (495) 229-8502, e-mail: 2018@vbaforum.ru, <http://vbaforum.ru>



ЛУЧШИЕ В РОССИИ: КОМПАНИИ, ПРОЕКТЫ И ПЕРСОНЫ ГОДА 2017



6 июня в Доме Союзов состоялось вручение ежегодной бизнес-премии "Лучшие в России 2017".

Премия проходит с 1998 года и отмечает успехи персон, компаний и проектов за прошедший год.

Победителей определяет экспертный совет, в состав которого входят влиятельные экономисты, бизнесмены, политические и общественные деятели. Организатор и учредитель премии — новостной портал Anews.com. Выбор лауреатов происходил на основании рэнкингов, подготовленных партнерами РА «Эксперт РА» и аналитическим агентством «Медialogия».

На мероприятии гостей ждало изысканное

угощение EXPERTCATERING, вода премиум качества «Лангвей», а так же сладкие угощения от Кондитерской фабрики «Волшебница» и компании СПЕЧНАЗ.

Героев года чествовали член Бюро Правления РСПП Давид Якобашвили, Генеральный директор Организационного комитета по подготовке и проведению чемпионата мира по футболу «Россия-2018» Алексей Сорокин, Генеральный директор ММБА Александр Борисов, начальник Управления по вопросам реализации городских программ поддержки физкультурно-спортивных организаций Департамента спорта и туризма города Москвы Дмитрий Краснюков, Вице-

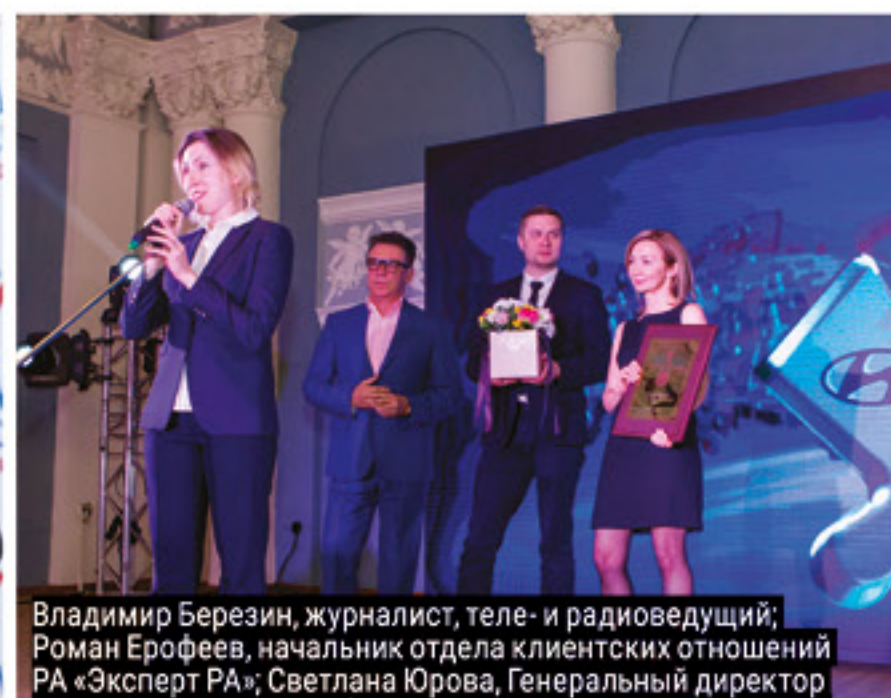
президент Общероссийской общественной организации "Деловая Россия" Татьяна Минеева, Председатель Комитета ТПП РФ по финансовым рынкам и кредитным организациям Владимир Гамза, экономист Института проблем глобализации Михаил Делягин, фигуристка и телеведущая, мастер спорта международного класса Анастасия Гребенкина, актриса театра и кино Анастасия Макеева, советский и российский диктор, актриса кино, теле- и радиоведущая Анна Шатилова, российская телеведущая, журналист, актриса Марина Ким, актер, журналист, теле- и радиоведущий Владимир Березин и многие другие.



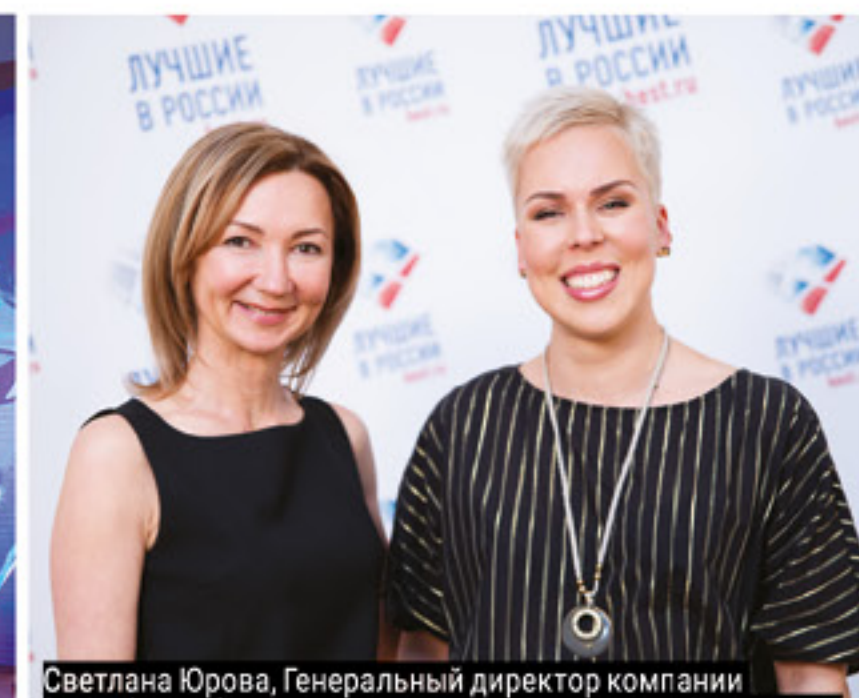
Андрей Разыграев, Ведущий Церемонии



Елена Борщева, актриса, ведущая



Владимир Березин, журналист, теле- и радиоведущий; Роман Ерофеев, начальник отдела клиентских отношений РА «Эксперт РА»; Светлана Юрова, Генеральный директор компании Brains& Brands; Юлия Тихонравова, Директор по связям с общественностью Хендэ Мотор Мануфактуринг Рус



Светлана Юрова, Генеральный директор компании Brains& Brands; Наталья Смирнова, Генеральный директор «Эмкварта. Персональный советник»



Елена Тетюнина, Заместитель генерального директора НПФ «Сбербанка»



Церемония награждения



Ким Так Хюн, Генеральный директор российского Представительства «Навиен Рус» (с наградой)



Дмитрий Краснюков, начальник Управления по вопросам реализации городских программ и поддержки физкультурно-спортивных организаций Департамента спорта и туризма города Москвы; Виталий Расницын, Президент Российской академии общественных связей; Валерий Светлов, Руководитель Группы охранных компаний «Карат-Ц»; Анастасия Гребенкина, фигуристка и телеведущая, мастер спорта; Александр Борисов, Генеральный директор ММБА



Елена Бирюкова, Исполнительный директор Премии, Владимир Березин, журналист, теле- и радиоведущий



Роман Блинов, Руководитель департамента аналитики «Международный Финансовый Центр»



Елена Борщева, актриса, ведущая; Анна Шатилова, диктор, теле- и радиоведущая; Владимир Березин, журналист, теле- и радиоведущий; Павел Соколов, певец



Антон Замков, Генеральный директор «РТ-Инвест Транспортные системы»



При поддержке



Официальный рейтинговый партнер



Аналитический партнер



Официальная площадка церемонии



Официальный кейтеринг



Сладкий партнер



Официальная вода



Партнер



Официальный печатный партнер



Генеральный информационный партнер



Информационные партнеры



На правах рекламы

РУССКИЕ ХАКЕРЫ СТАЛИ ЛУЧШИМИ В КИТАЕ

Команда L C BC из России победила в турнире по хакингу International Elite Challenge on Cyber Mimic Defense, который прошел на международном IT-саммите в Китае.

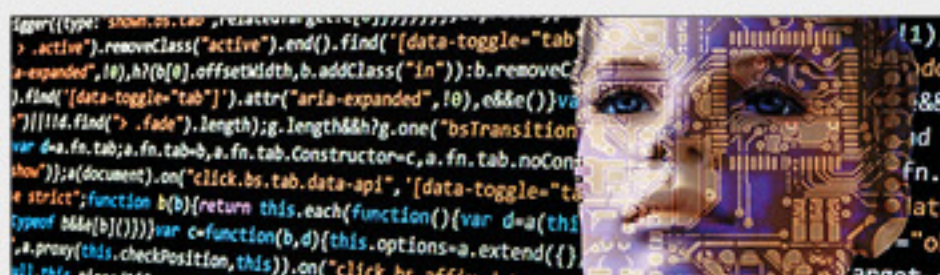
В соревновании принимали участие 22 команды из пяти стран. Любопытно, что ни одна из них даже после 500 000 атак не смогла уничтожить китайскую разработку, которая была представлена в виде мишени. Система безопасности в киберпространстве, основанная на предложенной Китаем «идеологической теории обороны», выдержала более полумиллиона хакерских атак и устояла. Тем не менее россияне в этой бесплодной борьбе заработали наибольшее число баллов.



ИИ НА ЗАЩИТЕ МОСКОВСКИХ АУКЦИОНОВ

В Москве на единой электронной торговой площадке начали применять технологии машинного обучения и нейронных сетей. Благодаря новым технологиям с начала года удалось предотвратить 73 вредоносные атаки.

Система информационной безопасности единой электронной торговой площадки в автоматическом режиме фиксирует все входящие и исходящие запросы. При этом искусственный интеллект отделяет запросы добросовестных пользователей от вредоносных атак и действий аукционных роботов, которые популярны среди мошенников.



ЦИФРОВАЯ ЭКОНОМИКА: КОНЦЕПЦИЯ ИЗМЕНИЛАСЬ

Министерство цифрового развития, связи и массовых коммуникаций РФ решило в течение лета 2018 г. радикально переписать программу «Цифровая экономика РФ» и повысить её статус до уровня «национального проекта».

«В существующем виде программе не хватает конечных продуктов: пока она направлена на создание обеспечивающих вещей, таких как информационная инфраструктура. В течение нескольких месяцев мы сформируем представление о том, что такое цифровая экономика для населения, бизнеса, государства. Переписав программу этим летом, я не вижу ничего зазорного в том, если через год мы снова все изменим», — сообщил глава Минцифры Константин Носков.

Представители ИТ-сообщества с удивлением восприняли информацию о такой ревизии. В частности, Наталья Касперская призналась, что не понимает, чем национальный проект будет от-

личаться от прежней программы. По ее мнению, основной причиной пробуксовки программы является отсутствие финансирования: на реализацию программы в 2018 г. планировалось выделить 27,17 млрд руб., но средств в бюджете не оказалось, поэтому сумма сократилась до 3 млрд руб. «Из них на направление «Информационная безопасность» решено направить 363 млн руб., но пока не выдано ни копейки», — посетовала Касперская.



БРАТЬЯ ДУРОВЫ ОТКРЫВАЮТ «ИНТЕРНЕТ В ИНТЕРНЕТЕ»

Павел и Николай Дуровы разрабатывают суперверсию даркнета для онлайн-платежей — платформу Telegram Open Network (TON). Платформа станет «интернетом в интернете» — надстройкой над нынешней глобальной сетью, но с архитектурой, при которой к ней нельзя будет безболезненно закрыть доступ или взломать привычными для «обычного» интернета способами.

Сеть планируется использовать для интернет-платежей и онлайн-магазинов компаний/частных лиц, которые будут эти платежи осуществлять. По функциональности TON окажется чем-то средним между порталом «Госуслуги» и платежной системой PayPal, при помощи которой можно оплачивать товары в интернет-магазинах или услуги наподобие такси или ж/д перевозок.

По мнению эксперта R-Style Softlab Максима Большова, такая сеть сможет функционировать в сложных условиях блокировки ее отдельных узлов безболезненно для себя, используя множественные связи между своими узлами. Однако, такой подход может вступить в противоречие с законодательством не только России, но и других стран. В то же время на практике такие проекты еще ни разу не осуществлялись, а значит, с противодействием со стороны государства и не сталкивались.



ИЗМЕНИЛАСЬ ФОРМА ОТЧЕТА О КИБЕРИНЦИДЕНТАХ

С 1 июля изменилась форма отчета о киберинцидентах. Теперь, в соответствии с указанием БР № 4753-У, информировать Банк России об инцидентах, в ходе которых похищены средства, будут не только банки, но и операторы систем денежных переводов.

В Банке России полагают, что такой подход поможет пролить свет на реальную картину с киберхищениями. Финансовым организациям теперь разрешается опустить технические показатели, однако необходимо

предоставлять экономические — те, которые подробно опишут последствия киберинцидентов для операторов и их клиентов. Банкам предлагается разбивать инциденты по типам хищений: через банкомат или терминал, с использованием реквизитов, через системы дистанционного банковского обслуживания и т.д.

Строго необходимо указывать похищенную сумму, а также сколько удалось вернуть из похищенных средств. Следует указывать и использование в ходе хищения методов социальной инженерии. Информация об атаках на банкоматы должна представлять собой более подробный отчет. Организации, работающие с электронными кошельками, также обязаны детализировать инциденты: имел ли место персонифицированный или неперсонифицированный электронный кошелек, использовалась ли социальная инженерия, сколько средств удалось вернуть и т.д.



САРАТОВСКИЙ ХАКЕР СТАЛ ГЕРОЕМ... WORLD OF TANKS

26-летний житель Саратова обвиняется в хищении денег с помощью фишингового сайта. Жертвами хакера стали 52 жителя из разных регионов страны. С их счетов были списано 384 тыс. руб.

В 2016 г. хакер приобрел через интернет образ сайта одного из крупных банков, доработал его и запустил. Затем в «Одноклассниках» разместил рекламный ролик о том, что банк проводит акцию, благодаря которой любой его клиент может получить денежное вознаграждение. Одно из условий — необходимо зарегистрироваться на сайте (и тут же ссылка, ведущая на «мошеннический» ресурс). Пользователи вводили свои идентификаторы, логины от личных кабинетов и СМС-коды подтверждения операций и попадали в руки злоумышленника.



Похищенные с чужих счетов деньги молодой человек переводил на электронные кошельки. Большую часть похищенного он потратил на приобретение аккаунта в компьютерной игре World of Tanks и дальнейшее участие в виртуальных битвах. Его успехи в игре признаны следователем значительными.

ЧТО ЗА ГАДЖЕТ?

Банк России для борьбы с отмыванием денег обязал кредитно-финансовые организации анализировать настройки и параметры устройств, которые клиенты используют при переводе средств. Этим устройствам банки должны присваивать идентификаторы.

В случае, если идентификаторы у разных клиентов совпадают, банк должен считать их клиентами с повышенным уровнем риска.

Многие банки уже используют IT-данные для анализа действий клиентов, а новые требования регулятора лишь закрепили существующую практику. Большинство банков сейчас фиксируют IP-адреса устройств клиентов, но для выполнения новых требований регулятора необходимы технологические доработки.



ВОТ НЕЗАДАЧА!

Сервер компании по продаже билетов в Комсомольске-на-Амуре атаковали хакеры. Сотрудники не могли получить доступ к системе, за вход преступники требовали перевести 30 тыс. рублей биткоинами.

При этом сайт для перечисления криптовалюты оказался заблокированным. Как установили эксперты, злоумышленники не справились с собственным зловредом — вирусом-шифровальщиком, который, «сорвавшись с цепи», успешно атаковал и своих хозяев. Все это было бы смешно, если бы вирус не заблокировал информацию о покупателях авиабилетов, в том числе, льготных пассажиров.

За компьютерную атаку горе-хакерам грозит лишение свободы сроком до четырех лет. Ведется следствие, устанавливается источник распространения вируса.



Андрей ВЫБОРНОВ
начальник отдела
методологии обеспечения
безопасности
информационных
ресурсов ГУБиСИ
Банка России

ЛУЧШИЕ ОКАЗАЛИСЬ ГОТОВЫ

ПОЛИТИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ФИНАНСОВОЙ СФЕРЫ

Финансовая сфера целиком подпала под действие Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ. В области его применения оказались все участники финансовой сферы: от крупнейших банков, бирж, страховых, инвестиционных компаний, брокеров, вплоть до микрофинансовых организаций, ломбардов и сельскохозяйственных кооперативов. Все до одного они являются субъектами КИИ — критической информационной инфраструктуры.

ЗНАЧИМОСТЬ ФИНАНСОВОЙ СФЕРЫ

Среди всех организаций финансовой сферы выделяются владельцы системно значимых объектов КИИ, определяемых согласно Постановлению Правительства РФ от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Категории значимости определяются по-разному для различных сфер и отраслей. Одним из критериев значимости для финансовой сферы является ежедневный объём финансовых операций, транзакций, выполняемых организацией. При достижении указанного уровня система банка, или, как говорится в законе, объект КИИ, становится значимой. Среди более двад-

цати тысяч организаций финансовой сферы порядка десяти соответствуют критериям объекта КИИ: крупнейшие банки, НСПК, Московская биржа.

Для финансового сектора нет особой разницы источников информационных угроз, технические это сбои или результат злонамеренного воздействия — внешней компьютерной атаки или действий инсайдера, внутреннего нарушителя. Международный и отечественный опыт свидетельствует, что в финансовом секторе намного более существенным фактором является время.

Во-первых, долговременность прерывания предоставления услуг — не более двух часов. Во-вторых, завершение финансовых транзакций не позднее окончания операционного дня, без перехода на следующий рабочий день. Чтобы обязательства не оказывались незакрытыми, не возникал кредит овернайт.

Для Банка России и многих подведомственных организаций требования ФЗ-187 не оказались неожиданными, не упали как снег на голову. Банк России развивал комплекс отраслевых стандартов информационной безопасности с учётом нормативных документов других органов федеральной исполнительной власти, участвующих в регулировании отрасли.

Это своего рода единая методологическая база, вбирающая в себя статьи новых федеральных законов и подзаконных актов, касающихся информационной безопасности финансовой сферы. Для подведомственных организаций, выполнявших положения обновляемых версий СТО БР ИББС, ФЗ-187 не принёс неприятных «сюрпризов».

ФИНЦЕРТ КАК ОТРАСЛЕВОЙ ЦЕНТР

Требования ФЗ-187 условно можно разделить на две группы, по двум уполномоченным в сфере КИИ государственным органам федеральной исполнительной власти — ФСТЭК России и ФСБ России. Первая — выполнение норм, которые устанавливает ФСТЭК России, — по за-

**СРЕДИ БОЛЕЕ ДВАДЦАТИ ТЫСЯЧ
ОРГАНИЗАЦИЙ ФИНАНСОВОЙ
СФЕРЫ ПОРЯДКА ДЕСЯТИ
СООТВЕТСТВУЮТ КРИТЕРИЯМ
ОБЪЕКТА КИИ: КРУПНЕЙШИЕ БАНКИ,
НСПК, МОСКОВСКАЯ БИРЖА**

щите информации. Приказы, выпущенные на текущий момент, частично воспроизводят нормы, содержащиеся в более ранних документах. В том числе, касающиеся защиты персональных данных, ранее воспроизведённые в нашем отраслевом стандарте.

Более новым является взаимодействие с ГосСОПКА, относящееся ко второй группе требований ФЗ-187, по линии ФСБ России. Для реагирования на компьютерные атаки субъект КИИ должен взаимодействовать с ГосСОПКА. Эта деятельность очень похожа на ту, которую в финансовой сфере ведёт ФинЦЕРТ Банка России, взаимодействуя с кредитными организациями.

Работа, проведённая в этом направлении, в значительной мере подготовила кредитные организации к выполнению второй группы положений ФЗ-187. Именно кредитные организации — участники информационного взаимодействия с ФинЦЕРТ. Банк России совместно с ФСБ России разрабатывают нормативные документы, которые позволят ФинЦЕРТу выполнять функции ведомственного («отраслевого») центра ГосСОПКА в финансовой сфере. Получается трёхуровневая структура взаимодействия: организации финансовой сферы — ФинЦЕРТ Банка России — ГосСОПКА. Аналогичная работа для создания отраслевого центра ведётся и для телекоммуникационных компаний.

Текущая задача заключается в том, чтобы включить в это взаимодействие некредитные финансовые организации (биржи, страховые, инвестиционные компании, брокеров, саморегулируемые объединения микрофинансовых организаций и т.п.), которые являются субъектами КИИ. Это позволит участникам отрасли избежать двойной отчётности в вопросах безопасности КИИ. Процедуры взаимодействия для десятки крупнейших банков в настоящее время прорабатываются.

ОБНОВЛЕНИЕ ФОРМАТА ВЗАИМОДЕЙСТВИЯ

Банк России не является прямым государственным регулятором КИИ, но, конечно, там, где затрагивается финансовая сфера, осуществляет взаимодействие с ФСБ России и ФСТЭК России. Участвуя в аккумулировании предложений, в разработке подзаконных нормативных актов, в выстраивании информационного взаимодействия. Однако надзор и контроль выполнения ФЗ-187 организациями отрасли, принятие мер к тем, кто не исполняет, — эти функции не входят в полномочия Банка России.

Банк России участвует в развитии федерального законодательства и в целом нормативно-правовой базы, связанной с обеспечением безопасности КИИ. 27 июня 2018 года Президентом РФ был подписан Федеральный закон 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств».

Новый закон легализует приостановление банками и платёжными системами транзакций при выявлении признаков того, что они могут совершаться без согласия плательщика. Указанные признаки должны устанавливаться Банком России и размещаться на его официальном сайте в сети Интернет. За ненадлежащее исполнение банками новой обязанности, в частности речь идет о не приостановке платежей, отвечающим указанным критериям, банки будут нести ответственность.

После принятия нового закона, в его развитие, Банком России будут изданы подзаконные нормативные акты, модернизирован стандарт обмена информацией с ФинЦЕРТом. Такой пакет документов должен быть подготовлен в течение 90 дней с момента официального опубликования нового закона. Новый закон откроет возможность работы в расширенном, более эффективном формате.

Будут задействованы два набора автоматически действующих идентификаторов. Первый — показатели, которые идентифицируют схемы хищений и вывода похищенных денежных средств (номера банковских счетов, мобильных телефонов и др.). Второй блок — технические данные, описывающие характеристики компьютерных атак, в формате, удобном для ГосСОПКА.

* * *

Предполагается, что организациям финансовой сферы потребуется около двух лет, чтобы в полном объёме достигнуть соответствия ФЗ-187. Обратная связь — реакции и отзывы, поступающие в Банк России от ведомственных организаций — говорит о том, что эта работа ведётся. Первоочередная мера для тех, кто ещё не успел, — подключение к информационному обмену с ФинЦЕРТом. Прежде такое взаимодействие было «факультативным», вроде участия в «клубе антидроперов». После принятия ФЗ-187 и подзаконных нормативных актов информационный обмен с ГосСОПКА через ФинЦЕРТ Банка России превращается в прямую обязанность организаций финансовой сферы.

ДО РАЗВИЛКИ И ДАЛЬШЕ

ДОРОЖНАЯ КАРТА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КИИ ДЛЯ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СФЕРЫ



Александр КУЗНЕЦОВ
руководитель направления
информационной
безопасности
ООО «НТЦ «Вулкан»,
CISM, MVP

Текущий сценарий развития активностей вокруг Федерального закона № 187-ФЗ чем-то напоминает ситуацию с Федеральным законом № 152-ФЗ: так же есть несколько регуляторов, так же есть множество подзаконных актов, частично введенных в действие, а частично нет, так же много предложений, конференций, заявлений и «шумихи».

Но, к сожалению, для многих организаций банковской сферы по-прежнему существует масса вопросов: нужно ли им вообще что-то делать, все ли нужно делать, с чего начать, чтобы не прогадать, когда все это нужно успеть и т.д. и т.п.

Давайте последовательно разбираться.

ГДЕ БАНК, ГДЕ КИИ?

Проблемы кибербезопасности в наше время становятся особо актуальными. Последние компьютерные атаки показывают, что сейчас хакерские группировки переключаются, в том числе, на технологические системы. Чтобы ввести борьбу с этим злом в правовое поле, в России подготовлен и с 1 января 2018 года вступил в силу Федеральный закон № 187-ФЗ [1], регулирующий отношения в области обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак.

К субъектам КИИ в том числе были отнесены российские юридические лица, которым на праве собственности, аренды или на ином законном основании принадлежат:

- ♦ информационные системы (ИС),
- ♦ информационно-телекоммуникационные сети (ИТС),
- ♦ автоматизированные системы управления (АСУ),

функционирующие в банковской сфере и иных сферах финансового рынка, а также российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Сюда же, согласно Доктрине [2], входят и организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка.

Таким образом, банки (кредитные организации) и некредитные финансовые организации, в том числе осуществляющие функции в соответствии с Федеральным законом № 7-ФЗ [3], а также субъекты национальной платежной системы выступают субъектами КИИ, а их отдельные ИС, ИТС и АСУ — объектами КИИ, ряд которых может быть отнесен к значимым. Этот тезис подтверждает Банк России, в частности, такое подтверждение было озвучено на прошедшем юбилейном X Уральском форуме [4].

ТОЧКИ НА ДОРОЖНОЙ КАРТЕ

Ну, а если это так, то встает вопрос: что же надо делать, чтобы выполнить положения Федерального закона № 187-ФЗ [1] организациям банковской сферы.

На наш взгляд, в первую очередь, стоит выделить мух от котлет. Следует выделить 2 основных направления работ:

- ♦ как создать свой элемент и/или встроиться в существующую структуру ГосСОПКА,
- ♦ как провести категорирование объектов КИИ и обеспечить безопасность значимых объектов КИИ.

Вот второму блоку и связанным с ним активностям посвящена настоящая статья.

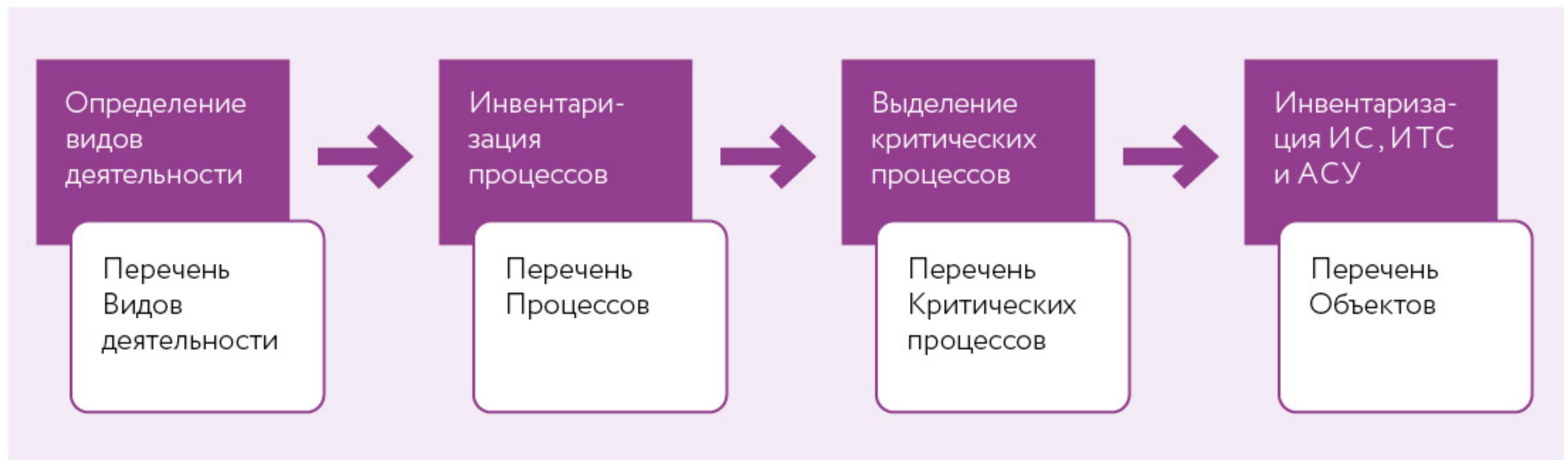
Обратим особое внимание, что согласно букве закона, ключевым моментом является то, что в первую очередь **требуется обеспечить безопасность значимых объектов КИИ**, то есть, прежде чем защищать объекты, необходимо понять, а есть ли вообще эти самые значимые объекты КИИ?

И как ни странно, первой точкой на дорожной карте будет не категорирование, которое активно обсуждается профессиональным сообществом, а инвентаризация (см. рис. 1)¹:

- ♦ существующих видов деятельности,
- ♦ существующих процессов,
- ♦ существующих ИС, ИТС и АСУ.

Дело в том, что несмотря на требование законодательства о том, что категорирование прово-

¹ Несмотря на то, что в п. 5 Правил [6] данные шаги включены в процесс категорирования, автором предлагается рассматривать их как отдельную задачу (проект), обусловленную значительной трудоемкостью и требующую участия работников организации, выходящих за пределы состава комиссии по категорированию.



дится комиссией, создаваемой субъектом КИИ, и четко описывается кто должен входить в эту комиссию, для работы такой комиссии необходимы первичные исходные данные. Но, как показывает уже накапливаемая практика, в 99% случаев такие данные отсутствуют или являются неактуальными.

Ну, а если учесть, что часть этих сведений требуется предоставить в ФСТЭК России, сбор и систематизация такой информации становится первоочередной задачей.

Кстати, только после этого можно поставить вторую точку на дорожной карте: только после уяснения всех процессов и идентификации систем/сетей в течение 1 года проводится категорирование.

Итак, с чего начать?

Начнется все с формирования перечня осуществляемых видов деятельности, а именно банковских операций и сделок, зафиксированных в уставе организации и имеющихся лицензиях (на выходе — «Перечень Видов деятельности»).

Далее, надо провести инвентаризацию всех управленческих, технологических, производственных, финансово-экономических и иных процессов и сформировать перечень реализуемых процессов (на выходе — «Перечень Процессов»).

Затем, среди этих процессов надо определить наиболее критические, то есть процессы, от нарушения которых может последовать ущерб, который можно будет позднее соотнести с критериями значимости, установленными Правительством РФ, а именно со среднестатистическим (по отношению к числу календарных дней в году) количеством осуществляемых операций, измеряемым в миллионах единиц:

- ◆ прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета;

- ◆ прекращение или нарушение проведения операций, осуществляемых организацией, яв-

ляющимся системно значимой кредитной организацией [7]²;

- ◆ прекращение или нарушение проведения операций оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем [8]³;

- ◆ прекращение или нарушение проведения операций системно значимой инфраструктурной организацией финансового рынка [9]⁴.

Правда, это не все, еще необходимо проследить соответствие по всем критериям, установленным Правительством РФ, в контексте конкретной организации, и только тогда, мы сможем сказать, что у нас есть окончательное решение (на выходе — «Перечень Критических процессов»).

И только после этого можно приступить к инвентаризации и формированию перечня всех ИС, ИТС и АСУ, обеспечивающих автоматизацию и информационное обеспечение критических процессов в вашей организации (на выходе — «Перечень Объектов»).

Далее именно объекты из Перечня Объектов уже можно категорировать. Сам Перечень Объектов направляется напрямую в ФСТЭК России, согласование с Банком России не требуется, т.к. последний не является государственным органом (т.е. п. 15 Правил [6] неприменим).

² АО ЮниКредит Банк, Банк ГПБ (АО), Банк ВТБ (ПАО), АО «АЛЬФА-БАНК», ПАО Сбербанк, ПАО «Московский Кредитный Банк», ПАО Банк «ФК Открытие», ПАО РОСБАНК, ПАО «Промсвязьбанк», АО «Райффайзенбанк», АО «Россельхозбанк».

³ АО КБ «ЮНИСТРИМ», ЗАО «НКК», ООО «ХэндиСолюшенс», ПАО АКБ «Связь-Банк», ООО «Платежная система «Виза», РНКО «Платежный Центр» (ООО), НКО АО НРД, ООО «Таможенная карта», «Мастеркард» ООО, ООО «Мультисервисная платежная система», Банк ВТБ (ПАО), ПАО Сбербанк, КБ «Геобанк» (ООО), ООО «БЭСТ», ООО «Цифровой Платеж», КИВИ Банк (АО).

⁴ НКО ЗАО «Национальный расчетный депозитарий» и ЗАО АКБ «Национальный Клиринговый Центр».

Рисунок 1. Шаги в рамках инвентаризации



Рисунок 2. Временная дорожная карта

Временной точкой отсчета всех дальнейших шагов выступает дата утверждения Перечня Объектов⁵ (см. рис. 2).

Приступая к непосредственно категорированию объектов КИИ, сначала надо провести полноценное моделирование угроз безопасности информации, а именно:

- ◆ рассмотреть возможные действия нарушителей в отношении объектов, а также иные источники угроз безопасности информации,
- ◆ проанализировать угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ.

Стоит отметить, что ГОСТ 57580.1 [10], который станет актуален для всех организаций финансовой сферы после внесения изменений в Федеральный закон № 86-ФЗ [11], определяет, что разработанные и утвержденные модели

⁵ Сроки формирования Перечня Объектов не определены, мы предлагаем ориентироваться на 2018 год. Позиция ФСТЭК России: если организации добровольно не начнут формировать данные перечни, то ФСТЭК России рассмотрит вопрос введения конкретного срока и административных мер за его несоблюдение.

угроз и нарушителей безопасности информации выступают в качестве основы для реализации финансовой организацией системы защиты информации. В данном случае мы предлагаем осуществлять моделирование угроз безопасности информации, учитывая положения и Правил [6], и ГОСТ [10].

Только имея всю указанную выше фактуру на руках, можно переходить непосредственно к сопоставлению для каждого отдельно взятого объекта КИИ организации, то есть для каждой (и это важно!) ИС, ИТС и АСУ, масштаба возможных последствий в случае возникновения компьютерных инцидентов со значениями показателя(ей), определенного(ых) в Правилах [6], и делать вывод о присвоении объекту одной из категорий значимости либо об отсутствии необходимости данного присвоения.

МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА КИИ

Когда разговор заходит о реализации мер по обеспечению безопасности значимого объекта, у специалистов может возникнуть резонный

вопрос: в связи с тем, что в форме сведений [5] для ФСТЭК России предусмотрены данные о:

- ♦ применяемых средствах защиты информации,
- ♦ функциях безопасности программного обеспечения, если в него встроены средства защиты информации,
- ♦ организационных мерах,
- ♦ технических мерах,

нужно ли успеть реализовывать положения приказов ФСТЭК России [11,12] до окончания процедуры категорирования?

Ответ: нет, организация подает сведения только о мерах, принятых на момент проведения категорирования. Дело в том, что категория значимости выступает неотъемлемой составляющей первичного документа для системы безопасности значимых объектов (СБЗО) — Технического задания.

При этом нужно учитывать, что основой для принятия решения в рамках категорирования является размер ущерба, который может быть причинен в результате возникновения компьютерных инцидентов. Если организация обладает определенным набором организационных и технических мер защиты информации, то может быть обоснована невозможность наступления определенных компьютерных инцидентов в результате реализации угроз безопасности информации вследствие неактуальности последних.

В связи с этим мы предлагаем начинать работу по обеспечению безопасности объектов, получая уже первые результаты в процессе категорирования, т.е. последовательно и планомерно расширять (масштабировать) область действия существующей системы защиты информации или создаваемой СБЗО.

В значимых объектах в зависимости от их категории значимости и угроз безопасности информации должны быть реализованы следующие организационные и технические меры [11]:

- ♦ идентификация и аутентификация (ИАФ),
- ♦ управление доступом (УПД),
- ♦ ограничение программной среды (ОПС),
- ♦ защита машинных носителей информации (ЗНИ),
- ♦ аудит безопасности (АУД),
- ♦ антивирусная защита (АВЗ),
- ♦ предотвращение вторжений/компьютерных атак (СОВ),
- ♦ обеспечение целостности (ОЦЛ),
- ♦ обеспечение доступности (ОДТ),
- ♦ защита технических средств и систем (ЗТС),
- ♦ защита системы (сети) и ее компонентов (ЗИС),

МЫ ПРЕДЛАГАЕМ НАЧИНАТЬ РАБОТУ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБЪЕКТОВ, ПОЛУЧАЯ УЖЕ ПЕРВЫЕ РЕЗУЛЬТАТЫ В ПРОЦЕССЕ КАТЕГОРИРОВАНИЯ

- ♦ реагирование на инциденты информационной безопасности (ИНЦ),
- ♦ управление конфигурацией (УКФ),
- ♦ управление обновлениями программного обеспечения (ОПО),
- ♦ планирование мероприятий по обеспечению безопасности (ПЛН),
- ♦ обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС),
- ♦ информирование и обучение персонала (ИПО).

Этапы выполнения работ классические, завязанные на жизненный цикл систем [11]:

- ♦ установление требований к обеспечению безопасности значимого объекта,
- ♦ разработка организационных и технических мер по обеспечению безопасности значимого объекта,
- ♦ внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие,
- ♦ обеспечение безопасности значимого объекта в ходе его эксплуатации,
- ♦ обеспечение безопасности значимого объекта при выводе его из эксплуатации.

А непосредственно дальнейшее функционирование СБЗО вкладывается в цикл непрерывного совершенствования [12], уже знакомый организациям банковской сферы:

- ♦ планирование и разработка мероприятий,
- ♦ реализация (внедрение) мероприятий,
- ♦ контроль состояния безопасности значимых объектов,
- ♦ совершенствование безопасности значимых объектов.

КТО ИДЕТ ПО МАРШРУТУ?

В состав комиссии по категорированию включают [6]:

- ♦ руководителя субъекта КИИ (председатель совета директоров организации) или уполномоченное им лицо,
- ♦ специалистов в области выполняемых функций или осуществляемых видов деятельности (представители бизнес подразделений),
- ♦ специалистов в области информационных технологий и связи (ИТ-специалисты),

- ◆ специалистов по эксплуатации основного технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов (технологии, если есть),

- ◆ специалистов, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов КИИ (ИБ-специалисты),

- ◆ специалистов подразделения по защите государственной тайны (в случае, если в объекте КИИ обрабатывается информация, составляющая государственную тайну),

- ◆ специалистов структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или уполномоченный по ГО и ЧС.

В случае если один или несколько объектов КИИ организации определены как значимые объекты КИИ [12], то возникает необходимость определения ответственного лица, на которое будут возложены следующие функции обеспечения безопасности значимых объектов КИИ:

- ◆ создание СБЗО,
- ◆ организация функционирования СБЗО,
- ◆ контроль функционирования СБЗО.

Плюс, должно быть сформировано структурное подразделение по безопасности или выделены отдельные специалисты, которые:

- ◆ разрабатывают предложения по совершенствованию локальных актов,

- ◆ проводят анализ угроз безопасности информации и выявляют уязвимости,

- ◆ обеспечивают реализацию требований по обеспечению безопасности,

- ◆ обеспечивают реализацию организационных мер защиты информации,

- ◆ осуществляют реагирование на компьютерные инциденты,

- ◆ организуют проведение оценки соответствия,

- ◆ готовят предложения по совершенствованию функционирования СБЗО.

Целесообразно коррелировать данные назначения с уже существующими в Вашей организации ИБ-специалистами, а также использовать это как дополнительный драйвер для расширения штата и бюджета ИБ-подразделения.

* * *

В заключение хочется еще раз отметить, что первым шагом для организаций банковской сферы является именно инвентаризация процессов, а не непосредственно категорирование систем или сетей «по таблице». Само же категорирование является ключевой развилкой, определяющей весь дальнейший маршрут обеспечения безопасности объектов КИИ организации банковской сферы, при этом своевременная и полноценная реализация мер защиты информации играет здесь ключевую роль.

ЛИТЕРАТУРА

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
2. Доктрина информационной безопасности Российской Федерации, утверждена указом Президента Российской Федерации от 05.12.2016 г. № 646.
3. Федеральный закон от 07.02.2011 № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте».
4. «Финансовая организация как субъект критической информационной инфраструктуры», презентация заместителя начальника Управления Главного управления безопасности и защиты информации Банка России, А. О. Выборнова.
5. Форма «Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий», утверждена приказом ФСТЭК России от 22.12.2017 г. № 236.
6. Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утверждены постановлением Правительства Российской Федерации от 08.02.2018 № 127.
7. Центральный банк Российской Федерации (Банк России). Пресс-служба «Информация. Об утверждении перечня системно значимых кредитных организаций» от 13.09.2017.
8. Реестр операторов платежных систем на 04.05.2018 (<http://www.cbr.ru/PSystem/rops/>)
9. Центральный банк Российской Федерации (Банк России). Пресс-служба «Информация. О признании инфраструктурных организаций финансового рынка системно значимыми» от 26.09.2014.
10. ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержден и введен в действие приказом Росстандарт от 08.08.2017 № 822-ст.
11. Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 № 86-ФЗ.
12. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждены приказом ФСТЭК России от 25.12.2017 № 239.
13. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утверждены приказом ФСТЭК России от 21.12.2017 № 235.

РАБОТАЕМ НА ПЕРСПЕКТИВУ

ОТЧЕТ С ДИСКУССИИ НА PHDAYS 2018
«БЕЗОПАСНОСТЬ КИИ: ПРАКТИЧЕСКИЕ АСПЕКТЫ»



Анна ВОРОБЬЕВА
корреспондент
BIS Journal

Тема реализации Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ) РФ» все еще на волне хайпа. Ее обсуждают на каждом экспертном ИБ-мероприятии. Особенно интересной и полезной нам показалась дискуссия, состоявшаяся на секции «Безопасность КИИ: практические аспекты» на Positive Hack Days 2018.

Закон вступил в силу полгода назад, а на ключевой вопрос о принадлежности к субъектам КИИ до сих пор нет однозначного ответа. В очередной раз участники дискуссии попытались разобраться в этом самостоятельно.

В обсуждении приняли участие начальник отдела эксплуатации и поддержки систем информационной безопасности «Ростелекома» Дмитрий Царев, директор департамента мо-

нитинга и реагирования на киберугрозы «Ростелекома» Владимир Шадрин, директор по развитию бизнеса Роман Кобцев (ГК «ИнфоТеКС»), генеральный директор R-Vision Александр Бондаренко, руководитель группы пресейла JSOC компании Solar Security Алексей Павлов, менеджер по продвижению продуктов Positive Technologies Сергей Куц, консультант по информационной безопасности компании «ICL Системные технологии» Руслан Замалиев.

ЧТО ЯВЛЯЕТСЯ КИИ?

Официальное трактование субъектов КИИ довольно широкое, что для многих становится проблемой. К тому же существуют разногласия в формулировках самих регуляторов — ФСБ и ФСТЭК. Среди тех, кто оказался на распутье «быть или не быть» — МЧС России. Представи-



Дискуссия на секции «Безопасность КИИ: практические аспекты» на Positive Hack Days 2018

тель ведомства обратился за помощью к экспертам с просьбой помочь разъяснить, является ли их структура субъектом КИИ. Согласно правилам категорирования, МЧС России принадлежит к таковым, а по определению — нет. Дать однозначный ответ участники сессии не смогли, поэтому было предложено идентифицировать себя самостоятельно.

Отечественная нормативная база, необходимая для ФЗ-187, только на старте. Правительство утвердило 100% документов по КИИ, ФСТЭК — 90%, ФСБ — только 20%. Компаниям, по мнению участников дискуссии, нужно настраиваться на «долгосрочный тренд в этом направлении», а не «бежать впереди паровоза». Была проведена аналогия с Законом о персональных данных, которому более 10 лет, а требования к его исполнению все еще меняются. В итоге те, кто первым стремился идти в ногу с законом, теряли немалые деньги.

КАТЕГОРИРОВАНИЕ КРУПНЫХ СУБЪЕКТОВ КИИ

Крупные отечественные компании уже приступили к выполнению Закона о КИИ, однако столкнулись с весомой проблемой — необходимостью проведения категорирования множества объектов, расположенных в территориально-распределенных филиалах.

По мнению участников обсуждения, если субъект КИИ имеет разветвленную сеть территориальных подразделений, целесообразно провести предварительную методическую работу по категорированию в центральном офисе. Прежде всего сформировать перечень всех подразделений, бизнес-процессов, а затем привязать их к региональным офисам. После чего выработать методические рекомендации по категорированию, в том числе, с описанием типизации объектов КИИ, и, если это возможно, разработать шаблоны документов (перечень объектов КИИ, подлежащих категорированию, акты категорирования, сведения, передаваемые во ФСТЭК по результатам категорирования).

Не стоит забывать про контрольную функцию — внедрить данные наработки в террито-

риальные подразделения, предварительно опробовав их на одном-двух офисах, сформировать перечень объектов КИИ, подлежащих категорированию, осуществить моделирование угроз для объектов КИИ из данного перечня, провести категорирование и сформировать на основе шаблонов отчетные документы.

Свою помощь активно предлагают коммерческие компании. К примеру, представитель «ICL Системные технологии» рассказал о системе, автоматизирующей процессы категорирования информационных систем и выпуска необходимой документации.

Категорирование влияет на объем выполняемых требований, поэтому изначально стоит, проанализировав постановления Правительства, попытаться изменить внутренние процессы так, чтобы «уйти от значимости или уменьшить свою категорию», — высказал мнение Александр Бондаренко.

Пока в России нет ни одной компании, которая прошла бы полный путь и выполнила все требования по КИИ. Поэтому, по мнению Бондаренко, необходимо выстраивать долгосрочную стратегию, учитывая, что все документы до конца не приняты. «Хотеть реализовать данный проект за полгода достаточно наивно. Эффективнее разбить его на несколько лет и расставить правильные приоритеты», — посоветовал гендиректор R-Vision.

ОПЫТ СУБЪЕКТОВ КИИ

Все игроки «большой четверки» операторов ведут активные работы по категорированию. На площадке Ассоциации документальной электросвязи совместно разрабатывается единый отраслевой стандарт для упрощения подходов и методик категорирования. «ФСБ и ФСТЭК поддерживают данную идею, поскольку в один прекрасный момент они могут утонуть в зоопарке подходов и методик к категорированию», — заметил руководитель Центра компетенции по безопасности КИИ «МегаФон» Дмитрий Афанасьев.

Еще в начале года оператор создал подразделение компетенции по защите КИИ и выделил штатные единицы. Филиальные подразделения «Мегафон» активно налаживают контакты с инфраструктурой. Главная проблема — широкая географическая сеть и множество объектов, которые подходят под категорию КИИ (вплоть до вышек с базовыми станциями). Чтобы решить проблему распределенной инфраструктуры, на уровне ЦОДов компания вводит типовые доверенные зоны по регионам.

Укрепляя оборону, оператор сотовой связи переходит на новую SIEM-платформу, а так-

**ОТЕЧЕСТВЕННАЯ НОРМАТИВНАЯ
БАЗА, НЕОБХОДИМАЯ ДЛЯ
ФЗ-187, ТОЛЬКО НА СТАРТЕ.
ПРАВИТЕЛЬСТВО УТВЕРДИЛО 100 %
ДОКУМЕНТОВ ПО КИИ, ФСТЭК —
90 %, ФСБ — ТОЛЬКО 20 %**

же строит собственный СОС. «Все требования ФЗ-187 планируется полностью реализовать к концу 2019 года», — заверил Афанасьев.

Начальник Управления режима ИБ Газпромбанка Алексей Плешков большой проблемы в реализации закона пока не видит, поскольку отечественные банки с 2004 года на плановой основе ведут аналогичную работу с Банком России, в том числе через ФинЦЕРТ. Сейчас главная задача — сопоставить требования регулятора и Закона о КИИ.

Тем не менее проблемы при внедрении ФЗ-187 в банковской сфере тоже существуют. Например, отсутствие в банках ниже ТОП-50 должного кадрового уровня. Плешков посоветовал малым и средним банкам задуматься о расширении персонала, ответственного за реализацию требований КИИ.

Представитель энергетического холдинга «Интер РАО» Дмитрий Васильев заметил, что пока неясно, как распределить ответственность за безопасность объектов КИИ, если крупная компания привлекает подрядчиков. «Не всегда отраслевой регулятор может выступать локомотивом и снабжать подведомственные организации необходимыми методиками и инструкциями по категорированию, а также участвовать в составе комиссии по категорированию, как это предписывает 127-ПП», — отметил Васильев. Поэтому в их компании, не дождавшись реакции от отраслевого регулятора, приступили к работам самостоятельно: разработали методические рекомендации по категорированию, составили комиссию, утвердив ее приказом и наделив участников определяющими функциями. В данный момент организация формирует перечень объектов КИИ, подлежащих категорированию.

ВЗАИМОДЕЙСТВИЕ С ГОССОПКА

Для реализации закона, помимо категорирования объектов КИИ, важно формализовать их присоединение к ГосСОПКА, создать или модернизировать собственные системы информационной безопасности значимых объектов КИИ.

Пока взаимодействие с ГосСОПКА добровольное, однако со временем станет обязательным. На данный момент к государственной системе подключились более 1,5 тысяч объектов КИИ.

В 2017 году с участием ГосСОПКА было собрано более 300 серьезных компьютерных инцидентов, что более чем в пять раз больше показателя 2016 года. При содействии центра было заблокировано свыше 3 тыс. вредоносных ресурсов.

Работа ГосСОПКА строится по двум основным направлениям: агрегация потоков ИБ-инцидентов, с которыми организации справились,

ДЛЯ РЕАЛИЗАЦИИ ЗАКОНА, ПОМИМО КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КИИ, ВАЖНО ФОРМАЛИЗОВАТЬ ИХ ПРИСОЕДИНЕНИЕ К ГОССОПКА

и помощь в устранении компьютерных инцидентов. Также ФСБ собирает информацию от участников системы, какую информацию об инцидентах им необходимо получать, чтобы «не зафлудить и соблюсти баланс».

Эксперты обратили внимание, что существует различие в формулировках ФСТЭК и ФСБ России понятия «компьютерный инцидент». Представитель Национального координационного центра по компьютерным инцидентам (НКЦКИ) Алексей Новиков пояснил, что имеется в виду нарушение штатного режима работы всей системы или ее элемента. А проблема состоит скорее не в самом определении, а в типизации инцидентов (сейчас определено 12 типов). Мнение ФСТЭК, к сожалению, не прозвучало. И тут мнение экспертов, конечно, едино: больше хотелось бы не слов представителей регулятора, которые к делу не подошьешь, а официальных документов.

Однако Новиков заверил, что ФСБ уже работало, но пока не открыло доступ к разъяснениям, что считать инцидентом без привязки к конкретной сфере. Также уже есть документ, разработанный НКЦКИ, описывающий форматы передачи данных в ГосСОПКА. Его можно получить по запросу в НКЦКИ.

Перечень информации, передаваемой в ГосСОПКА приведен в соответствующем проекте приказа ФСБ («Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»). Проект будет утвержден и передан в Минюст в течение месяца.

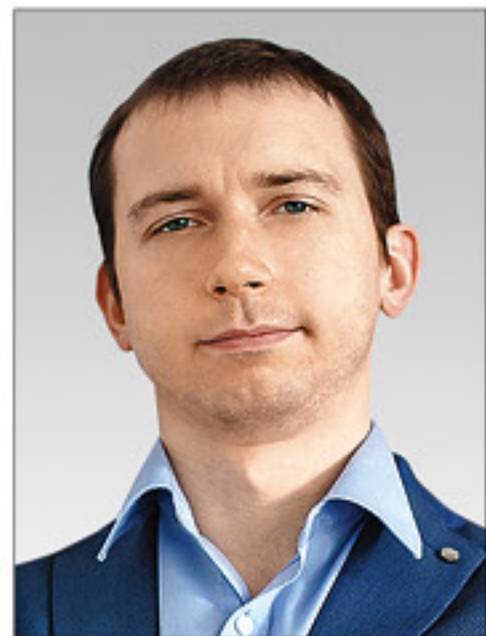
* * *

Участники дискуссии сошлись во мнении, что реализация, как и применение, ФЗ-187 только в начале длинного и тернистого пути, поскольку ещё ни одна организация в стране не прошла полный цикл подготовки к его выполнению. К тому же существует проблема несоответствия терминологии. Но выполнять требования компании обязаны уже сейчас, поэтому и действуют они самостоятельно и с энтузиазмом. Понятно, это в их интересах.

Но и в интересах государства тоже.

МОЖЕТ ЛИ ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ПО ЗАЩИТЕ КИИ ПОВЫСИТЬ РИСКИ ИБ?

КАК СДЕЛАТЬ ТАК, ЧТОБЫ ЭТОГО НЕ ПРОИЗОШЛО



Павел КОРОСТЕЛЕВ
руководитель
отдела продвижения
продуктов компании
«Код безопасности»

Закон «О безопасности критической информационной инфраструктуры» всколыхнул всю российскую отрасль ИБ. Широкая область действия и критерии категорирования, жесткие меры по защите значимых объектов КИИ, а также риск уголовной ответственности не только за атаки, но и за ненадлежащую защиту, приковали внимание тысяч организаций к этой теме. Однако инвестиции в защиту КИИ могут парадоксальным образом ухудшить общий уровень информационной безопасности. Необходимость выполнения множества требований повлечет за собой внедрение дополнительных средств обеспечения ИБ. Необходимо будет набрать персонал, как для администрирования этих средств, так и для мониторинга. При этом, согласно приказу № 235 ФСТЭК России, эти сотрудники не могут совмещать функции работников ИТ- и ИБ-отделов. Они должны заниматься именно ИБ, а в идеале, только ИБ объектов КИИ.

Понятно, что субъекты КИИ, особенно в регионах, будут неохотно выделять дополнительные штатные единицы под эти задачи, что выльется в перегруженность специалиста по обеспечению ИБ задачами по администрированию и настройке средств защиты, а также отслеживанию потенциальных инцидентов. В вышеупомянутом 235-м приказе перечислено семь различных типов средств защиты, то есть администратору придется кроме непосредственно мониторинга ИБ тратить время на семь различных консолей управления и решение вопросов эксплуатации этих средств. В таких условиях возрастает вероятность сбоя в работе всего объекта КИИ, вызванного, например, ошибкой администратора, несовместимостью средств обеспечения ИБ между собой или атакой злоумышленника, признаков которой администратор не заметил.

Что же делать, чтобы инвестиции в безопасность КИИ принесли пользу?

КОМПЛЕКСНЫЙ ПОДХОД

Необходим комплексный подход для защиты всех элементов инфраструктуры с помощью ми-

нимального количества продуктов. Только это вместе с удобным централизованным управлением повысит эффективность защиты объектов КИИ в условиях крайне ограниченного времени специалистов и снизит вероятность ошибок.

Подход включает в себя три направления:

- ♦ повышение эффективности работы администратора;
- ♦ защита сетевой инфраструктуры вне зависимости от размера, производительности и среды;
- ♦ комплексная защита как физических, так и виртуальных серверов.

Подход реализуется с помощью нескольких продуктов компании «Код Безопасности»:

- ♦ АПКШ «Континент» для защиты сетевой инфраструктуры и создания каналов связи с шифрованием по алгоритмам ГОСТ;
- ♦ СОВ «Континент» для обнаружения и предотвращения вторжений в сетевую инфраструктуру и интеграции с ГосСОПКА;
- ♦ Secret Net Studio для комплексной защиты рабочих станций серверов и виртуальных машин;
- ♦ vGate для защиты и сегментации виртуальной инфраструктуры, а также фильтрации трафика в виртуализованных сетях.

Как эти продукты помогут защитить объекты КИИ?

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ АДМИНИСТРАТОРА

В условиях динамично развивающейся инфраструктуры, дефицита компетентных специалистов и высокой цены ошибки необходимо внедрять в систему защиты принципы автоматизации. Политика безопасности должна применяться к элементам инфраструктуры автоматически, а администратор — тратить минимум действий на ее изменение. Исключение ручных рутинных операций значительно снизит риск простоя системы по вине администратора.

Приказ ФСТЭК России № 239 описывает более 150 мер, которые необходимо выполнить для защиты объекта КИИ, при этом заказчик



сначала должен их выполнить, а потом регулярно проводить аудит для контроля исполнения. И процедура первичной настройки, и процедура внутреннего аудита требуют от обслуживающего персонала дополнительных ресурсов, поэтому используемые средства защиты должны иметь предустановленные шаблоны настроек, которые позволят быстро внедрить их в соответствии с требованиями ФСТЭК, а также оперативно и без дополнительных затрат продемонстрировать выполнение требуемых мер.

Этот механизм реализован в продуктах Secret Net Studio и vGate. Он позволяет использовать существующий или создать собственный шаблон настроек безопасности на основе требований ФСТЭК, чтобы сэкономить ресурсы, с одной стороны, при внедрении системы защиты, а с другой — при прохождении аудита на соответствие настроек требованиям 239-го приказа ФСТЭК.

ЗАЩИТА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Усложнение сетевой инфраструктуры, сопряжение технологических и офисных сетей, а также повышение пропускной способности вну-

тренней сети накладывают дополнительные требования на подсистему защиты сетевой инфраструктуры. Согласно требованиям 239-го приказа, каждый значимый объект КИИ должен быть выделен в отдельный сетевой сегмент и закрыт межсетевым экраном. Если объект КИИ обменивается с другими элементами инфраструктуры большими объемами трафика, межсетевой экран может сам по себе стать бутылочным горлышком, что негативно повлияет на технические процессы, обслуживаемые объектом КИИ. В других случаях, чтобы добиться подобной производительности можно пожертвовать уровнем журналирования или количеством правил фильтрации трафика — это повысит производительность, но снизит уровень безопасности.

При использовании новой версии АПКШ «Континент» 3.9 нет необходимости жертвовать безопасностью ради производительности. Пропускная способность межсетевого экрана этой наиболее производительной на данный момент платформы превышает 10 Гбит/с, что позволяет обеспечить эффективную фильтрацию трафика.

Отдельной проблемой является межсетевое экранирование в виртуализованных сетях. Высокая скорость изменений виртуальной инфраструктуры делает фильтрацию на основе IP-адреса виртуальных машин малоэффективной, при этом затрудняется фильтрация трафика между двумя виртуальными машинами. Ответом может стать виртуальный межсетевой экран, но злоумышленникам по силам обойти эту меру. Для эффективной защиты лучше всего использовать межсетевой экран уровня гипервизора, который обеспечивает фильтрацию трафика не только на основе традиционных атрибутов (IP-адреса и порта), но и специфических для виртуальной среды. Такой межсетевой экран реализован в механизме vFirewall, включенном в продукт vGate: он позволяет создавать правила фильтрации трафика на основе меток безопасности vGate или имени виртуальной машины. Важной особенностью vGate vFirewall является низкая нагрузка на процессор хоста гипервизора.

Таким образом, средства защиты сети позволяют фильтровать трафик даже в высокопроизводительных сетях, не влияя на работу всей сетевой инфраструктуры субъекта КИИ.

ЗАЩИТА СЕРВЕРНОЙ ИНФРАСТРУКТУРЫ

Серверы и рабочие станции из состава объектов КИИ обеспечивают те самые процессы, которые необходимо защищать. Они являются «последней линией обороны». Применение обычных антивирусов на подобных системах неэффективно, так как в продвинутых атаках используются образцы вредоносного программного обеспечения, неизвестные разработчикам средств защиты. Эвристические способы поиска вредоносного ПО генерируют слишком большой «белый шум», который отвлекает на себя внимание администратора ИБ. Эффективной стратегией защиты будет своевременное обновление и устранение уязвимостей как в ОС, так и в прикладном ПО. Однако в реальности этот путь работает далеко не всегда, так как у субъекта КИИ часто может не быть ресурсов для тестирования всех обновлений либо технологические окна для развертывания обновлений могут быть очень короткими и редкими.

Для эффективной защиты конечных точек необходимо применить принцип «Default Deny», который предполагает явное указание доверенных процессов и контроль их целостности. В этом случае любой неавторизованный процесс или несанкционированное изменение процесса будет считаться инцидентом ИБ. Этот прин-

цип реализован в механизмах контроля целостности объектов ОС и замкнутой программной среды в Secret Net Studio.

Но что делать, если используется не физический сервер, а виртуальная машина? Ведь если злоумышленник скомпрометирует всю виртуальную инфраструктуру, он получит неограниченные права доступа буквально к каждой машине. Некоторые компании в этом случае разделяют виртуальную среду на несколько независимых сегментов: виртуальные машины с разным уровнем доверия физически разнесены на разные хосты гипервизоров. Однако такой подход требует дополнительных ресурсов со стороны администраторов виртуальной среды, а также снижает ту самую гибкость, ради которой и внедряется виртуализация серверов.

Более эффективным подходом станет защита виртуальной инфраструктуры с помощью наложенных средств. В этом случае для эффективной защиты необходимо контролировать несколько направлений:

- ♦ контроль безопасности настроек виртуальной среды;
- ♦ разделение виртуальных машин по нескольким контурам безопасности;
- ♦ разграничение доступа и контроль действий администратора виртуальной среды.

Эти механизмы реализованы в продукте vGate. Кроме сегментации виртуальной среды vGate может реализовать «принцип четырех глаз», когда определенные команды администратора виртуальной среды не будут выполнены без согласования администратора безопасности.

* * *

Защита критической информационной инфраструктуры — это сложная и трудоемкая задача. Зачастую она требует переосмысления всех элементов стратегии ИБ в организации. Суровое наказание в случае невыполнения требований и пристальное внимание к теме со стороны регуляторов не позволяют спустить тему «на тормозах». Но при правильном подходе проект по защите КИИ — это возможность значительно усилить уровень информационной безопасности предприятия. Комплексное применение продуктов «Кода безопасности» позволяет достичь этой цели оптимальным образом. Такой путь обеспечивает высокий уровень защиты объектов КИИ, а также экономит время и силы администраторов ИБ.

Finopolis – крупнейшее событие в области финтеха в России

- / Все лидеры финансового и ИТ-рынков, e-commerce, представители Банка России и органов власти, науки и образования на одной площадке.
- / Обсуждение горячих трендов развития, инициатив и проектов в области финансовых технологий и дигитализации экономики.
- / Презентация новейших отечественных и зарубежных технологических продуктов и инфраструктурных решений.

КЛЮЧЕВЫЕ ТЕМЫ

- / Цифровая трансформация: успеваем ли мы?
- / «Цифра» для потребителя
- / Fast loan decision: новаторские решения в финансовых услугах населению и малому бизнесу
- / Регулятивная «песочница»: игра без правил или правила игры
- / Homo technologicus. Какой он?
- / Рынки капитала: победили ли роботы?
- / Новинки InsurTech: новая модель отношений с клиентами
- / RegTech и SupTech: направления развития
- / Маркетплейс: больше платформ хороших и разных
- / Кибербезопасность: цифровой иммунитет рынка
- / И другие

/ Подробности и регистрация на **finopolis.ru**

Специальные условия при
регистрации до 10 августа

Организатор:



Банк России

 РОСКОНГРЕСС

Реклама 6+



Анатолий АКСАКОВ
председатель Комитета
Государственной Думы
РФ по финансовому
рынку

ДОЛГОЖДАНИЕ ПЕРЕМЕНИ К ЛУЧШЕМУ

ВОЗМОЖНОСТИ БАНКОВ
ПРЕДУПРЕЖДАТЬ ХИЩЕНИЯ ДЕНЕЖНЫХ
СРЕДСТВ СУЩЕСТВЕННО РАСШИРЯЮТСЯ



Принятый Государственной Думой РФ и подписанный Президентом РФ Федеральный закон от 27 июня 2018 года №167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» расширяет полномочия как Банка России, так и операторов платежей, в частности, банков. Центробанк должен будет формировать общую базу данных подобных инцидентов, а операторы платежей наделяются правом определять и приостанавливать подозрительные транзакции. В новом законе закрепляются нормы и процедуры регулирования этой деятельности.

ЗЛОУМЫШЛЕННИКИ МЕШАЮТ РОСТУ

В последние годы наблюдается устойчивая тенденция роста числа несанкционированных операций, совершенных с использованием систем дистанционного банковского обслуживания — ДБО. По информации Банка России, в 2016 году было совершено порядка 300 000 несанкционированных операций с использованием платежных карт, эмитированных российскими кредитными организациями, на общую сумму более 1 млрд рублей. При постепенном сокращении доли несанкционированных операций, осуществляемых с использованием банкоматов и платежных терминалов, наблюдается устойчивый рост числа несанкционированных операций,

осуществленных посредством сети интернет и устройств мобильной связи.

В 2016 году в Банк России была представлена информация о 717 несанкционированных операциях со счетов юридических лиц на общую сумму 1,89 млрд рублей. При этом более 50 % всех попыток осуществить несанкционированный перевод денежных средств со счетов юридических лиц прошли успешно, т.е. денежные средства были списаны со счета клиента полностью или частично.

По прогнозам Банка России и экспертов, в 2017–2018 годах ожидается дальнейший рост числа атак на счета клиентов, в том числе через платежные системы, платформы для оплаты государственных услуг, средства мобильной связи и системы ДБО. Необходимо отметить, что методы и технические средства, оборудование и программное обеспечение, используемые мошенниками для проведения несанкционированных операций, постоянно совершенствуются. Также в настоящее время наблюдаются процессы самоорганизации мошенников, создания ими разветвленных (в том числе, транснациональных) группировок, что создает дополнительные предпосылки для роста числа несанкционированных операций.

Учитывая изложенное, в настоящее время многими кредитными организациями активно проводится политика, направленная на предотвращение несанкционированных операций до наступления окончательности перевода денежных средств. В том числе осуществляется текущий анализ операций с использованием различных систем фрод-мониторинга, а также информирование клиентов о рисках, что позволяет уже сейчас останавливать более 50 % всего объема несанкционированных операций в системах ДБО.

Борьба с мошенничеством в сфере использования электронных средств платежа должна носить комплексный характер, затрагивая как правовые, так и технические аспекты данной противоправной деятельности. В этой связи необходимо отметить создание в Банке России Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТа), в который в настоящее время добровольно представляют информацию о хищениях денежных средств со счетов клиентов порядка 365 кредитных организаций.

ХИЩЕНИЯ ПРОЩЕ ПРЕДОТВРАЩАТЬ

Увеличение доли и объемов электронных расчетов, которым препятствует киберпреступность в финансовой сфере, является значимым фактором экономического роста. Поэтому законодательное решение указанных проблем превратилось в насущную задачу, и работа над законопроектом в Государственной Думе РФ велась динамично. Законопроект был представлен на заседании 17 января 2018 года официальным представителем Правительства России, заместителем министра финансов РФ А.В. Моисеевым и прошёл первое чтение, 22 мая был принят во втором и 5 июня — оконча-

БАНКАМ ПРЕДОСТАВЛЯЕТСЯ ВОЗМОЖНОСТЬ ПРЕДПРИНИМАТЬ ПРЕВЕНТИВНЫЕ МЕРЫ, А ИМЕННО БЛОКИРОВАТЬ ОПЕРАЦИИ, КОТОРЫЕ СОДЕРЖАТ ПРИЗНАКИ ХИЩЕНИЙ

тельно в третьем чтении. 27 июня он был подписан Президентом и стал законом №167-ФЗ.

Закон № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации (в части противодействия хищению денежных средств)» направлен на формирование механизма противодействия несанкционированным переводам денежных средств, не требующего существенных временных и финансовых трудовых затрат. Это будет важным шагом к созданию унифицированной комплексной системы противодействия любым несанкционированным операциям на финансовом рынке, которая в дальнейшем может быть распространена и на другие сектора финансового рынка — рынок ценных бумаг, страховой рынок и т.д.

Закон № 167-ФЗ призван решить две большие проблемы, с которыми мы сталкиваемся, когда противодействуем злоумышленникам. Действующее законодательство ставило банкам и платёжным системам жёсткие сроки осуществления транзакций по платёжным поручениям клиентов. Тем самым, в случае наличия признаков попытки хищения, не оставалось времени на разбирательство и получение дополнительных подтверждений подлинности платежа. Вторая проблема заключалась в том, что действующее законодательство не допускало формирования полноценной единой базы подобных инцидентов, участников схем хищения, юридических и физических лиц.

Ограничения накладывались нормами ряда федеральных законов, затрудняя межбанковское взаимодействие в противодействии злоумышленникам. Закон № 167-ФЗ призван устранить эти препятствия, создав комплексный правовой механизм противодействия переводам денежных средств без согласия клиента. Предусмотрено внесение изменений в ряд федеральных законов.

ПРИЗНАКИ СОМНИТЕЛЬНОСТИ

Банкам предоставляется возможность предпринимать превентивные меры, а именно блокировать операции, которые содержат признаки хищений. Срок блокировки для проведения расследования определён до двух суток. Таким образом, предупреждается сама возможность хищений, в то время как ранее для этого приходилось разыскивать и возвращать похищенные деньги.

Перечень признаков несанкционированных операций устанавливается главным регулятором финансовой сферы, Банком России. В случае, если параметры платёжного поручения подпадают под эти признаки, банк обязан приостановить подозрительную транзакцию и заблокировать

электронное средство платежа на срок до двух дней. В первоначальном тексте законопроекта существовали положения о праве банков устанавливать дополнительные признаки сомнительных операций. Вокруг этой темы была острая полемика, так как это могло привести к формированию разных подходов к практике антифрода и стать причиной ущемления прав клиентов банков. В итоге решили такого права не давать. Банки будут пользоваться единым перечнем признаков сомнительных операций от Банка России. При этом банки будут применять эти признаки с учетом профиля своих клиентов.

Это значит, что, если с Каймановых островов приходит распоряжение о списании денег с карточки бабули, которая живет в Подмосковье, то понятно, что это скорее всего несанкционированная транзакция. А если такое распоряжение касается счета клиента, который часто передвигается и ведет бизнес, то это совсем другая история.

Для того, чтобы оператор осуществил приостановленный перевод денежных средств и отменил блокировку электронного средства платежа, потребуется незамедлительно получить согласие клиента на осуществление этих действий. Такое подтверждение может быть получено способами, предусмотренными внутренними регламентами банка и договором обслуживания клиента: посредством телефонного звонка, СМС и другими способами связи. На проведение этих процедур закон отводит срок до двух дней.

ПРОЦЕДУРЫ ВОЗВРАЩЕНИЯ ДЕНЕГ

Процедура возвращения денег клиентам — физическим лицам, похищенных в результате не санкционированного клиентом перевода и снятия денежных средств, давно уже действует, согласно ст. 9 Федерального закона «О национальной платежной системе» от 27 июня 2011 года № 161-ФЗ. Если клиент заявил о незаконном списании в течение суток после инцидента, кредитная организация обязана незамедлительно возместить эти деньги. Конечно, такой возврат происходит не всегда. Банк может доказать, что причиной возникновения несанкционированных операций стало нарушение клиентом порядка использования электронного средства платежа. Например, сообщение вами третьим лицам реквизитов вашей банковской карты, ПИН-кода, логина, пароля, а также небрежное хранение карты и информации о ПИН-коде, в результате чего к ним получили доступ третьи лица. Однако до закона № 167-ФЗ не существовало правового механизма приостановления перевода денежных средств юридических лиц. Это не позволяло избежать убытков даже в случаях своевременного направления сообщения об отсутствии согласия клиента на осуществление перевода денежных средств. Закон № 167-ФЗ вводит на случай подобных инцидентов особый порядок действий оператора по возврату денежных средств законному владельцу — юридическому лицу.

Это несудебная процедура подтверждения оператором-получателем обоснованности получения переведенных денежных средств. Возврат денежных средств возможен только до зачисления денежных средств на банковский счет. Полу-

чив от оператора-плательщика уведомление о несанкционированном снятии денежных средств, оператор-получатель приостанавливает зачисление денежных средств. Затем незамедлительно запрашивает у получателя документы, подтверждающие обоснованность получения переводимых ему денежных средств.

Такие документы получатель должен предоставить в течение пяти рабочих дней. В случае, если подтверждающие документы в указанный срок не предоставлены, оператор-получатель обязан вернуть сумму подозрительной операции.

ЕДИНАЯ БАЗА ИНЦИДЕНТОВ

Законом № 167-ФЗ Банк России наделен полномочием формировать и вести базу данных о случаях и попытка совершения перевода денежных средств без согласия клиента. Такая база данных будет вестись с учетом правовых механизмов защиты банковской тайны.

Банк России уполномочивается определять для операторов переводов денежных средств, платёжных систем и платёжной инфраструктуры информации порядок предоставления и получения данных из такой единой базы. Оперативно обновляемая единая база данных об инцидентах, их фигурантах и прочих существенных обстоятельствах поможет консолидировать общие усилия, вывести противодействие злоумышленникам на качественно новый уровень.

Закон № 167-ФЗ предусматривает отсрочку вступления в силу в 90 дней после дня официального опубликования, чтобы дать время Банку России принять подзаконные нормативные акты — о признаках совершения перевода денежных средств без согласия клиента и др., а также адаптировать антифродовые системы финансовой сферы к установленным требованиям.

* * *

Следует упомянуть, что закон для противодействия совершению несанкционированных переводов денежных средств закрепляет полномочия Банка России устанавливать для подведомственных организаций обязательные требования к обеспечению защиты информации при осуществлении банковской деятельности и деятельности в сфере финансовых рынков. Эти требования предварительно согласуются федеральными органами исполнительной власти, уполномоченными в областях обеспечения безопасности (ФСБ России), противодействия техническим разведкам и технической защиты информации (ФСТЭК России).

Комитет Государственной Думы РФ по финансовому рынку активно участвовал в разработке и принятии закона № 167-ФЗ. Реализация его положений позволит минимизировать количество несанкционированных операций, совершённых с использованием системы дистанционного банковского обслуживания, а также потери кредитных организаций с банковских счетов юридических и физических лиц.

**Андрей ВЫБОРНОВ**начальник отдела методологии обеспечения
безопасности информационных ресурсов
ГУБиЗИ Банка России

ОЦЕНИ КИБЕРРИСКИ ПРИ АУТСОРСИНГЕ, ПРИМИ ОПТИМАЛЬНОЕ РЕШЕНИЕ

СТАНДАРТ СТО БР ИББС-1.4-2018 «УПРАВЛЕНИЕ
РИСКОМ НАРУШЕНИЯ ИБ ПРИ АУТСОРСИНГЕ»
ЗНАЧИМ, АКТУАЛЕН И ВОСТРЕБОВАН
ОРГАНИЗАЦИЯМИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

Ситуация в финансовой сфере в настоящее время характеризуется высоким уровнем киберрисков. В этой связи востребована высокая компетенция специалистов, актуальным является привлечение новых высокооплачиваемых сотрудников. Банки встают перед лицом значительных финансовых затрат на обеспечение киберустойчивости своих бизнес-процессов. Приемлемым решением проблемы оказывается аутсорсинг, при условии должного уровня его безопасности.

АКТУАЛЬНОСТЬ АУТСОРСИНГА

На рынке труда кадровый ресурс специалистов бывает ограничен, является дефицитом. Неудивительно, что многие кредитные организации в этом плане испытывают затруднения. Поэтому для малых и средних банков и финансовых организаций актуален аутсорсинг некоторых организационных аспектов обеспечения информационной безопасности. В этом случае они могут привлекать организации, сторонних исполнителей, обладающих необходимым уровнем компетенций.

Но и для крупных банков актуальна безопасность аутсорсинга, хотя, возможно и в других аспектах, в том числе в области облачных технологий, работы с внешними центрами обработки данных. Использование этой услуги позволяет крупным банкам оптимизировать свои бизнес-процессы, связанные с информатизацией.

При использовании аутсорсинга управление рисками в любом случае всё равно должно оставаться на стороне кредитной организации, в зоне её ответственности. Выбирая

поставщиков услуг, формулируя для них техническое задание, кредитные организации должны руководствоваться определёнными принципами и требованиями. Чтобы сохранить управление имеющимися рисками и контроль их минимизации.

Центральные банки развитых зарубежных стран (США, Евросоюз, Сингапур и др.) активно занимаются регулированием аутсорсинга информационной безопасности в финансовой сфере. Ими издаются соответствующие нормативные документы, этот опыт был тщательно изучен специалистами Банка России и использован применительно к нашей практике. В Сингапуре, где многие компании специализируются на предоставлении облачных сервисов, это рекомендации Центрального банка. В США также действуют рекомендации в этой области.

Аутсорсинг информационной безопасности, её обеспечение во внешних сервисах — тема, актуальная и интересная для банков. Среди вынесенных банком на аутсорсинг процессов могут быть обслуживание и защита информации в облачных сервисах — центрах обработки данных, услуги СОСов, промышленных систем антифрода, sms-рассылки и т.п. Повторим: для малых и средних банков это возможность использовать сторонние компетенции, для крупных — оптимизировать затраты на основные бизнес-процессы.

ПЕРЕПЛЕТЕНИЯ РИСКОВ

Банки, с которыми осуществлялось взаимодействие в ходе разработки стандарта, интересовались в основном compliance — соответствием требованиям к защите информации.

На этом вопросе они сейчас в большей степени сконцентрированы, чем на минимизации рисков. Банк России создавал комплексную методическую базу, чтобы оба эти аспекта аутсорсинга рассматривались в совокупности.

Необходимость регулирования рисков нарушения ИБ при аутсорсинге в финансовой сфере возникла в связи с перспективами включения рисков киберустойчивости, информационной безопасности в основные, операционные банковские риски, чтобы после этого заниматься ими по единой методологии, на основе оценки этих рисков оценивать общее финансово-экономическое состояние банка, устойчивость кредитно-финансовой организации и других участников финансовой сферы.

Передавая обработку информации на аутсорсинг, банки становятся зависимыми от поставщика услуг. Но риски при этом сохраняются на стороне банка, в зоне его ответственности. Поэтому важно, как банки выстраивают свои отношения с поставщиком услуг аутсорсинга, какой заключают с ним договор, какие в нём прописываются обязательства.

В информационной безопасности риски сводятся, как правило, к двум основным. Первый — нарушения бесперебойности предоставления поставщиком тех или иных услуг, что может приостановить предоставление услуг уже самой финансовой организацией. Второй риск — утечки информации, чреватые как ущербом репутации кредитно-финансовой организации, так и, отдельная тема, — несанкционированными транзакциями, хищениями денежных средств. Эти риски при аутсорсинге остаются на стороне банков, а не поставщиков услуг, именно банки должны продолжать контролировать минимизацию этих рисков, потому что придётся нести ущерб при их реализации.

ОПТИМАЛЬНО ВЫСТРОИТЬ ОТНОШЕНИЯ

Главными адресатами СТО БР ИББС-1.4–2018 являются кредитно-финансовые организации. Деятельность поставщиков услуг банкам Банк России не может контролировать по закону. Однако опосредованно, косвенно новый стандарт касается поставщиков-аутсорсеров, поскольку рекомендует банкам выстраивать отношения с ними по определённым правилам. Включая возможность внешнего аудита, чтоб банк заранее мог определить уровень защищённости, который поставщик в состоянии предоставить. И чтобы этот уровень подтверждался независимой внешней оценкой.



Это комплексная проблема: отдавая свои бизнес-процессы внешнему исполнителю, банк чаще всего не имеет компетенции оценить, насколько поставщик способен обеспечивать киберустойчивость и защиту информации. Банк не владеет механизмами оценок деятельности поставщиков услуг, соответствия её результатов требованиям и рекомендациям Банка России.

Банк России позаботился о том, чтобы создать атмосферу доверия к поставщикам через механизм внешнего аудита. Чтобы финансовая организация, используя его итоги, могла объективно оценивать свои риски при аутсорсинге. Таким образом, СТО БР ИББС-1.4–2018 должен помочь банкам оптимально выстроить отношения с аутсорсерами.

Новый стандарт востребован банками, сигналы об этом поступали в течение нескольких лет. Нормативная база в сфере защиты информации, в том числе при аутсорсинге, активно развивается не только Банком России, но и другими уполномоченными государственными органами, регули-

рующими отрасль — ФСБ России, ФСТЭК России, Роскомнадзором и другими.

Банк России старался обеспечить принятие СТО БР ИББС-1.4-2018 к моменту, когда потребность банков в аутсорсинге и обеспечении его безопасности стала массовой по экономическим причинам. В случаях, когда банкам просто невыгодно создавать и обслуживать новые специализированные вычислительные структуры, брать в штат высокопрофессиональных, но узких специалистов. Объём услуг аутсорсинга на рынке стал значительным, его доля в банковском деле заметно возросла.

ОТ «ВХОДА» ДО «ВЫХОДА»

Логическая структура СТО БР ИББС-1.4-2018 строится следующим образом. Вначале речь идёт о вовлечённости руководства — Совета директоров, исполнительных органов — в процессы построения системы управления аутсорсингом, об определении политики кредитной организации в этом вопросе. Далее — об оценке рисков при выборе поставщика таких услуг: результат выбора должен соответствовать рискам, принятым руководством банка. Следующий шаг — заключение банком соглашения, договора с поставщиком услуг — аутсорсером, включающие требования обеспечения информационной безопасности.

Потом описывается, как банку, осознавая имеющиеся риски, нужно организовать мониторинг деятельности, по-

рученной внешнему поставщику услуг. Завершает текст стандарта «стратегия выхода», процедуры завершения взаимодействия банка с поставщиком. В том числе и для перехода к услугам другого поставщика. СТО БР ИББС-1.4-2018 описывает аутсорсинг «на всех этапах жизненного цикла», от выработки соответствующей политики руководством банка, выбора компании-аутсорсера и заключения с ним договора вплоть до завершения работы с данным поставщиком.

Суть стандарта в том, чтобы помочь банкам, посредством рекомендуемых процедур, сформировать компетенции в области выбора поставщика услуг — аутсорсера, заключении с ним договора и контроля выполнения переданных ему бизнес-процессов. Для этого нужны организационные мероприятия: выработка политики, подготовка юридической документации. А также получение данных о деятельности поставщиков, анализ показателей, как для выбора поставщика, так и для контроля его деятельности.

Отдавая бизнес-процесс на аутсорсинг, банку не нужно специально нанимать сотрудника, который бы вёл мониторинг исполнения. Контроль качества может осуществлять уже имеющийся в штате сотрудник, делать это он должен на основе определённых показателей и критериев. Это всё чисто организационные действия, помогающие банку контролировать свои риски при использовании аутсорсинга, обеспечивать информационную безопасность.



Василий ОКУЛЕССКИЙ

кандидат технических наук, Центр исследования безопасности ИТ

Прочитал статью, потом стандарт, потом еще раз статью. И сам стандарт, и статья о нем оставляют ощущение очень неоднозначное. Пока читаешь — все вроде правильно, все слова складываются в толковые рассуждения. Но в тот момент, когда начинаешь мысленно выстраивать всю эту конструкцию применительно к Банку, понимаешь, что нам предлагают оценить степень разрушения айсберга только по его видимой части. Чтобы эта конструкция заработала, необходима совсем не локальная революция в мышлении, способах взаимоотношений участников и прочее, прочее, прочее...

Простая аналогия. Сама по себе проблема подтверждения соответствия некоторым требованиям решается давно и успешно в рамках, например, системы менеджмента качества (попробуйте в стандартах серии ГОСТ Р ИСО 9000

BIS-КОММЕНТАРИЙ

заменить слова «менеджмент качества» на «менеджмент информационной безопасности» — очень интересный эффект!). Там все на своих местах. Вот сюда система оценки рисков аутсорсинга легла бы практически идеально.

НО.

Чтобы все заработало, необходимо всего ничего:

1. Создание системы аккредитации (?) компаний-аудиторов ИБ, мнение которых будет приниматься как объективная оценка третьей стороной, Реестр доверенных (?) компаний — ?

2. Создание системы подготовки и аттестации аудиторов-специалистов, которые будут проводить эти самые аудиты, ведение реестра аудиторов, контроль своевременной их переподготовки и переаттестации — ?

3. Создание системы внешней оценки соответствия требованиям для этих самых аутсорсеров и ведение реестра «доверенных» поставщиков услуг.

Идея стандарта, безусловно, правильная и очень своевременная. Но этого совершенно недостаточно. Я просто набросал несколько мыслей-вопросов, без ответа на которые все замечательные начинания останутся благими намерениями сделать лучше, а вот что получится?

Как всегда?

ОТ РЕКОМЕНДАЦИЙ К ТРЕБОВАНИЯМ

Стандарт СТО БР ИББС-1.4-2018 «Управление риском нарушения ИБ при аутсорсинге», как и аналогичные документы за рубежом, носит рекомендательный характер. Этот Стандарт, как и другие отраслевые документы этого комплекса, разрабатывался не как некий свод правил, а как «настолярная книга», методическое «руководство к действию» для специалистов по ИБ финансовых организаций.

Действует такая концепция: вначале создаётся отраслевой стандарт — методические рекомендации. Банкам даётся время на их изучение, апробацию, внедрение, выполнение в добровольном порядке. Если сейчас банк при аутсорсинге не будет выполнять предложенные правила, ему грозят «только» повышенные риски прерывания бизнес-процессов, обслуживания клиентов, утечек конфиденциальной информации и хищений денежных средств.

Следующий шаг — придание отраслевому стандарту статуса государственного (национального), ГОСТ Р, переход к обязательному применению. В обозримом будущем положениям стандарта в конкретизированных, более чётких

формулировках может быть придан статус обязательных требований, закреплённый нормативными документами Банка России.

Блок, посвящённый аутсорсингу информационной безопасности, использованию сторонних сервисов, может пройти этот путь ориентировочно за два года. В настоящее время принятие и выполнение СТО БР ИББС-1.4-2018 — дело руководства банка. После того, как прописанные в нём нормы превратятся в обязательные требования, они будут закреплены нормативными актами.

* * *

Вопросы киберустойчивости, информационной безопасности в перспективе предстоит рассматривать в рамках операционных рисков организаций финансовой сферы. Причём — среди основных рисков, существенно влияющих на систему управления капиталом. Низкий уровень информационной безопасности будет означать рост рисков и потребует «страхового» увеличения капитала.



Сергей ВИХОРЕВ,
заместитель руководителя направления
информационной безопасности
ООО «НТЦ «Вулкан»

Да, статья интересная, я бы даже сказал, программная. Многие эксперты скажут: «Все хорошо, но проблема еще не решена, надо еще прикладывать усилия, чтобы создать механизмы реализации этого документа». Позволю вступить с ними в полемику. Да, начало положено, да, аутсорсинг принимает правовые очертания. Это хорошо. Но дальше еще требуется много чего, чтобы эта благородная идея стала реальностью. Но это дальше, впоследствии.

Мне кажется, что один из главных тезисов этой статьи говорит о необходимости доверия между заказчиком и провайдером аутсорсинга. Эти факторы доверия должны иметь не меньшее значение при выборе провайдера, чем целевой уровень защищённости информационных ресурсов или экономические преимущества от сотрудничества.

И очень отраднo, что Банк России, по заявлению автора, позаботился о том, чтобы создать атмосферу доверия к поставщикам через механизм внешнего аудита. Но, к сожалению, на сегодня действенных механизмов достижения такого доверия — нет. Их предстоит выработать. И, думаю, экспертному сообществу надо сосредоточиться именно на

выработке этого механизма, а не на критике самого документа. Каждый мыслит по-своему, каждый решает за себя, но это не значит, что стандарт по аутсорсингу — плохой или неправильный. Но также нельзя забывать про принципиальное решение о передаче функций по информационной безопасности на аутсорсинг — по воле заказчика. Можно передать функции, можно передать некоторые риски, можно передать даже часть ответственности — но не само решение.

И еще, хочу обратить внимание на две ипостаси, которые раскрывает стандарт. С одной стороны, это обеспечение информационной безопасности при передаче бизнес-процессов на аутсорсинг. И с другой стороны — передача непосредственно функций информационной безопасности на аутсорсинг. Это две разные функции. При передаче функций информационной безопасности риски аутсорсинга связаны с нарушением свойств информации, а уж потом, как следствие, нарушение бизнес-процессов. При передаче на аутсорсинг бизнес-процессов — эти риски напрямую в нарушении бизнес-процессов. И об этом всегда надо помнить.

Ну, и напоследок, ложку дегтя. Непонятно почему автор говорит о том, что вопросы киберустойчивости, информационной безопасности в перспективе предстоит рассматривать в рамках операционных рисков организаций финансовой сферы. На мой взгляд, эти вопросы надо рассматривать уже сейчас, а не откладывать на будущее. Разрывать бизнес-процессы, а следовательно и операционные риски от информационной безопасности нельзя.

BIS-КОММЕНТАРИЙ



Сергей ВАЛУЙСКИХ
управляющий
директор — начальник
центра киберзащиты
Сбербанка

ВТОРОЙ СОС СБЕРБАНКА

ТЮНИНГ ИЛИ НОВАЯ МОДЕЛЬ?

Модернизацию Security Operation Centre Сбербанка в самом Сбербанке называют одним из крупнейших в Европе и самым масштабным в России проектом трансформации SOC. Речь идёт не только о технологических новшествах, но и о вещах фундаментальных: внедряется абсолютно новая процессная модель, вводится новая оргштатная структура и, самое главное, меняется профессиональное сознание людей, так или иначе участвующих в проекте.

На вопросы ведущего рубрики «SOC России» Александра Бодрика о причинах и предпосылках этой инициативы, структуре и взаимодействии SOC 2.0 со смежными подразделениями отвечает управляющий директор — начальник центра киберзащиты Сбербанка Сергей Валуйских.

ИСТОРИЯ, СТРУКТУРА И ЗАДАЧИ

— До последнего времени не вызывал сомнения тот факт, что SOC Сбербанка справляется со своими задачами и имеет запас прочности на несколько лет вперёд. Расскажите, пожалуйста, историю формирования SOC Сбербанка вообще и историю возникновения SOC 2.0 в частности?

— SOC в том или ином виде существует в банке давно, и пока Сбербанк был классическим банком, работающая в нём система кибербезопасности полностью соответствовала выдвигаемым требованиям.

Трансформация Сбербанка в серьёзную и мощную технологическую компанию связанная с растущей диджитализацией, выходом на рынок цифровых услуг и созданием цифровых платформ, повлекла за собой необходимость перехода функции безопасности в новое качество. SOC, который до этого устраивал компанию, перестал отвечать на новые вызовы.

SOC 2.0 часто называют Intelligence-Driven SOC, однако чёткого определения не существует. Для кого-то это просто внедрение новых технологий, таких, как UBA (User Behavior Analytics). Для нас же это понятие выходит

за рамки внешнего «тюнинга» и означает глубокую трансформацию на всех уровнях: в процессах, технологиях и, самое важное, в сознании людей.

— Минимизация ущерба от масштабных инцидентов требует координации усилий многих подразделений. Какая структура у вашей службы кибербезопасности?

— В состав службы кибербезопасности входят крупные операционные подразделения, в первую очередь, центр киберзащиты и управление противодействия кибермошенничеству. Они полностью отвечают за инцидент-менеджмент и выполняют все оперативные функции реагирования на инциденты. В зону ответственности управления методологии кибербезопасности входит нормативная база — стандарты, регламенты, политики. Центр внутрикорпоративного взаимодействия — связующее звено между кибербезопасностью и бизнес-подразделениями банка. Управление экспертизы кибербезопасности участвует в разработке программных продуктов. Дирекция программ и проектов отвечает за реализацию проектов по кибербезопасности. Лаборатория кибербезопасности проводит перспективные исследования в области кибербезопасности.

— Как структурирован сам SOC? В чём отличие структур и функционального назначения SOC и SOC 2.0?

— SOC Сбербанка географически распределён. Основные подразделения расположены в Москве, но существуют ещё четыре региональных сервисных центра. Все они имеют чёткую структуру:

◆ Круглосуточная дежурная смена отвечает за мониторинг событий кибербезопасности и реагирование на инциденты в режиме 24/7.

◆ Отдел реагирования на инциденты кибербезопасности, в котором трудятся высококвалифицированные эксперты, подключается, когда компетенций дежурной службы оказывается недостаточно.

◆ Отдел киберугроз (Cyber Threat Intelligence) занимается аналитикой в сфере киберугроз и



ранним предупреждением о рисках возникновения угроз и инцидентов.

◆ Отдел средств защиты администрирует все системы, стоящие «в разрыв», то есть непосредственно влияющие на предоставление сервисов банка, к примеру, межсетевые экраны.

◆ Отдел мониторинга сопровождает все остальные средства и системы защиты, например, все системы поддержки процессов СОС, такие как SIEM, Ticketing, Reporting и многие другие.

Основное отличие СОС и СОС 2.0 с точки зрения оргштатной структуры — в наличии подразделения Cyber Threat Intelligence. Оно должно заменить реактивную модель СОС на проактивную: пресечь возможный инцидент до его возникновения.

— **Занимается ли служба кибербезопасности мониторингом доступности и эффективности бизнес-процессов силами СОС?**

— Эффективность — нет, но бизнес-метрики мониторинг. Обеспечение доступности сервисов — одна из задач службы кибербезопасности. И если, скажем, среднестатистический показатель числа пользователей, использующих

Сбербанк Онлайн, вдруг резко уменьшается, это может быть признаком снижения доступности. Другой пример — при защите от DDoS-атак мы постоянно отслеживаем метрики доступности атакуемых систем.

— **Развитые СОС часто идут по пути технического улучшения, например, форензики, реверс-инжиниринга и киберразведки. Какие из этих практик применяются в Сбербанке?**

— Все. Киберразведкой занимается, в частности, подразделение Cyber Threat Intelligence. Реверс-инжинирингом — отдел реагирования. Кстати, реверс-инжиниринг активно применялся при разборе напугавших вирусных эпидемий WannaCry, NotPetya, Bad Rabbit, и используется ежедневно при реагировании на фишинговые атаки. Форензика входит в задачи отдела расследований центра киберзащиты, который привлекается для сбора цифровых доказательств в случае крупных, резонансных инцидентов. Кроме этого, в составе центра киберзащиты работает команда Red Team. Она производит постоянную оценку защищенности систем банка, тестируя их на проникновение. Это важное направление, которое является, в том числе элементом СОС 2.0.

— Входит ли в SOC служба фрод-мониторинга?

— Сейчас нет, но с внедрением модели Fusion Centre дежурная служба фрод-мониторинга войдет в его состав. Сейчас же дежурная служба SOC и фрод-мониторинга активно сотрудничают.

— Многие крупные корпорации при создании SOC выносят операционное ядро в регионы, надеясь снизить затраты и получить доступ к менее конкурентным, чем московский, рынкам труда. Как распределяются по регионам подразделения вашего SOC?

— Как я уже отметил, SOC географически распределён. Частично это действительно связано с некоторой экономией, но это не единственная причина такого решения. В Москве часто приходится иметь дело с чем-то глобальным, а в регионах дефицит информации стимулирует желание разобраться в предмете детальнее.

На базе региональных SOC мы создаем центры компетенций, каждый из которых отвечает за определенную зону защиты (к примеру, периметр сети) и является уникальным подразделением в структуре SOC.

ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ SOC

— Сбербанк известен высокой степенью автоматизации SOC. Какие ключевые системы вы бы выделили? Чем в этом смысле отличается SOC 2.0?

— Применительно к SOC я бы выделил, в первую очередь, системы поддержки процессов SOC. Прежде всего, Ticketing System и Reporting System. Они полностью внедрены в SOC. Также сейчас мы активно внедряем Threat Intelligence Platform и Incident Response Platform — системы, которых не было в SOC и которые являются неотъемлемой частью SOC 2.0.

— Главной проблемой баз данных управления конфигурации (Configuration Management Database) обычно является их быстро устаревающее наполнение. Как эта проблема решается у вас?

— Проблема присуща всем системам CMDB, особенно в компаниях с развитой инфраструк-

турой. Мы используем ту же CMDB, что и в IT. Уровень её актуальности достаточно высок и для её поддержания в IT выделено целое подразделение. Чтобы наполнение не устаревало, необходимо соблюдать своего рода «гигиенический» IT-минимум: каждый сотрудник как владелец определенного ресурса должен следовать инструкции и поддерживать свои записи в базе в актуальном состоянии. Это должно войти в привычку: внёс изменения — сделал запись. Иначе никакой отдел не поможет.

— Для служб кибербезопасности характерна проблема приоритетности задач по доработке Service Desk для IT над задачами кибербезопасности. Вы используете общий с IT Service Desk или отдельный?

— Для работы с инцидентами кибербезопасности мы используем свою тикетинг-систему, о которой я уже говорил. Почему свою? В рамках проекта модернизации SOC в условиях сжатых сроков и необходимости автоматизации многих процессов было необходимо динамично её дорабатывать. Это очень сложно, когда вы не являетесь владельцем системы. Кроме того, в силу специфики, доступ к нашей информации должен быть ограничен для остальных сотрудников. В одном решении сложно соблюсти все условия, поэтому пока используем своё. Возможно, в будущем, если мы найдем продукт, который удовлетворяет требованиям обоих подразделений, ИБ и IT, в том числе по разграничению прав доступа, мы сможем использовать общее решение.

— Ведёте ли вы разработку ПО для потребностей SOC?

— Да. Как я уже говорил, Сбербанк — высокотехнологичная компания, и это касается и кибербезопасности. У нас есть команды разработчиков, которые занимаются только нашим специализированным ПО.

— Используются ли решения на базе Open Source?

— Да, как основу для ряда решений мы используем компоненты открытого программного обеспечения. В дальнейшем мы конечно их кастомизируем, но как база они активно используются.

— Как вы решаете проблему контроля регионов, учитывая слабые каналы связи там?

— Все подразделения банка работают онлайн с централизованными IT-системами, поэтому проблемы каналов связи у нас нет.

ПРОЦЕССЫ РАБОТЫ SOC

— Как распределяются полномочия в SOC в рамках мониторинга угроз?

— Основная нагрузка выпадает на дежурную смену, которая состоит из трёх линий. На пер-

**НА БАЗЕ РЕГИОНАЛЬНЫХ SOC МЫ
СОЗДАЕМ ЦЕНТРЫ КОМПЕТЕНЦИЙ,
КАЖДЫЙ ИЗ КОТОРЫХ ОТВЕЧАЕТ
ЗА ОПРЕДЕЛЕННУЮ ЗОНУ ЗАЩИТЫ
И ЯВЛЯЕТСЯ УНИКАЛЬНЫМ
ПОДРАЗДЕЛЕНИЕМ В СТРУКТУРЕ SOC**

вой линии проводится, собственно, мониторинг угроз. Анализируется подозрение на инцидент на предмет ложного срабатывания и, в случае реальной угрозы, заводится инцидент и передается на вторую линию. Вторая линия занимается категоризацией и маршрутизацией инцидентов. Нужно правильно определить приоритет и направить его в соответствующую группу реагирования. Зачастую инцидент происходит на стыке групп реагирования, и важно понять, какая из групп должна взять инцидент в работу. Третья линия непосредственно реагирует на инцидент.

— Какой ролевой модели работы вы придерживаетесь? Изменится ли она с появлением SOC 2.0?

— Помимо этих трёх линий есть определенная модель эскалации инцидента, когда подключаются более квалифицированные специалисты, руководство. Есть дополнительные роли, связанные с Threat Intelligence и Use Case Management, работающие с проактивной компонентой реагирования. Именно последнее, на мой взгляд, и является признаком SOC 2.0 с точки зрения ролей.

— Какие основные критерии влияют на решение о критичности инцидента?

— У нас разработана политика реагирования на инциденты. Есть матрицы принятия решений как по приоритетам, так и по эскалациям. Критериев много. Основные из них связаны с ущербом — потенциальным или реальным. Пока влияние потенциальное, мы работаем в нижнем диапазоне приоритетов (низкий, средний, высокий). При реальном влиянии на сервис банка приоритет синхронизируется с приоритетом соответствующего ИТ-инцидента. В случае реального влияния возможен переход в верхний диапазон приоритетов (очень важно, критический, широко-масштабный).

— Насколько у вас высок уровень формализации процессов?

— Все процессы в SOC подробно расписаны и формализованы. Все действия сотрудников тоже стандартизованы: заводится инцидент, фиксируется время и действия. Это важно, в том числе для оценки операционных показателей работы SOC и сбора статистики для принятия управленческих решений, корректировки деятельности, повышения эффективности.

— Сейчас очень популярна тема обмена информацией (Data Sharing). Происходит ли у вас такой обмен?

— Обязательно. После прошлогодних мощных атак все поняли: только объединив усилия, можно эффективно противостоять угрозам, и

У НАС ЕСТЬ РЯД УНИКАЛЬНЫХ ПРОЕКТОВ, В ТОМ ЧИСЛЕ В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ОБРАБОТКИ БОЛЬШИХ ДАННЫХ, НО НА СЕГОДНЯШНИЙ ДЕНЬ ОСНОВНОЕ НОУ-ХАУ — ЭТО ЛЮДИ

информационный голод — самое страшное в таких обстоятельствах. Реагируя на тот или иной инцидент, в отчёте по угрозе мы формируем открытую и закрытую части. Открытая часть может использоваться для распространения. Мы подписали соглашения по взаимодействию со многими организациями, чтобы обмениваться информацией.

О КАДРАХ И НОУ-ХАУ

— Как в SOC решается кадровый вопрос? Чем мотивируете, удерживаете людей, как развиваете потенциал сотрудников?

— Проблема дефицита технических специалистов стоит довольно остро, особенно для крупных подразделений кибербезопасности. Но если человек к нам попадает, Сбербанку есть чем его удержать — интересные проекты и задачи сами по себе неплохо мотивируют. Кроме того, у нас предусмотрена программа обучения и сертификации специалистов, причём обязательная. Сбербанк заключил соглашения с несколькими крупными вузами — это один из источников поиска сотрудников среди молодых специалистов.

— Как происходит набор людей для SOC 2.0?

— В SOC 2.0 используются уникальные технологии, пока не очень распространенные в России, поэтому в основном мы используем собственные кадровые ресурсы. Кроме того, мы сотрудничаем с крупными производителями решений, в том числе в части обучения сотрудников.

— Какие ноу-хау, присущие только Сбербанку, используются в работе SOC и SOC 2.0?

— У нас есть ряд уникальных проектов, в том числе в области искусственного интеллекта и обработки больших данных, но на сегодняшний день основное ноу-хау — это люди. В прошлом году команда кибербезопасности создала очень серьезную, проработанную до мелочей процессную модель. В ходе работы над ней изменилась профессиональная культура команды. Мы считаем это важным достижением, которое повлияет на наше развитие в будущем.

SOLAR SECURITY В НОВОЙ РОЛИ... СТАЛКЕРА

СТАНЕТ ЛИ РОСТЕЛЕКОМ НАЦИОНАЛЬНЫМ ЛИДЕРОМ В СФЕРЕ ИБ?



Анна ВОРОБЬЕВА
корреспондент
BIS Journal

В конце мая компания Ростелеком объявила о приобретении 100% акций одного из крупнейших в России поставщиков услуг центра мониторинга информационной безопасности — Solar Security. Стоимость покупки составила 1,5 млрд рублей.

С приобретением мощного ИБ-разработчика в компании создадут Центр компетенции коммерческих услуг кибербезопасности. Новое подразделение под управлением Игоря Ляпунова станет развивать стратегию кибербезопасности Ростелекома, предлагая на базе ЦОДов компании различные сервисы ИБ. В дополнение к обслуживаемым сегодня крупным корпоративным клиентам и государственным ведомствам, будет существенно расширяться клиентская база ИБ-сервисов, прежде всего, за счёт средних и малых отечественных предприятий.

Одним из продуктов станет страхование киберрисков, другое перспективное направление — обеспечение безопасности объектов критической информационной инфраструктуры (КИИ), законодательные требования к которым затрагивают большое количество государственных и частных организаций.

Основным препятствием для расширения деятельности на рынке ИБ может стать недостаток квалифицированных кадров — прежде всего, хорошо знакомых с отраслевой спецификой менеджеров. Утолять кадровый голод компания планирует за счёт расширения сотрудничества со школами, высшими учебными заведениями, участия в проведении профильных соревнований и олимпиад, подготовительных курсов.

Развитие российской экономики тесно связано с активным внедрением цифровизации, открывающей безусловные возможности. Все

больше таких возможностей открывает для себя телеком-оператор Ростелеком. Купив одного из российских лидеров в сфере киберзащиты — компанию Solar Security — и усилив тем самым свои позиции на рынке ИБ, Ростелеком решил взять на себя роль «национального лидера в информационной безопасности».

В процессе слияния основной акцент ставится на внедрение и развитие отечественных технологий. Глава Solar Security, он же директор Центра компетенций и вице-президент Ростелекома Игорь Ляпунов отметил, что это часть долгосрочной уверенной стратегии развития. «Государство, бизнес и население в условиях динамики внешней среды и роста киберугроз нуждаются в очень серьезном партнере. Ростелеком вкладывает в это направление значительные интеллектуальные и финансовые ресурсы. Мы ставим своей задачей стать таким партнером в обеспечении информационной и национальной безопасности», — добавил Ляпунов.

В планах обновленного телеком-оператора занять 70–80% российского рынка кибербезопасности. При этом упор будет делаться на реализацию программы импортозамещения, несмотря на то, что «процесс внедрения тяжелый, требует много времени и средств». «Защищать себя мы должны нашими средствами», — подчеркнул директор Solar Security.

Важным этапом станет наращивание кадрового потенциала, в том числе и целенаправленная работа с молодыми талантами. И хотя в настоящее время штат ИБ-подразделения Ростелекома укомплектован на 100%, в ближайшие два года для Москвы и регионов этого станет недостаточно. Компания уже анонсировала план найма более 100 специалистов по ИБ.

В то же время Центр компетенции планирует выращивать специалистов и создавать профессиональную среду кадрового резерва ИБ самостоятельно. «Правильная подготовка и выращивание специалистов, накачивание их практическим опытом даст серьезный прирост ИБ-рынку и национальной безопасности. Работа с талантами в вузах и школах — сейчас это единственный возможный способ наращивать мышечную массу, поскольку заниматься

ОДНИМ ИЗ ПРОДУКТОВ СТАНЕТ СТРАХОВАНИЕ КИБЕРРИСКОВ, ДРУГОЕ ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ — ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ

на очень узком рынке перетягиванием специалистов из одной компании в другую — всегда сложная и экстенсивная работа... Мы занимаем созидательную позицию, создавая профессиональное комьюнити», — рассказал Игорь Ляпунов.

По его словам, сегодня большинство специалистов, работающих в SOC Solar Security, — это люди, которые вышли из вузов, прошли у них стажировку и все уровни технической подготовки.

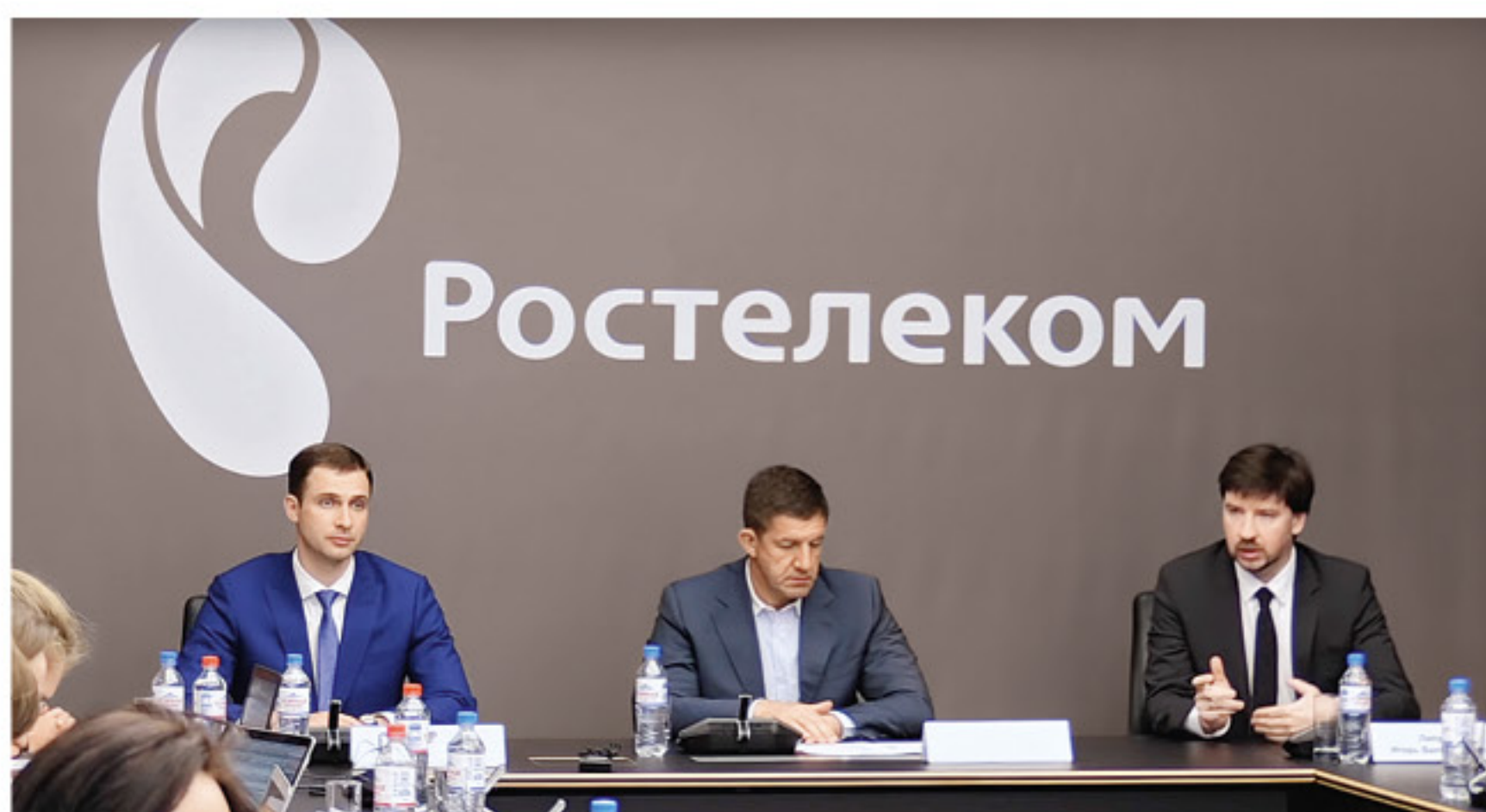
Наращивание кадрового потенциала позволит Ростелекому активнее работать и со старшами и с состоявшимися отечественными компаниями. «Мы будем инвестировать в те компании и решения, в которых будем видеть серьезную перспективу. Поэтому эта сделка (с Solar Security — ред.) также даст возможность быстро наращивать собственные знания и независимость от внешних решений», — обратил внимание президент Ростелекома Михаил Осеевский.

Уже этим летом национальный оператор совместно с образовательным центром «Сириус» проведет для школьников Всероссийскую олимпиаду по кибербезопасности. Ее победители осенью поедут на специализированную учебную смену в Сочи и пройдут соответствующую подготовку с участием ведущих ИБ-экспертов. Данную практику планируется сделать ежегодной, поскольку именно такие ребята становятся «костяком той команды, на которую мы будем делать ставку в дальнейшем движении вперед. Кибербезопасность — это вопрос только кадров, здесь ни нефть, ни газ не помогут», — добавил Осеевский.

В перспективе у Ростелекома есть планы открыть на базе ОЦ «Сириус» специализированную лабораторию для более системной работы с молодым поколением.

Также к сотрудничеству с оператором присоединился образовательный фонд «Талант и успех». Во время проведения Петербургского международного экономического форума (ПМЭФ-2018) Михаил Осеевский и руководитель фонда Елена Шмелева подписали стратегическое соглашение для привлечения в сферу информационных технологий школьников и студентов — получателей грантов Президента РФ и наиболее результативных выпускников образовательного центра «Сириус» с целью их профессионального развития и будущего трудоустройства в отрасли.

Для поддержки и развития одаренных детей стороны будут работать над созданием и запуском образовательных программ, учебно-методических и научно-популярных материалов



Первый вице-президент ПАО «Ростелеком» Владимир Кириенко, президент ПАО «Ростелеком» Михаил Осеевский, вице-президент ПАО «Ростелеком» по кибербезопасности Игорь Ляпунов

в области информационных технологий, в том числе для педагогов.

О том, что Ростелеком наращивает свой потенциал в сфере ИБ, стало понятно еще в прошлом году, когда оператор заключил ряд соглашений с ведущими ИБ-компаниями для развития собственной экспертизы. К примеру, в 2017 году было подписано соглашение с компанией Digital Security, специализирующейся на анализе защищенности систем и исследованиях в области информационной безопасности. Компании решили осуществлять совместную работу в области анализа ИБ, обмена данными, технологиями и опытом.

Эксперты полагают, что Ростелеком имеет достаточно высокий потенциал и возможности для укрепления своих позиций на рынке информационной безопасности, так как зачастую естественным образом находится на передовой противостояний.

По мнению некоторых специалистов, на покупке Solar Security амбициозные планы Ростелекома не закончатся. И в это довольно легко поверить, поскольку совсем недавно через поглощение компании SafeData, которая занимала 2-е место в рейтинге крупнейших ЦОД по количеству введенных в эксплуатацию стойко-мест на российском рынке, национальный оператор вышел на рынок центров обработки данных. Тогда за приобретение SafeData «Ростелеком» заплатил 4,05 млрд руб.

Подробности события и интервью с президентом «Ростелеком» Михаилом Осеевским и вице-президентом по кибербезопасности Игорем Ляпуновым — в рубрике «В центре внимания» на BIS TV (tv.ib-bank.ru).

ЗАЩИТА ПРЕМИУМ-КЛАССА

СПЕЦИФИКА ИБ ИНВЕСТИЦИОННОГО БАНКИНГА



Андрей БАЖИН
директор
по информационной
безопасности ВТБ
Капитал

Финансовая сфера многолика и разнообразна, и информационная безопасность ее подотраслей также неоднородна, часто значительно. BIS Journal решил разобраться в специфике направлений банковской ИБ, для чего и открывает рубрику, которая так и называется: «Специфика ИБ». Для начала наш эксперт, обозреватель и ведущий новой рубрики Александр Бодрик встретился с директором по информационной безопасности АО «ВТБ Капитал» Андреем Бажиным. Это и понятно: инвестиционный бизнес — элитарный, а значит, его ИБ уж точно отличается от среднестатистической.

— Андрей, какова структура бизнеса инвестиционного банка с точки зрения службы ИБ?

— Исторически инвестбанковский бизнес (CIB — corporate investment business) обслуживает в первую очередь так называемых институциональных клиентов, а также крупные корпорации и финансовые институты — участники финансовых рынков. Инвестиционные банки помогают привлекать деньги, структурировать сделки при покупке и продаже бизнеса, обеспечивать крупные операции при торговле ценными бумагами и производными финансовыми инструментами.

Клиентский менеджмент и процессы продаж продуктов коммерческого и инвестиционного банка в целом похожи в силу своей природы, основное отличие — в меньшем круге потенциальных клиентов у инвестбанка. Поэтому для инвестбизнеса гораздо более высока критичность репутации, утверждение «Банкир — это прежде всего репутация» является законом. Из-за того,

что круг клиентов ограничен, самих инвестбанков на рынке не так много, и для каждого из них связка «инвестиции — доброе имя — доверие» всегда актуальна.

Реноме зарабатывается стабильно высоким уровнем сервиса и надежностью процессов при оказании услуг. Соответственно, требования к операционным процессам и к информационной безопасности как их неотъемлемой части высокие. Одновременно используются классические организационные и технические контроли — как в традиционном банке, но опять же на более высоком уровне.

— Какие основные цели и задачи ставит перед собой служба информационной безопасности инвестиционного банка?

— Тут два магистральных направления: обеспечение информационной безопасности, включая кибер-безопасность, и соответствие требованиям регуляторов.

В части обеспечения информационной безопасности — это, во-первых, гарантия конфиденциальности для поддержания доверия клиентов. Об операциях никому не должно быть известно. В том числе, кстати, и для того, чтобы противодействовать манипулированию рынком. Во-вторых, обеспечение доступности и целостности как компонента доступности: сервисы должны работать, как часы, в том числе быть устойчивыми к внутренним и внешним воздействиям — как просто ошибкам, так и умышленным действиям.

В части соответствия требованиям регуляторов — это соответствие как локальным нормативным актам стран присутствия, так и требованиям основных торговых площадок, бирж, через которые инвестбанки осуществляют часть своих операций.

— Какие процессы и активы инвестиционно-банковский бизнес обычно просит обеспечить целевым уровнем защиты?

— Клиентские данные, внутренние ноу-хау, которые обеспечивают конкурентное преимущество инвестиционного банка, в том числе и понимание специфики того или иного финансового рынка, специфики законодательства и опреде-

ДЛЯ ИНВЕСТБИЗНЕСА ГОРАЗДО БОЛЕЕ ВЫСОКА КРИТИЧНОСТЬ РЕПУТАЦИИ, УТВЕРЖДЕНИЕ «БАНКИР — ЭТО ПРЕЖДЕ ВСЕГО РЕПУТАЦИЯ» ЯВЛЯЕТСЯ ЗАКОНОМ



ленных аспектов конкретных сделок. Также важна безопасность крупных операционных платформ, которые обеспечивают операционную деятельность инвестбанка, — их доступность, по сути дела, определяет доступность бизнеса.

— Сейчас набирает популярность тренд использования на финансовых рынках различных ботов и стратегий автоматизированных торгов. Каковы риски и контроли для таких технологий?

— Если бизнес-логика бота понятна, если обработка данных ботом соответствует законодательству, если определен владелец бота, реализована ролевая модель управления правами доступа, в том числе и то, кто может его настроить и через какие интерфейсы он управляется, то в целом с точки зрения ИБ с ним все хорошо. По сути, это элемент искусственного интеллекта, который будет развиваться и дальше. При этом основной плюс бота — у него нет эмоций, основной минус — нет и интуиции.

— Каковы общие особенности обеспечения информационной безопасности инвестиционного бизнеса в целом и классических бизнес-единиц (например, global markets, брокерский бизнес, работа с валютой и долговыми обязательствами) в частности?

— На первый взгляд, специфика небольшая: малый time-to-market, сервис-ориентированная культура внутри организации. Служба ИБ

понимает, что она — обеспечивающее подразделение. Также часто нужно уметь находить компромиссные решения: в инвестбанке много участников сделок и бизнес-процессов, и баланс интересов крайне важен.

Существует и довольно много локальных нормативных требований, причем каждая торговая площадка при подключении часто выдвигает свои.

Отдельная тема — это обеспечение информационной безопасности M&A, в частности применение data room для реализации управляемого множественного доступа участников и консультантов по сделке к большому объему информации от разных стран и юрисдикций.

— Какова типовая структура службы ИБ инвестиционного банка и особенности ее взаимодействия со смежными подразделениями?

— Типовой структуры службы ИБ в инвестиционном банкинге, пожалуй, нет, но стоит заметить, что именно инвестбанки одними из первых стали выделять ИБ в отдельное подразделение.

Есть специфика внутреннего взаимодействия. Бизнес — быстрый, оперативный, и тут важны горизонтальные связи, проактивный подход и совместное достижение низкого time-to-market. Бюрократии в инвестбанках минимум — фокус на результат. Учитывая скорость бизнес-процессов в инвестбанках, важно предугадывать

ВСЕ КЛАССИЧЕСКИЕ КОНТРОЛИ АКТУАЛЬНЫ ДЛЯ ИНВЕСТИБИЗНЕСА, НО ЕСТЬ ПОВЫШЕННЫЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ, А ЗНАЧИТ, УСИЛЕНО УПРАВЛЕНИЕ ДОСТУПОМ

потребности бизнеса. Потом времени может и не оказаться.

Большинство моделей ИБ в инвестбанках все-таки строится на ISO 27к. На базе гибкой и стандартизированной системы достаточно легко учесть требования регуляторов и контрагентов.

— **Кто основной заказчик/куратор/внутренний заказчик процессов и внутренних сервисов службы ИБ?**

— Основной заказчик — руководство компании, но бывает и по-другому, так как многое зависит от истории вопроса ИБ в банке и опыта руководителей. Бывают запросы от руководителей бизнес-линий — кто за какие данные отвечает (data governance). Клиентские подразделения озабочены защитой клиентских данных, в том числе персональных. Линия Corporate Finance требует обеспечения безопасности документов в рамках подготовки сделок. Корпоративное ИТ просит помощи по специфическим вопросам технологий ИБ.

Наконец, работает и проактивный подход. Служба ИБ часто сама предлагает новые процессы, решения.

— **Какие подразделения инвестбанка участвуют в реализации процессов ИБ?**

— Ключевой участник процессов ИБ — менеджмент для определения риск-аппетита при принятии решений в сфере ИБ, лояльный и обученный персонал и, безусловно, ИТ.

— **Какие внутренние сервисы ИБ наиболее востребованы?**

— Все классические контроли актуальны для инвестибизнеса, но есть повышенные требования к обеспечению конфиденциальности, а значит, усилено управление доступом, в том числе на основе ролевой модели, а также закладывается дополнительный запас прочности во все контроли ИБ на внутренних сервисах.

— **Какие специалисты востребованы службой ИБ инвестбанка?**

— У специалистов мы, прежде всего, хотим видеть наличие международных сертификатов в сфере информационной безопасности и смежных областях (CISA, CISM, CISSP), знание английского языка. Также для нас крайне важ-

ны soft skills — умение мягко, ненавязчиво, но терпеливо и убедительно отстаивать интересы функции ИБ внутри и вне компании. Фактически это все качества внутреннего консультанта.

Нужно понимать, что люди в этом бизнесе — успешные и динамичные. Они требовательны и к себе, и к другим, в том числе и к специалистам по ИБ. Многие учились за рубежом, понимают лучшие мировые практики и требуют понимания специфики бизнес-процессов. Например, нельзя отвлекать трейдеров во время торгов, и в общем есть повышенные требования к культуре общения.

— **Как изменилось регулирование для инвестбанков за последние три года?**

— Самое важное изменение — Центробанк стал мегарегулятором, и его требования распространяются на финансовые рынки. Объединения участников фондового рынка тоже ведут работу в этом направлении, пусть и не столь заметную. Актуален ряд зарубежных требований, ведь инвестбанк строит бизнес в соответствии с международной финансовой системой.

— **Изменился ландшафт угроз в инвестбанкинге?**

— Ландшафт угроз для инвестбанка сходен с ландшафтом угроз финансовой организации, разве что нет такого фокуса на физических лиц, как у розничного банка. В частности, приходится по-прежнему заниматься так называемой «наложенной ИБ», ведь рынок использует системные платформы и протоколы, такие как Windows и TCP/IP. При их проектировании разработчиком вопросы интероперабельности были поставлены на первое место, а вопросы ИБ решаются, на мой взгляд, посредством управления рисками и в большей степени — наложенными средствами защиты и процессами.

— **Каковы основные направления развития службы ИБ инвестбанков на 3 года вперед?**

— Во-первых, повышение внимания к data management/data governance. Бизнесу все интереснее, кто, что и с какими данными делает.

Второе — это постепенная интеграция процесса управления рисками ИБ в рамках управления рисками организации в целом, с использованием инструментария операционных рисков. В частности, с помощью накопления и использования статистики инцидентов ИБ, самооценки, а также анализа ключевых индикаторов риска (KRI, Key Risk Indicators) в контексте информационной безопасности.

И третье — выполнение требований регуляторов: ЦБ РФ, международных требований (например, GDPR), которое требует постоянного тюнинга контролей в части поддержания соответствия.

В ОДИН КЛИК

АССОЦИАЦИЯ ФИНТЕХ СОВМЕСТНО С БАНКАМИ-УЧАСТНИКАМИ И БАНКОМ РОССИИ ПРЕЗЕНТОВАЛИ КОНЦЕПЦИЮ СИСТЕМЫ БЫСТРЫХ ПЛАТЕЖЕЙ

Ассоциация ФинТех совместно с банками-участниками и Банком России презентовали концепцию Системы Быстрых Платежей (СБП), с помощью которой можно будет осуществлять переводы денежных средств по номеру телефона, e-mail или другим простым идентификаторам.

Система Быстрых Платежей даст возможность пользователям осуществлять переводы в любом месте и в любое время. Платеж можно сделать по простым и понятным реквизитам, которые всегда под рукой: по номеру телефона или по адресу электронной почты. Пользователь может сделать перевод в своём мобильном банке или в другом привычном интерфейсе — будь то мессенджер, социальная сеть или сайт интернет-магазина.

«Система Быстрых Платежей создает принципиально новые возможности в области платежных сервисов как для населения, так и для организаций. Устранение межбанковских барьеров, снижение издержек участников рынка и повышение удобства финансовых услуг для пользователей — ключевые задачи СБП. Важно отметить роль Ассоциации ФинТех в координации этого проекта и в выстраивании конструктивного диалога между участниками рынка и Регулятором», — комментирует Ольга Скоробогатова, Первый заместитель Председателя Банка России.

На пресс-конференции, которая состоялась на площадке Ассоциации ФинТех, было отмечено, что в условиях активного роста электронной коммерции и развития цифрового взаимодействия между участниками рынка, становится очевидной потребность финансового сектора в подобной системе. Создание инфраструктуры быстрых платежей и переводов — одна из ключевых инициатив по развитию розничного платежного пространства на российском рынке.

«Когда мы говорим о real-time платежах, мы подразумеваем прежде всего доступ 24/7/365 для клиентов и возможность осуществлять сделки в один клик. Причем не имеет значения, каким платежным механизмом пользуется человек, подтверждение транзакции происходит мгновенно или в течение нескольких секунд. Мгновенность стала нормой образа жизни потребителя», — пояснил Сергей Солонин, генеральный директор Ассоциации ФинТех.

На Наблюдательном Совете АФТ было принято решение об организационно-правовой модели будущей Системы Быстрых Платежей, где роль операционного, платежного и клирингового центра будет выполнять АО НСПК.

«Перед нами стоит задача построить принципиально новую платформу, которая не связана с тем, что происходит сегодня в карточном бизнесе. Но все прорывные проекты реализуются, только когда есть вызов. У НСПК есть опыт реализации сложнейших проектов в сжатые сроки и компетентные эксперты, лучшие в своей области, которые будут работать над созданием бесшовной инфраструктуры, позволяющей перевести деньги по любому идентификатору. Уверен, что у нас есть прекрасный шанс при поддержке банковского сообщества выйти на передовые рубежи современных платежных технологий», — подчеркнул генеральный директор НСПК Владимир Комлев.

Участники пресс-конференции также рассказали о тех возможностях, которые запуск СБП предоставит игрокам финансового рынка и потребителям.

Оливер Хьюз, председатель правления Тинькофф Банка, прокомментировал: «Мы в Тинькофф Банке рады принимать участие в развитии системы быстрых платежей. На данный момент успешно провели техническое тестирование и планируем быть в числе первых участников при запуске системы. СБП будет способствовать развитию платежной инфраструктуры России, а также значительно упростит жизнь клиентов банков».

Владимир Верхошинский, член правления ВТБ, отметил: «С переходом клиентов в digital каналы наиболее востребованы простые и быстрые решения по проведению ежедневных банковских операций. Статус перевода будет прозрачным: через секунды после отправки получатель сможет воспользоваться полученными денежными средствами, а отправитель узнает, что деньги дошли по назначению. СБП позволит также просто осуществлять онлайн покупки и осуществлять взаиморасчеты между юридическими лицами».

Система Быстрых Платежей станет доступна пользователям уже с 2019 года.



**Кристина
БОРОВИКОВА**
старший консультант
KPMG



Андрей ДРОЗДОВ
старший менеджер KPMG,
CISA, CISM, CGEIT

GDPR.

А ТАК ЛИ СТРАШЕН ЧЕРТ?

25 мая 2018 года в полном объеме вступил в силу новый закон Европейского союза о защите данных — GDPR (General Data Protection Regulation), отличающийся беспрецедентными штрафными санкциями (до 20 млн евро или до 4% от общего глобального дохода, в зависимости, что больше), а также способный оказать влияние на деятельность организаций вне ЕС. В настоящей статье мы рассмотрим основные требования GDPR и случаи их применимости к российским организациям. Сразу оговоримся, что поскольку РФ не входит в ЕС, непосредственное применение санкций на территории РФ вряд ли возможно, однако в случае обработки данных субъектов (физических лиц), находящихся на территории ЕС безотносительно их гражданства, российским компаниям следует быть в курсе этих требований. Следует отметить, что поскольку официального перевода GDPR на русский язык не существует, использованная в настоящей статье терминология отражает только точку зрения авторов.

СРАВНЕНИЕ ЗАКОНОДАТЕЛЬСТВА ЕС И РФ О ПЕРСОНАЛЬНЫХ ДАННЫХ

Европейское и российское законодательство в области защиты ПДн имеют много общего. Прежде всего, оба законодательства были основаны на «Конвенции по защите физических лиц при автоматизированной обработке персональных данных» Совета Европы от 1981 года, которую в 2005 году Российская Федерация ратифицировала и приняла отражающий ее ос-

новные принципы Федеральный закон 152-ФЗ «О персональных данных». В свою очередь, руководящими органами Европейского союза в 1995 году на основе той же Конвенции была принята Директива Европейского союза о защите данных 95/46/ЕС, которую и заменил GDPR в мае 2018 года. Основное отличие Директивы от GDPR в том, что последний фактически является законом прямого действия, унифицируя, в частности, размеры штрафов для всех стран.

На основании анализа российского закона и GDPR можно сделать вывод, что требования к операторам (controller) и обработчикам (processor) ПДн, приведенные в новом регламенте, во многом совпадают, особенно в части основных принципов обработки данных и прав субъектов ПДн. Тем не менее есть и отличия.

Для удобства последующих ссылок для читателя, мы будем приводить номера статей GDPR и оригинальные названия их официальных комментариев от Рабочей группы Еврокомиссии (правительства ЕС) по защите персональных данных (Article 29 Working Party).

С вводом GDPR в действие за его внедрение должен отвечать специально созданный орган — Европейский совет по защите данных (European Data Protection Board — EDPB), в который будут входить представители регуляторов по защите данных из стран ЕС (Data Protection Authority — DPA).

Рисунки 2–3 иллюстрируют схожесть основных принципов обработки данных и прав субъектов ПДн (физических лиц).

Как видно, налицо совпадение по большинству позиций (разве что в GDPR появилось пра-

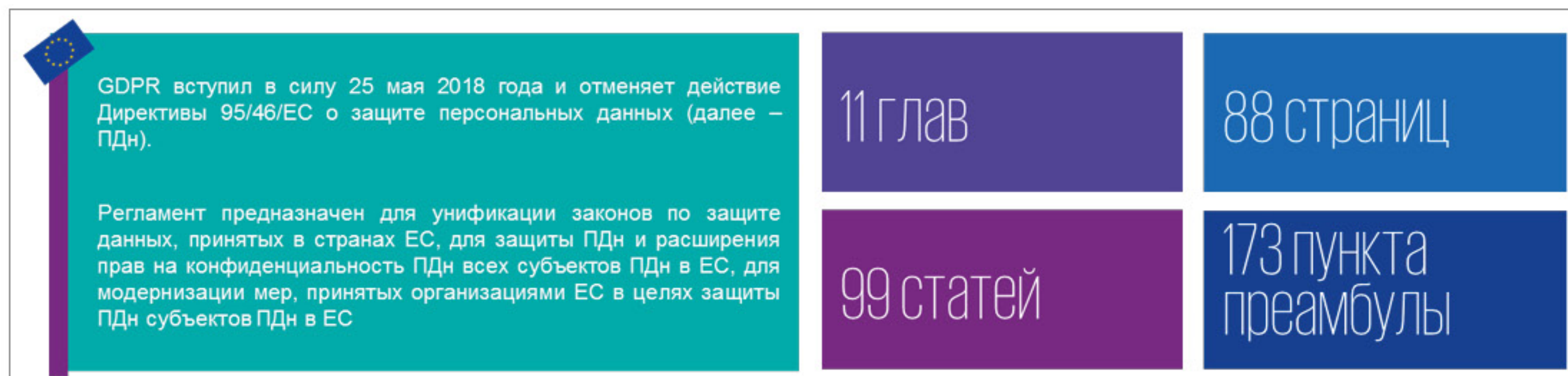


Рисунок 1. GDPR: цифры и факты



Рисунок 2. Сравнение основных принципов обработки ПДн, определенных в GDPR и 152-ФЗ



Рисунок 3. Сравнение прав субъектов ПДн, определенных в GDPR и 152-ФЗ

во субъекта требовать переноса данных от одного оператора к другому. Казалось бы, простое требование, но для его реализации (как и для уничтожения, еще говорят «право быть забытым») от оператора/обработчика требуется как минимум знать, как структурированы данные и в каких системах находятся. Несмотря на зако-

нодательные требования как в ЕС, так и в РФ, некоторые операторы иногда не слишком ясно и детально спрашивают согласие физического лица на обработку его данных и слишком широко трактуют цели обработки. Например, несмотря на то, что в конце мая приглашенный в Европарламент владелец социальной сети Face-

GDPR ГЛАВНЫМ ОБРАЗОМ ЗАТРОНУЛ РОССИЙСКИЕ ОРГАНИЗАЦИИ, ЧЬИ ФИЛИАЛЫ, ПРЕДСТАВИТЕЛЬСТВА И ДОЧЕРНИЕ ОБЩЕСТВА РАСПОЛОЖЕНЫ НА ТЕРРИТОРИИ ЕС

book заявил о намерении соблюдать требования GDPR, депутаты задавали ему много вопросов, в частности о таргетированной рекламе в контексте целей обработки данных пользователей социальной сети.

КОГО ЗАТРАГИВАЕТ GDPR ЗА ПРЕДЕЛАМИ ЕС

Ключевой статьей GDPR в отношении организаций вне ЕС, в частности российских, является Ст. 3 «Территориальная область применения». Согласно этой статье действие нового европейского закона распространяется на организации, учрежденные на территории ЕС или обрабатывающие ПДн субъектов из ЕС в рамках предоставления товаров и услуг или мониторинга поведения субъектов в ЕС.

GDPR главным образом затронул российские организации, чьи филиалы, представительства и дочерние общества расположены на территории ЕС (пункт 1 Ст 3). Кроме того, российская организация, предоставляющая свои товары и услуги субъектам, находящимся на территории ЕС, например, с использованием веб-сайта, доступного на территории ЕС, также попадает под действие пункта 2а статьи 3 GDPR. Действие данного пункта распространяется и на организации, осуществляющие мониторинг поведения субъектов ПДн в ЕС с использованием средств автоматизации обработки данных (пункт 2b статьи 3 GDPR).

Российским организациям, оказывающим услуги европейским контрагентам, на платной или безвозмездной основе работающим с гражданами ЕС или находящимися на территории ЕС, гражданам других стран/лиц без гражданства, следует определить степень влияния GDPR на организацию и выявить риски несоответствия требованиям GDPR. Следует учитывать, что помимо штрафных санкций несоответствие может повлечь за собой ущерб для репутации организации, блокировку веб-сайта или прекращение деятельности организации на территории ЕС.

Следующие типы российских организаций могут стать субъектами права GDPR:

- ♦ транспортные компании, гостиницы, банки, операторы мобильной связи;

- ♦ компании, имеющие офисы в ЕС (в том числе дочерние структуры транснациональных компаний, расположенные в РФ);

- ♦ компании, расположенные в РФ, но получающие ПДн субъектов ЕС для обработки (к примеру, компании с централизованной ИТ-инфраструктурой и серверами в РФ);

- ♦ компании, взаимодействующие с контрагентами из ЕС;

- ♦ компании, предоставляющие услуги обработки данных операторам из ЕС.

В целях приведения процессов обработки ПДн в соответствие требованиям GDPR организации следует определить потоки ПДн с учетом мест сбора, использования и хранения ПДн, перечень обрабатываемых ПДн, перечень участвующих в обработке ПДн информационных систем, баз данных, аппаратных средств и структурных подразделений организации. На основании полученной информации составить карту потоков данных, далее провести оценку рисков утечки ПДн и влияния утечки на права и свободы субъектов ПДн, а также связанные с этим риски для организации. По результатам проведенного анализа принять решение о разработке и внедрении организационных и технических мер защиты, при этом по возможности минимизируя потоки ПДн или обезличивая данные.

К тому же деловые партнеры в ЕС должны учитывать степень адекватности защиты с учетом требований GDPR в стране (организации) куда данные будут передавать.

В результате внедрения мер защиты ПДн в организации должно быть обеспечено наличие следующих доказательств соответствия GDPR:

- ♦ документированные процедуры управления рисками;

- ♦ закрепленные роли и ответственность за обеспечение конфиденциальности данных;

- ♦ документированные процедуры обработки ПДн, включающие описание порядка удаления ПДн субъектов по запросу субъекта с учетом требований законодательства страны присутствия организации, порядка прекращения обработки ПДн субъекта по запросу субъекта, порядка предоставления субъектам данных о процессах обработки ПДн, в том числе с использованием «стандартизированных иконок», порядка передачи ПДн субъекту или иной организации по запросу субъекта (data portability), порядка трансграничной передачи ПДн в страны, не обеспечивающие адекватный уровень защиты ПДн, и порядка обеспечения конфиденциальности данных;

- ♦ актуальная информация об обработке ПДн в организации с указанием целей обработки ПДн, сроков хранения данных, категорий ПДн

и субъектов ПДн, перечня организаций, в которые ПДн передаются, перечня стран-получателей ПДн, перечня мер защиты ПДн;

♦ шаблоны понятных и детальных согласий субъектов на обработку ПДн;

♦ задокументированная ответственность поставщиков услуг за обеспечение конфиденциальности данных, закрепленные требования к поставщикам услуг в договорах в части обеспечения защиты данных и инструкции по защите данных для поставщиков услуг;

♦ документированные процедуры управления инцидентами ИБ.

КЛЮЧЕВЫЕ ОТЛИЧИЯ GDPR ОТ 152-ФЗ

Российским организациям следует рассмотреть возможность внедрения следующих мер и процедур, отличных от 152-ФЗ:

♦ определить необходимость назначения Data Protection Officer-DPO (ответственного за защиту ПДн). Ст. 37 GDPR и «Guidelines on Data Protection Officers (‘DPOs’): Article 29 data protection working party. Хотя в РФ, в отличие от многих стран (в том числе ЕС) наличие ответственного за обработку ПДн является обязательным для всех организаций (GDPR требует не для всех), к DPO предъявляются и специфические требования, проиллюстрированные на рисунке 4.

♦ определить необходимость назначения представителя в ЕС: представитель необходим, если оператор или обработчик ПДн расположен не в ЕС и осуществляет на регулярной основе обработку больших объемов ПДн (специальные категории, данные о правонарушениях или приговорах). Ст. 27 GDPR;

♦ определить необходимость проведения оценки воздействия на конфиденциальность данных (Data Privacy Impact Assessment — DPIA), провести DPIA с учетом требований GDPR и рекомендаций Article 29 data protection working party, внедрить необходимые организационные и технические меры для снижения выявленных рисков. Ст. 35 GDPR и «Guidelines on Data Protection Impact Assessment (DPIA) and determin-



Рисунок 5. Описание DPIA



Рисунок 4. Требования к DPO

ing whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679»: Article 29 data protection working party;

- ♦ предусмотреть возможность субъекта ПДн обратиться к оператору или обработчику с возражением против обработки ПДн, с запросом на удаление / обновление ПДн с использованием электронных средств;

- ♦ обеспечить предоставление субъектам данных о процессах обработки ПДн, в том числе с использованием «стандартизированных иконок»;

- ♦ реализовать права субъекта на получение и передачу своих ПДн от одного оператора другому. Ст. 20 и «Guidelines on the right to data portability»: Article 29 data protection working party;

- ♦ разработать процедуры идентификации субъектов ПДн при обращении субъектов ПДн к оператору или обработчику с использованием электронных средств;

- ♦ обеспечить уведомление регуляторов об утечках данных в течение 72 часов с момента регистрации инцидента и своевременное уведомление субъектов ПДн. Ст. 33, 34 и «Guidelines on Personal data breach notification under Regulation 2016/679»: Article 29 data protection working party. В случае отсутствия офисов и представителя на территории ЕС, оператор/обработчик самостоятельно определяет регулятора для предоставления отчетности по инцидентам с учетом страны местонахождения субъектов ПДн;

- ♦ провести анализ наличия правовых оснований (см. рисунок 6) для обработки ПДн и задокументировать результаты анализа;

- ♦ проверить соответствие согласия на обработку ПДн требованиям GDPR. Ст. 7, 8 GDPR и «Guidelines on consent under Regulation 2016/679»: Article 29 data protection working party;

- ♦ определить, осуществляет ли организация обработку специальных категорий ПДн, к примеру, данные о членстве субъекта ПДн в профсоюзе относятся к специальным категориям ПДн согласно GDPR.

ТРЕБОВАНИЯ НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЗ ЕС

Особое внимание следует обратить на то, что передача ПДн в другую страну или международную организацию может осуществляться беспрепятственно только в том случае, если Европейская Комиссия приняла решение (Adequacy decision), что данная страна или территория, или один или несколько конкретных секторов этой страны, или соответствующая международная организация обеспечивают надлежащий уровень защиты. Передача ПДн в страны, не обеспечивающие надлежащий уровень защиты возможна в случае наличия одного из следующих правовых оснований: обязательные внутрикорпоративные правила (Binding Corporate

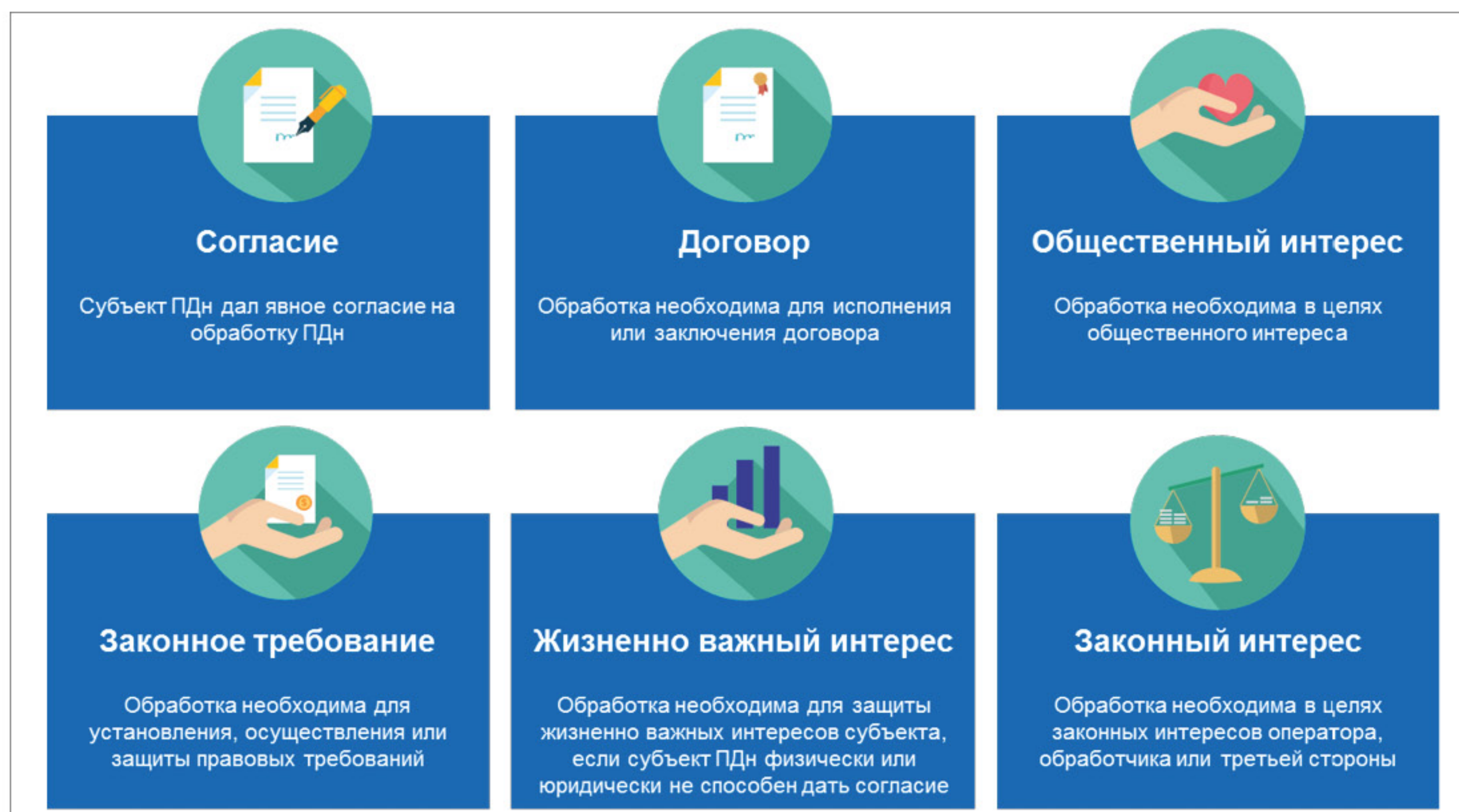


Рисунок 6. Перечень правовых оснований обработки ПДн

Rule), стандартные положения о защите данных в договоре (Standard Data Protection Clauses), Кодекс поведения (Code of Conduct) или по результатам сертификации.

Рассмотрим подробнее эти ситуации.

Страны с надлежащим уровнем защиты персональных данных на уровне законодательства. Вне Евросоюза пока список небольшой: Андорра, Аргентина, Фарерские острова, Гернси, Израиль, Остров Мэн, Джерси, Новая Зеландия, Швейцария, Уругвай. В список также еще вошли две страны, но с ограничениями: Канада (только в отношении коммерческих организаций, в отношении которых действует надлежащий национальный закон) и США (поскольку там отсутствует аналогичный национальный закон, то только в отношении организаций, присоединившихся в программе EU-US Privacy Shield Framework). В настоящее время ведутся переговоры с Японией и Южной Кореей.

Если страна не оказалась в «белом списке», необходимо удостовериться в наличии надлежащей защиты у конкретной организации вне ЕС с помощью одного из механизмов, описанных ниже:

- ♦ **стандартные положения о защите данных в договоре** о передаче данных разрабатываются и утверждаются Еврокомиссией;

- ♦ **обязательные корпоративные правила** удобны для транснациональных компаний. Когда они утверждены регулятором (DPA), можно передавать данные беспрепятственно внутри группы. Обычно корпоративные правила направляются только одному DPA в стране, где находится штаб-квартира или место наибольшего присутствия в ЕС;

- ♦ **кодекс поведения** обычно заключается между операторами ПДн в рамках отраслевой ассоциации. Подлежит утверждению DPA;

- ♦ **сертификация** — добровольное подтверждение соответствия компании требованиям GDPR. Проводится аккредитованной организацией или самим DPA. На период подготовки статьи, примеров сертифицированных компаний найти не удалось. По идее, механизм должен напоминать сертификацию по ISO 27001, PCI DSS.

Передача персональных данных субъектов из ЕС из страны не из «белого списка» при отсутствии одного из вышеописанных механизмов возможна только как исключение и требует, в частности, информирование субъекта о возможных рисках и получения согласия на такую передачу.

При приведении процессов обработки ПДн в соответствие требованиям GDPR следует учитывать внедренные в организации меры защи-

ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ПДн В GDPR КОНКРЕТНО НЕ РАССМАТРИВАЮТСЯ — ГОВОРИТСЯ ЛИШЬ О НЕОБХОДИМОСТИ ОБЕСПЕЧЕНИЯ НАДЛЕЖАЩЕГО УРОВНЯ

ты данных во избежание дополнительных временных и ресурсных затрат.

GDPR равно как и 152-ФЗ являются законодательными актами, содержащими ключевые положения по обработке и защите данных, фокусирующимися на защите прав субъектов данных. Например, технические меры защиты ПДн в GDPR конкретно не рассматриваются — говорится лишь о необходимости обеспечения надлежащего уровня. За детализированными инструкциями по построению системы защиты стоит обращаться к документам регуляторов (например, 21 приказ ФСТЭК), а также к международным отраслевым стандартам и практикам в области информационной безопасности, а также рекомендациям Рабочей Группы 29 (WP Art 29).

* * *

Прошло совсем немного времени с момента вступления GDPR в силу, практика его применения и контроля со стороны регуляторов ЕС пока не наработана. Однако ряд поставщиков услуг (в том числе российских) уже направили своим клиентам обновленные политики по защите данных с учетом нового законодательства, а некоторые крупные компании в РФ, работающие с физлицами в Евросоюзе запустили проекты по обеспечению соответствия требованиям GDPR. Тем не менее, как показывают различные глобальные опросы, большинство компаний (даже в ЕС) не соответствуют всем требованиям GDPR, поэтому представляется, что первыми внимание европейских регуляторов, скорее всего, привлекут организации в Евросоюзе, а из остальной части мира — компании, преимущественно нацеленные на клиентов-физлиц на территории ЕС. Тем не менее, всем российским организациям, оказывающим услуги субъектам данных, находящимся на территории ЕС и/или осуществляющим мониторинг их поведения, следует оценить возможность применимости Ст 3. GDPR и риски несоответствия. Если рисков нет — и черта нет, а если есть — черт не страшен подготовленным.



Антон СВИНЦИЦКИЙ
директор по консалтингу
АО «ДиалогНаука»

SWIFT В СТРАНЕ БЕЗОПАСНОСТИ

ТРЕБОВАНИЯ SWIFT CSCF КАК ИНСТРУМЕНТ ДОВЕРИЯ

Международная система обмена платежными поручениями SWIFT существует давно. Она обеспечивает обмен платежными поручениями между банками в разных странах, реализуя разветвленные международные транзакции. Объемы транзакций между участниками системы SWIFT огромны, что и привлекает к ней внимание компьютерных мошенников.

ПРОБЛЕМЫ SWIFT

Большое количество участников и существенные объемы транзакций делают систему очень привлекательной для хакеров, которые уже давно изучают возможности манипуляции платежными поручениями на уровне клиентов системы SWIFT (банков) — такие махинации очень прибыльны даже в единичных случаях. При этом для подготовки и проведения атаки, направленной на отправку нелегитимного платежного поручения, используется не только инфраструктура SWIFT, размещенная в корпоративной сети банка, но и ее окружение.

Наиболее известный пример атаки на SWIFT — «цифровое» ограбление национального банка Бангладеш на общую сумму 81 млн долл., которое было совершено в феврале 2016 года. Злоумышленниками было организовано около 40 фиктивных запросов на общую сумму 951 млн долл., из которых четыре транша было пропущено, и в результате со счетов ЦБ Бангладеш в ФРС Нью-Йорка было переведено в филиппинские казино 81 млн долл. Атака была совершена с помощью троянской программы, которая обеспечила удаленный контроль узла доступа к инфраструктуре SWIFT в банке.

Аналогичная атака была совершена и на один российский банк в середине декабря 2017 года, хотя ни имя банка, ни ущерб не озвучиваются. Сообщается только, что украденные средства были переведены за рубеж, а при проверке системы безопасности банка со стороны Банка России, проведенной после данного инцидента, были обнаружены серьезные проблемы. Эксперты Group-IB посчитали, что к преступлению может иметь отношение группировка Cobalt.

Последняя же крупная зафиксированная атака на SWIFT относится уже к апрелю этого года, когда неизвестные злоумышленники вывели около 20 млн долл. из национального банка Мексики. С учетом этой тенденции можно с уверенностью предположить, что атаки на банки и инфраструктуру SWIFT, направленные на несанкционированный перевод денежных средств, будут продолжаться.

Следует отметить, что не всегда проблемы возникают на стороне SWIFT — во многих случаях банки, из которых выводятся деньги, сами виноваты в проблемах, поскольку не уделяли достаточного внимания вопросам обеспечения информационной безопасности корпоративной информационной системы и организации безопасного информационного взаимодействия в рамках реализации процесса перевода денежных средств через систему SWIFT.

ТРЕБОВАНИЯ SWIFT CSCF

Понимая важность обеспечения защиты не только внутри самой сети, но и клиентов, SWIFT в мае 2016 года инициировала процесс реализации единого подхода к формированию требований по обеспечению информационной безопасности инфраструктуры SWIFT, размещенной у банков, а также проведения самооценки участков обмена на предмет наличия у них необходимых контролей.

С УЧЕТОМ ЭТОЙ ТЕНДЕНЦИИ МОЖНО С УВЕРЕННОСТЬЮ ПРЕДПОЛОЖИТЬ, ЧТО АТАКИ НА БАНКИ И ИНФРАСТРУКТУРУ SWIFT БУДУТ ПРОДОЛЖАТЬСЯ

Сами требования формализованы в документе SWIFT Customer Security Controls Framework (CSCF) и состоят из 27 контролей, 11 из которых пока являются рекомендуемыми к реализации.

Требования SWIFT CSCF скорее технические и больше похожи на стандарт PCI DSS, чем на обобщенные требования, описанные в международном стандарте ISO/IEC 27002:2013. Впрочем, в самом документе есть таблица соответствия между контролями SWIFT CSCF и следующим набором стандартов: PCI DSS 3.2, ISO/IEC 27002:2013 и NIST Cybersecurity Framework v1.0. Это упрощает задачи специалистов, которые ранее использовали в своей работе перечисленные стандарты, и позволяет им быстрее разобраться в требованиях SWIFT. Набор требований, необходимых к реализации, зависит от типа подключения к сети SWIFT: выделено четыре типа подключения клиента в зависимости от расположенных в корпоративной сети клиента компонент. Но даже в случае подключения к сети SWIFT через поставщика услуг, необходимо реализовывать 11 обязательных контролей, направленных на защиту процесса перевода и ИТ-инфраструктуры.

Стандарт безопасности формулирует требования для основных компонентов и объектов среды их обработки: приложений (ПО, реализующее интерфейсы взаимодействия, SWIFTNet Link, коннекторы), сетевых сегментов размещения инфраструктуры SWIFT, сетевого оборудования, съемных носителей, оборудования (серверы, рабочие станции, HSM), рабочих мест операторов, а также иных систем и компонентов, обеспечивающих формирование и передачу сообщений SWIFT.

МЯГКАЯ СИЛА SWIFT CSCF

До 31 декабря 2017 года банки должны были провести самооценку и отчитаться о ее результатах в SWIFT. Однако никаких штрафов и наказаний за отсутствие результатов самооценки не будет, кроме возможного предупреждения со стороны регулятора, в случае России — Центробанка РФ. Списки банков, не заявивших о завершении процедуры самооценки, уже должны быть переданы российскому регулятору в начале 2018 года.

РИСК НЕСОБЛЮДЕНИЯ ТРЕБОВАНИЙ НА ДАННОМ ЭТАПЕ ИСКЛЮЧИТЕЛЬНО РЕПУТАЦИОННЫЙ, ЧТО ДЛЯ МЕЖДУНАРОДНОЙ БАНКОВСКОЙ СРЕДЫ МОЖЕТ ОКАЗАТЬСЯ ПРИНЦИПИАЛЬНЫМ

В рамках самооценки банки должны либо заявить о реализации контроля, либо указать срок, в течение которого контроли будут реализованы. Однако этот срок ограничен 4 кварталом 2018 года.

То есть до конца этого года все организации, имеющие собственный BIC, должны реализовать все требуемые контроли, если они не хотят привлекать внимание основного регулятора. В дальнейшем предполагается раз в год также проводить переоценку ситуации, чтобы не упустить происходящих изменений.

Следует отметить, что SWIFT не создает собственной системы проведения аудита — компания полностью доверяет в этом вопросе регуляторам и партнерам. Так, например, компания ДиалогНаука входит в список Directory of CyberSecurity Service Providers, опубликованный на сайте SWIFT, где указаны компании, готовые предоставлять услуги по кибербезопасности для клиентов SWIFT, в том числе услуги по проведению оценки соответствия требованиям стандарта CSCF.

Риск несоблюдения требований на данном этапе исключительно репутационный, что для международной банковской среды может оказаться принципиальным. Предполагается, что если банк не выполнил требования безопасности SWIFT, об этом должны узнать его партнеры, которые самостоятельно принимают решения о том, доверять ли сообщениям от данного контрагента или нет. От самой SWIFT штрафов за несоблюдение требований не предполагается, но международную репутацию может быть очень трудно исправить.

САМООЦЕНКА И ПРИВЕДЕНИЕ В СООТВЕТСТВИЕ

Сама процедура самооценки предполагает следующие этапы:

- ♦ определение области действия стандарта и типа подключения к инфраструктуре SWIFT;

- ♦ составление плана и программы аудита, что может быть выполнено в том числе и сторонней организацией;

- ♦ проведение оценки соответствия, во время которой клиенты должны заполнить специальную анкету, где перечислены все обязательные и рекомендательные контроли и их реализация;

- ♦ регистрация отчета на портале The KYC Registry, где и нужно указать напротив каждого контроля его статус. Варианты могут быть следующие: «соответствие рекомендациям Implementation Guidelines», «соответствие с применением альтернативных мер», «планируемое соответствие» с указанием срока, «несоответствие» и «не применимо»;

- ♦ формирование плана устранения несоответствий, в результате которого поля, отмеченные как «несоответствие», должны быть заменены на «планируемое соответствие» с указанием даты.

Предполагается, что к концу этого года нужно запланировать и привести в соответствие все контроли SWIFT.

* * *

На текущий момент гибкий подход SWIFT к возможности заменить любой контроль, описанный в SWIFT CSCF, на аналогичный контроль, направленный на снижение таких же рисков информационной безопасности, позволяет учитывать особенности ИТ-инфраструктуры и технологических процессов, но не позволяет сравнивать результаты оценки соответствия разных организаций. Скорее всего, дальнейшее развитие стандарта будет зависеть от практики внедрения и успешности/неуспеха хакерских атак на систему.



Марат РАХИМОВ
ведущий инженер
ООО «Газинформсервис»

БЕЗОПАСНОСТЬ БЛОКЧЕЙНА

УЯЗВИМОСТИ ТЕХНОЛОГИИ И ИНСТРУМЕНТЫ АУДИТОРА СМАРТ-КОНТРАКТОВ

В последнее время всё чаще встречается термин «цифровая трансформация», и всё чаще обсуждаются вопросы применения передовых технологий для цифровизации различных сфер жизни общества. Блокчейн является одним из самых ярких примеров всеобщей увлеченности новым технологическим трендом за последние несколько лет. Но давайте взглянем на технологию глазами специалистов по информационной безопасности и попробуем разобраться, какие риски скрывает в себе эта технология?

Под блокчейном подразумевают распределенную peer-to-peer сеть для обмена транзакциями. О конечном состоянии сети в каждый момент времени её участники приходят с помощью специальных протоколов к консенсусу. Копия данных сети в виде неразрывной цепочки блоков с информацией о проведенных к настоящему моменту транзакциях хранится у каждого участника. Таким образом достигается высокая степень отказоустойчивости си-

стемы и неизменности хранящихся в ней данных.

О блокчейне широко начали говорить на волне популярности криптовалют, в основе которых лежит эта технология. Возможно, если бы не ажиотаж вокруг биткоина — самой популярной криптовалюты, IT-сообщество не обратило бы столь пристального внимания на саму технологию блокчейн.

С появлением в 2014 году платформы Ethereum технология блокчейн стала ассоциироваться не только с криптовалютами. С помощью смарт-контрактов, появившихся в платформе Ethereum, стало возможным реализовывать на блокчейне бизнес-логику, необходимую для проведения ICO (Initial coin offering) — проектов по привлечению инвестиций.

Рост экосистемы Ethereum за 2016 и 2017 годы был действительно впечатляющим. Как видно из диаграммы (рис. 1), в ICO-проекты вкладываются большие суммы денег.

Фокус хакеров сместился с банковских систем на ICO-проекты, и за последние несколько лет было совершено множество атак на ICO. Незрелость технологии и возможность относительно легко получить доступ к средствам, собираемым в ходе ICO проектов, привлекли внимание большого числа злоумышленников.

Ключевыми элементами любого ICO являются:

- ♦ команда;
- ♦ ИТ-инфраструктура: сайт и децентрализованное приложение (decentralized application или DApp);
- ♦ коммуникации (социальные сети, white paper, рекламные каналы).

Каждый из приведенных элементов — потенциальный вектор для ата-

ки хакеров. Многие атаки были сделаны без использования уязвимостей самой технологии блокчейн, по «старым» методам:

- ♦ фишинг;
- ♦ дефейс сайта;
- ♦ хищение паролей;
- ♦ xss;
- ♦ взлом инфраструктуры, связанной с ICO проектом.

УЯЗВИМОСТИ ПЛАТФОРМЫ ETHEREUM

Но наиболее нашумевшие инциденты использовали уязвимости новой технологии.

Первой крупной атакой на блокчейн-проект стал взлом The DAO (decentralized autonomous organization) — проекта по децентрализованному управлению инвестициями. В июне 2016 года хакер, использовав уязвимость в смарт-контракте The DAO, смог вывести из проекта инвестиционные средства в виде криптовалюты Ethereum на сумму более чем 3,6 млн эфиров, что на тот момент было эквивалентно 60 млн долларов.

В 2017 году с интервалом в несколько месяцев произошли два резонансных инцидента с криптовалютным кошельком Parity. В июле 2017 года уязвимость в смарт-контракте кошелька Parity привела к убыткам в 30 млн долларов, а в ноябре 2017 года в результате эксплуатации уже другой уязвимости были заблокированы средства пользователей в размере 300 млн долларов.

Приведенные примеры наглядно демонстрируют, что проекты, использующие технологию блокчейн, подвержены атакам и требуют тщательной проработки вопросов, связанных с безопасностью.

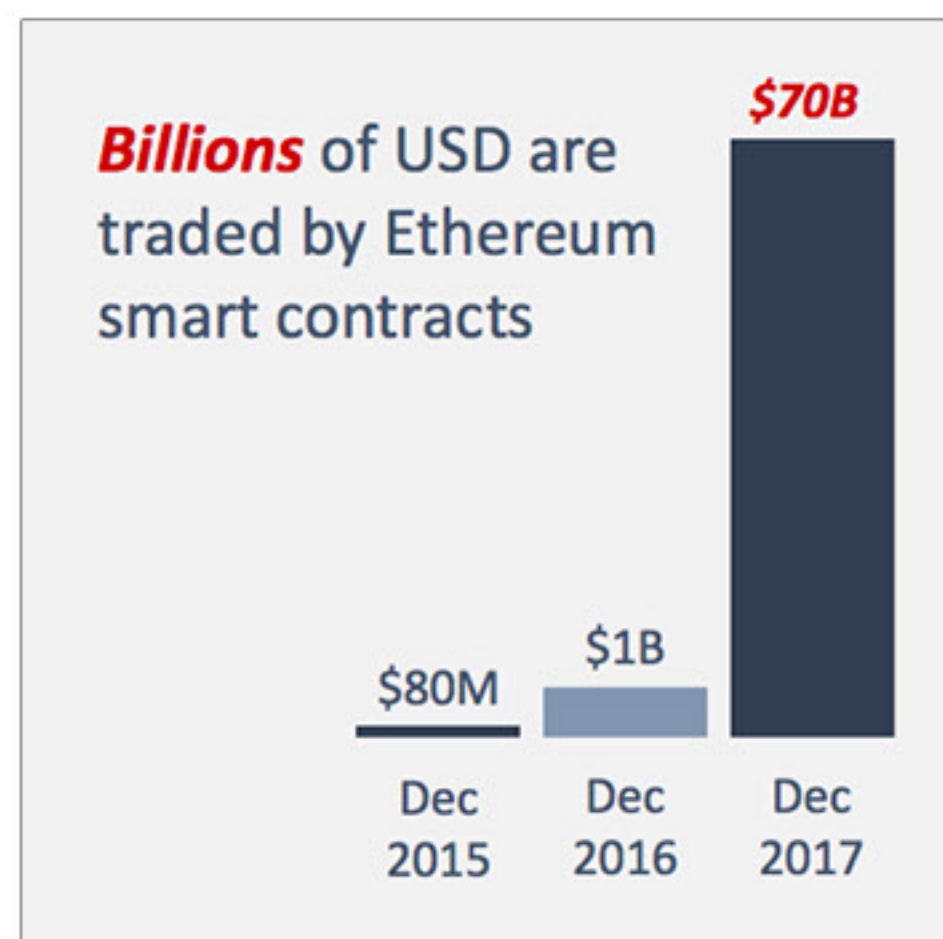


Рисунок 1. Вложения в Ethereum в 2015–2017 гг.

Исходя из архитектуры блокчейна уязвимости могут возникнуть на одном из трёх уровней:

1. Уровень сети блокчейна. В силу открытости блокчейна возникают угрозы конфиденциальности данных. Также большая опасность может исходить от майнеров — участников сети блокчейн, которые при обработке транзакций могут менять их порядок.

2. Уровень виртуальной машины. Все транзакции, проводимые в сети блокчейн, обрабатываются виртуальной машиной Ethereum, программная реализация которой также может быть уязвима к атакам хакеров.

3. Уровень языка Solidity, который используется для программирования смарт-контрактов. Уязвимости в коде Solidity представляют самый широкий класс уязвимостей. Самым распространённым примером уязвимости в смарт-контрактах является уязвимость re-entrancy (именно ее использовали при взломе The DAO).

ИНСТРУМЕНТЫ АУДИТОРА СМАРТ-КОНТРАКТОВ

Для поиска уязвимостей в смарт-контрактах Ethereum применяются различные инструменты.

«Mythril». Одним из широко используемых является инструмент «Mythril» от компании ConsenSys. Это анализатор безопасности, который работает с так называемым байт-кодом, который программа предварительно компилирует из исходного кода. На вход принимается байт-код, который затем анализируется с использованием связки статического анализа, символического анализа и проверки control flow.

В «Mythril» реализована собственная EVM на Python. Внутреннее устройство

этой виртуальной машины состоит из глобального состояния, содержащего в себе еще три — Machine State, Environment и World State. Каждое из состояний обозначается буквами, используя которые можно создавать формулы для проверки с помощью инструментов автоматического доказательства теорем. (рис. 2).

«Mythril» на основе байт-кода строит control-граф выполнения программы. Все условия <if> в смарт-контракте представляются в виде байт-кода и в виде ограничений путей. Стоит отметить, что такое представление позволяет использовать Z3 solver. Он позволяет визуальным образом представить все возможные состояния контракта для дальнейшего решения прикладных задач.

«Oyente». Второй инструмент — «Oyente» — начал активно развиваться после взлома The DAO. Это анализатор кода, который также основан на символическом выполнении. Есть его онлайн-версия, которая работает в связке с Remix — самой распространённой IDE для написания смарт-контрактов.

«Oyente» состоит из нескольких модулей и содержит в том числе builder для построения потока выполнения программы и анализатор путей выполнения программы. Также анализатор дает визуальные отображения и валидирует найденные уязвимости, доказывая, что они действительно «true», а не «false positive». «Oyente», так же как и «Mythril», использует Z3 solver (рис. 3).

Анализатор автоматически проверяет, нарушаются ли утверждения (assert), а также поддерживает работу с циклами. Кроме того, инструмент позволяет настраивать состояние блокчейн-окру-

жения для анализа внешних контрактов. «Oyente» генерирует тесты для проверки условий пути, которые можно использовать в других фреймворках, например, Truffle. Анализатор для оптимизации и ускорения работы может упрощать символьные переменные. Из плюсов стоит отметить возможность работы с большинством контрактов, однако требует большого числа вычислительных ресурсов.

«Manticore». Изначально создавался как анализатор для Linux, затем к нему добавился анализатор EVM-машины. Он выявляет все функции в смарт-контракте, генерирует наборы транзакций, соответствующих различным путям выполнения смарт-контракта и проверяет наличие ошибок в соответствующих путях.

РЕКОМЕНДАЦИИ

В заключение — несколько рекомендаций по безопасной разработке смарт-контрактов:

♦ При разработке смарт-контрактов необходимо пользоваться уже проверенными библиотеками, кодом и накопленным сообществом Ethereum опытом. Многие типовые задачи уже безопасно реализованы профессиональными разработчиками и компаниями лидерами в области безопасности смарт-контрактов (Zeppelin, ConsenSys).

♦ Обязательно необходимо проводить аудиты блокчейн-проектов силами сторонних аудиторов и реализовывать программу bug-bounty, тем самым мотивировать white-хакеров искать уязвимости в вашем проекте.

♦ Также для безопасной разработки необходимо глубоко погружаться в язык Solidity и платформу Ethereum.

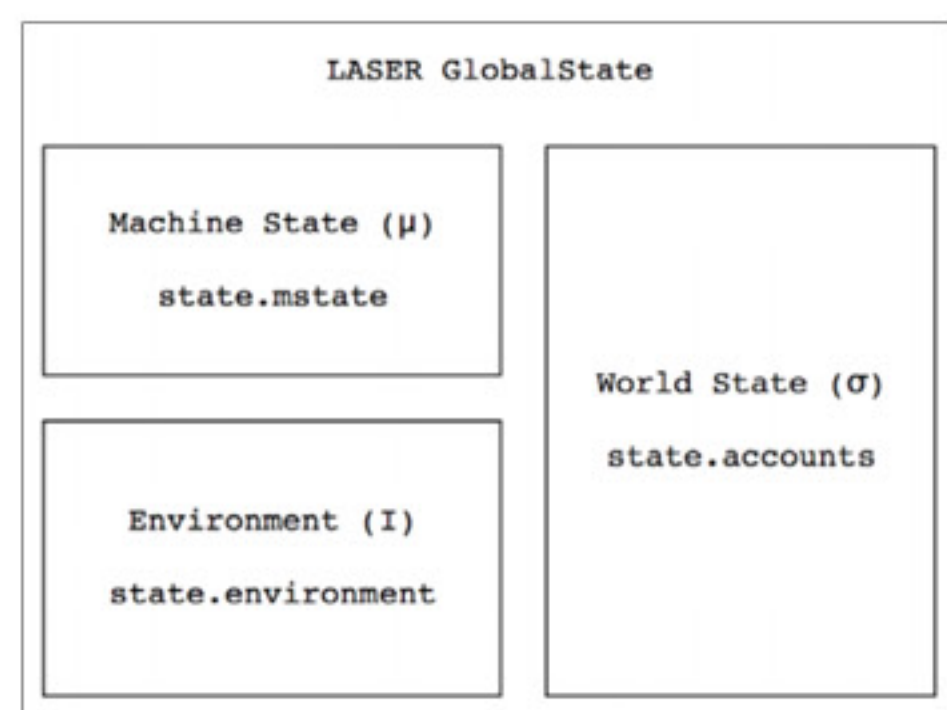


Рисунок 2. Модель состояний «Mythril»

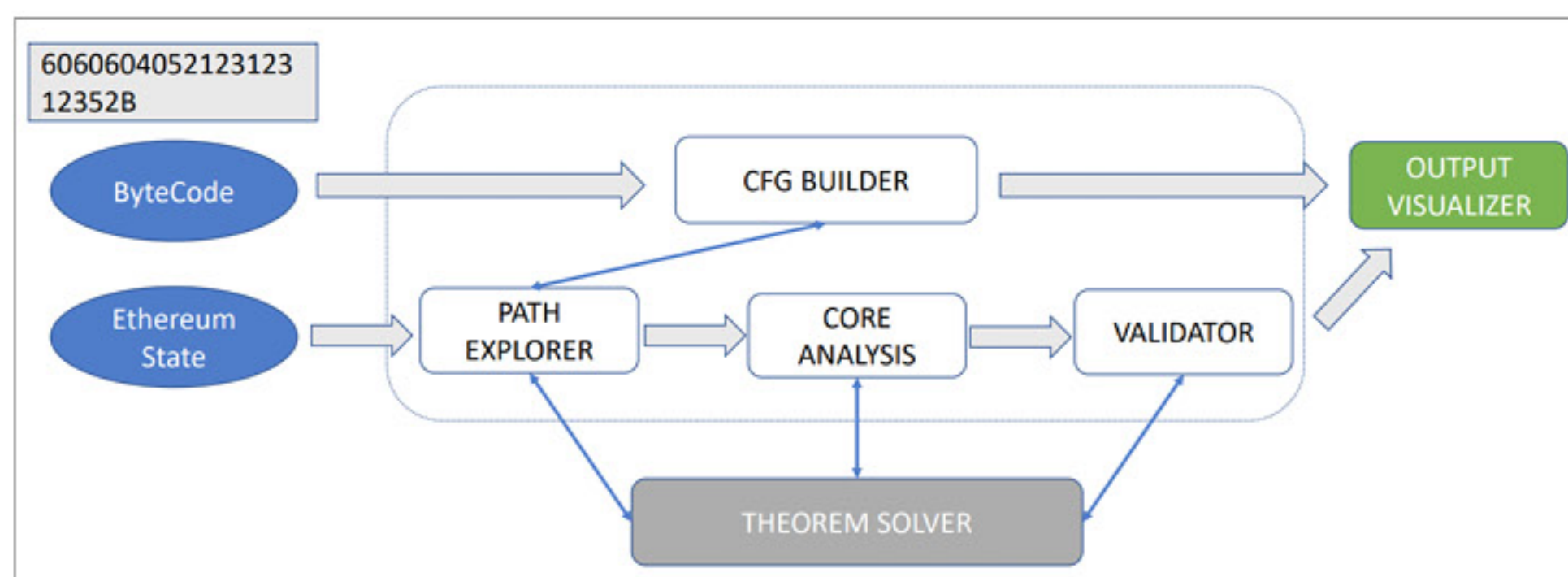


Рисунок 3. Архитектура «Oyente»



Дмитрий МИХЕЕВ
технический директор
компании «АйТи
БАСТИОН»

СТРАХ И НЕНАВИСТЬ ПРИ УДАЛЕННОМ ДОСТУПЕ

ТРИ СВЕЖИХ ПРОЕКТА КОМПАНИИ
«АЙТИ БАСТИОН»

Проблемы безопасности беспокоили банки задолго до возникновения такого феномена как ИТ. Более того, многие практики и способы решения проблем, принятые в том, что мы сейчас называем информационной безопасностью, были разработаны, опробованы и отточены как часть инфраструктуры обеспечения финансовых операций. Разграничение полномочий, эшелонирование средств защиты, вопросы, связанные с формальным подтверждением эффективности — все это в том или ином виде много лет назад использовали и венецианские банковские дома и конторы Ганзейского союза.

Говоря о современной практике ИБ, мы можем увидеть, что существует много способов добиваться необходимого уровня управления рисками: сколько банков, столько и подходов к решению задач. Задачи же у всех примерно одни и те же. За текущий год у нашей технической команды было несколько интересных проектов по задачам ИБ по направлению обеспечения контроля действий администраторов, как внешних подрядчиков, так и внутренних исполнителей. Проекты отличались как по масштабу, так и по фокусу усилий в рамках проекта.

ПРОЕКТ ПЕРВЫЙ. С ПОРТАЛОМ ДОСТУПА

Например, в одном из проектов мы старались решить задачу предоставле-

ния единой точки доступа для внешних подрядчиков в рамках распределенной инфраструктуры банка. Ключевыми требованиями проекта, помимо собственно предоставления доступа внешним подрядчикам, было обеспечение контроля данных доступов разнообразными средствами защиты.

Кроме того, так как у банка организовано несколько точек концентрации оборудования, система контроля внедрялась в каждой из этих точек. Таким образом, этот проект оказался хорошей возможностью применить так называемый Портал доступа — дополнительный модуль, позволяющий реализовать единую точку входа, для работы с которым достаточно только браузера, способного работать в режиме html5. Так как Портал — это веб-приложение, с ним удобно взаимодействовать как в целях балансировки на надежность и производительность, а также обеспечивать необходимые дополнительные средства защиты, например, использовать WAF.

В результате проведенных работ удалось отказаться от существующих нескольких точек доступа для подрядчиков, объединив необходимые пути входа в рамках нового узла доступа, с сохранением привычных возможностей. Заказчик получил возможность всегда знать, кто и когда выполняет работы, а также средство для проведения оперативного контроля выполняемых действий.

ПРОЕКТ ВТОРОЙ. ДЛЯ УДОБСТВА АУДИТА

Еще одним проектом с использованием модуля Портала стал проект, где основной задачей ставилось удобство аудита действий внешних подрядчиков и работающих удаленно собственных сотрудников.

Понятно, что специалистам по безопасности сложно сочетать в одном предложении «удаленный доступ» и «инфраструктура банка». Тем не менее, учитывая высокие требования к показателям работоспособности различных элементов информационного хозяйства банка, а также сложности с кадрами, приходится решать и такие задачи тоже. Для удаленного доступа в инфраструктуру банка были выделены необходимые ресурсы для удаленной работы, отработан регламент предоставления таких доступов и особенности жизненного цикла таких вариантов входа.

Конечно, это потребовало серьезных усилий — все-таки, это банк, и требования к подобного рода организациям серьезные, как и последствия за нарушения. Тем не менее для обеспечения продуктивной работы руководство банка на такие жертвы идет — это, по-видимому, наиболее прямой способ добиваться результата имеющейся подготовленной и сработавшейся командой. Чтобы сохранять необходимый контроль угроз и минимизировать риски, для доступа к определенным элементам инфраструктуры было применено наше решение по контролю действий администраторов, с интеграцией с подсистемой многофакторной авторизации, использующейся в компании. Для авторизации внешних ис-

**ПОНЯТНО, ЧТО СПЕЦИАЛИСТАМ ПО
БЕЗОПАСНОСТИ СЛОЖНО СОЧЕТАТЬ
В ОДНОМ ПРЕДЛОЖЕНИИ «УДАЛЕННЫЙ
ДОСТУП» И «ИНФРАСТРУКТУРА БАНКА»**

полнителей систему дополнительной авторизации удалось подключить по протоколу Radius минимальными усилиями. В качестве «токена» выбранное решение позволяет использовать авторизатор на смартфоне, что снижает затраты на управление доступом.

По мнению специалистов банка, это решение позволяет исполнителям выполнять технические задачи наиболее оперативно, без компрометации требований по безопасности. Для удобства работы офицеров безопасности, на которых легла обязанность контролировать доступ привилегированных пользователей, был внедрен модуль Портала доступа. Одной из возможностей Портала является возможность полнотекстового поиска по всем данным сессий удаленной работы, где зафиксированы команды, вводившиеся с клавиатуры, открытые окна, URL адреса и другие мета-данные, которые наша система собирает в процессе предоставления доступа. Средства полнотекстового поиска и «легкий» веб-интерфейс позволяют аудиторам выполнять оперативный мониторинг и действия по расследованию возникающих инцидентов за минимальное время, часто — непосредственно до завершения сессии удаленной работы, вызвавшей вопросы.

Таким образом, поставленные задачи проекта были успешно решены штатным функционалом нашей системы контроля действий администраторов. Средства поиска и анализа инцидентов позволяют контролировать и расследовать инциденты, связанные с удаленными работами, а выбранные технические решения — с минимальными затратами обеспечивать жизненный цикл заявок на предоставление доступа.

ПРОЕКТ ТРЕТИЙ. БОЛЬШАЯ ИНФРАСТРУКТУРА

Если два упомянутых проекта различались «фокусом», на котором сосредотачивались усилия при внедрении, то третий проект, который хочется вспомнить, оказался очень серьезным испытанием для нашей технической команды. Огромная инфраструктура, с которой нам пришлось столкнуться, потребовала напряженной работы как на этапе проектирования, так и на

НАШИ ЗАДАЧИ, КАК РАЗРАБОТЧИКА СИСТЕМЫ КОНТРОЛЯ, — ОБЕСПЕЧИТЬ В ПРОДУКТЕ ДОСТАТОЧНУЮ ГИБКОСТЬ И ТЕХНИЧЕСКУЮ ГОТОВНОСТЬ ПОДДЕРЖИВАТЬ РАЗНЫЕ ПОДХОДЫ

стадии внедрения и опытной эксплуатации. Нам поставили задачу автоматизировать контроль доступа к элементам инфраструктуры, предоставляемой как сервис в рамках облачной системы банка.

Для выполнения этих задач, мы реализовали слой интеграции с VmWare Orchestrator, чтобы при выполнении задач по развертыванию блоков инфраструктуры по заявкам от рабочих групп, необходимые административные доступы автоматически добавлялись в политику системы контроля доступа. Так как инфраструктура в сети заказчика разделена на несколько непересекающихся сегментов, такие узлы интеграции потребовалось организовать для каждого из них. Бизнес-логика оркестратора полностью отделена от слоя интеграции и предоставления доступа, к системе контроля от нее приходят наборы команд на добавление и удаление объектов политики.

Кроме того, так как инфраструктура заказчика расположена более чем в двух дата-центрах, потребовалось реализовать нестандартный механизм репликации настроек и политики узлов системы, чтобы обеспечить управляемость, требования к надежности системы в целом.

Для реализации этого механизма, мы использовали возможности штатного программного интерфейса, предоставляемого нашей системой. Это позволило не использовать в реализации такие подходы как синхронизация баз данных, физическую репликацию. Хотя программный интерфейс не проектировался для выполнения конкретно данного сценария работы, нам удалось добиться необходимого результата без изменения ядра системы, в короткие сроки.

Выбранные технические решения позволяют построить распределенную систему контроля доступа к ресурсам с

коротким жизненным циклом, минимизировать ручные операции по предоставлению доступа, а также реализовать контроль рисков, связанных с нарушением сетевой связности сети управления.

Сложность проекта заключалась не только в количестве доработок, но и в масштабе — очень большая инфраструктура, очень много правил и крайне серьезный уровень «бумажной» проработки, т.к. проект был частью крупного проекта по модернизации ИБ, с участием нескольких крупных интеграторов и других подрядчиков. Обычно на пилотных проектах и изначальных внедрениях мы начинаем взаимодействовать с подрядчиками ближе к завершению работ, здесь же наши коллеги и партнеры оказали нам неоценимую помощь, за что им, конечно, огромная благодарность.

* * *

Как можно наблюдать по этим историям, задачи у разных финансовых организаций довольно схожи — в частности, вопросы контроля доступа администраторов к критичным элементам, обрабатывающим персональные или финансовые данные, возникают и требуют обработки. При этом в зависимости от состояния инфраструктуры и сложившихся традиций и подходов, детали реализации могут серьезно отличаться. Наши задачи, как разработчика системы контроля, — обеспечить в продукте достаточную гибкость и техническую готовность поддерживать разные подходы, как с технической точки зрения, так и в части желания идти на потенциально сложные проекты. Кроме того, что это позволяет лучше решать задачи заказчиков, такие проекты еще и довольно интересны нам, как специалистам по ИБ.



Леонид БОНДАРЕНКО

руководитель отдела информационной безопасности АО «Кросс технолджис»

УТЕЧКИ ДАННЫХ

НОВЫЕ ИНСТРУМЕНТЫ ДЕТЕКТИРОВАНИЯ И КОНТРОЛЯ



```

0 1 0 0 1 0 0 0 0 1 0 0
0 1 0 1 0 1 0 0 1 1 0 0
0 1 0 0 1 0 0 0 0 1 0 0
0 1 0 1 0 1 0 0 1 1 0 0
0 1 0 0 1 1 0 0 0 1 0 0
1 1 1 1 0 1 0 0 1 0 0 0
0 1 0 0 0 1 0 1 0 1 0 0
1 1      0      0 1 1 0 0
  
```

Высокое проникновение информационных систем во все сферы бизнеса, промышленности и государства порождает и соответствующие угрозы. Угроза нарушения конфиденциальности информации — одна из самых опасных. Нарушение конфиденциальности равно утечка данных.

НАПИСАНО МНОГО

Проблематика утечек и борьбы с ними описаны довольно обширно и подробно. Новости про громкие утечки появляются ежемесячно, их освещают как издания и информационные порталы по информационной безопасности, так и бизнес-ресурсы. Вендоры решений по информационной безопасности публикуют периодические отчеты, в которых приводится неутешительная статистика и постоянно растущие цифры числа утечек и понесенного в результате этих утечек ущерба, и статьи с подробным описанием того или иного инцидента.

Изучая информационное поле вокруг инцидентов, связанных с утечками данных, становится очевидно, что проблемы есть во всех вертикалях и от размера компании не зависят — во всех организациях и компаниях есть информация, которую требуется защищать, и люди, мотивированные этой информацией завладеть. Даже если таких людей нет, то случайные утечки не менее частый инцидент, чем преднамеренные.

Про борьбу с утечками также написано много и подробно. Но технологии не стоят на месте и на проблемы, которые ранее считались не решаемыми, находят ответы. О некоторых из таких ответов пойдет речь дальше.

DLP

Для снижения рисков утечек данных обычно применяются специализированные системы защиты от утечек данных (Data Loss Prevention — DLP).

Для того, чтобы утечки информации контролировать, просто установить DLP-систему недостаточно, ее нужно

очень тщательно настроить. Определить разрешенные и запрещенные способы передачи и вывода информации в политиках. Самое сложное в этом процессе — каким-то образом описать информацию, перемещение которой нужно контролировать.

В DLP-системах для идентификации информации используются различные методы: ключевые слова, регулярные выражения, цифровые отпечатки, детектирование форм и печатей и т.д., которые являются автоматическим инструментом принятия решения на основании заложенных правил. Но, как и во всех системах, которые необходимо настраивать на детектирование, для DLP-систем применимы понятия ошибок первого и второго рода.

ОШИБКИ

Ошибки первого рода — ложноположительные срабатывания, ошибки второго — ложноотрицательные. Соответственно, добиться ситуации, когда все события в DLP-системе являются утеч-

ками, можно, но в таком случае есть большая вероятность, что многие из утечек пропущены. И наоборот, когда персонал, работающий с DLP-системой, хочет, чтобы максимальное число утечек детектировалось, большая вероятность того, что в системе будет много событий, утечками не являющихся.

Для снижения ложных срабатываний нужен механизм, позволяющий однозначно сказать, является ли информация в передаваемом файле контролируемой.

АКТУАЛЬНЫЕ ПОЛИТИКИ

Так как специалисты, настраивающие систему, не являются владельцами или создателями информации внутри компании, то и политики, описывающие эту информацию, формируются периодически, и, как показывает практика, достаточно редко. А новая информация создается практически каждый день. При этом получаем защиту только формально: система в эксплуатацию введена, но актуальных политик нет.

Для того, чтобы такую ситуацию исправить, необходимо вовлекать владельцев и создателей информации в непрерывный процесс ее классификации, который должен происходить в реальном времени. Причем эта классификация должна выполняться таким образом, чтобы ее можно было применить в политиках DLP-системы. Помимо этого, классификация должна быть обязательной, и создатель\владелец должен сам принимать решение к какому типу информации нужно относить сведения, содержащиеся в файле, в соответствии с принятым в организации перечнем защищаемой информации.

Для этого необходимо внедрять средства автоматизации классификации создаваемых и обрабатываемых электронных документов, которые позволяют классифицировать документы при их сохранении или выводе на печать. Такие инструменты позволяют пользователю выбрать метку конфиденциальности из списка доступных и представить ее в документ как правило в двух видах: визуальная метка и скрытая.

МАШИННОЕ ОБУЧЕНИЕ

Использование современных методов машинного обучения может позволить

НЕОБХОДИМО ВОВЛЕКАТЬ ВЛАДЕЛЬЦЕВ И СОЗДАТЕЛЕЙ ИНФОРМАЦИИ В НЕПРЕРЫВНЫЙ ПРОЦЕСС ЕЕ КЛАССИФИКАЦИИ, КОТОРЫЙ ДОЛЖЕН ПРОИСХОДИТЬ В РЕАЛЬНОМ ВРЕМЕНИ

проанализировать информацию в уже проклассифицированных документах и подсказать пользователю, как проклассифицировать новый документ. Но окончательное решение и в этом случае должно оставаться за пользователем.

При этом инструменты классификации документов и контроля перемещения документа по метке конфиденциальности позволяют проследить весь жизненный цикл документа от его создания до уничтожения, включая его перемещение внутри организации и выход за пределы контролируемой зоны при интеграции с DLP-системой.

Инструменты аудита систем классификации электронных документов позволяют воссоздать и систематизировать всю историю создания документа вне зависимости от существующих в компании систем документооборота: восстановить цепочку создания версий, копий, черновиков документа с чистого листа и до его финальной версии, в том числе все отправки на печать, по каждому документу определить его местонахождение, а также кто, где и когда с ним работал, оперативно выявить попытки и факты нарушения установленного режима защиты информации и политик информационной безопасности в рамках конфиденциального электронного документооборота, по каждому пользователю найти документы, к которым у него есть доступ, узнать где, когда и с какими из них он работал.

УДОБНЫЕ ИНСТРУМЕНТЫ

Инструменты классификации могут быть дополнены аналитикой, которая позволит выявить, кто в компании создаёт наиболее ценную информацию, кто ее обрабатывает, как она перемещается. Эти данные могут стать частью Security Intelligence (SI) или User Behavior Analytics (UBA).

Удобным инструментом в системах классификации является визуализация жизненного цикла документа в виде графического дерева.

Наличие скрытой метки в документе так же помогает при расследовании инцидентов утечек данных, давая возможность определить принадлежность к компании документов, найденных за пределами организации.

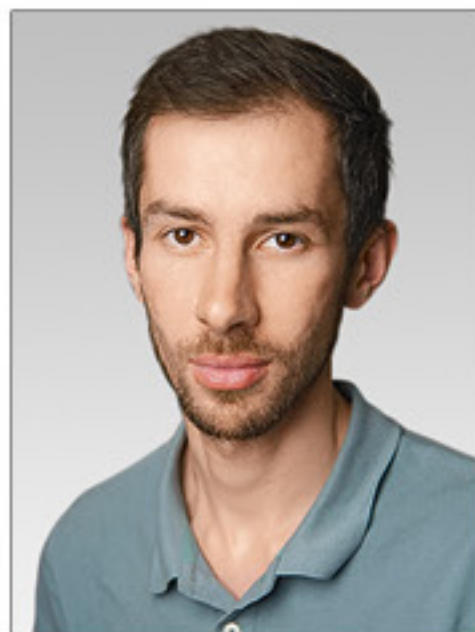
Так как вся аналитика и возможность гранулированной настройки DLP-системы базируется на метке, проставленной в файл, то должное внимание должно отводиться и защите самой метки от подмены или удаления.

IRM

Принимая во внимание тот факт, что ни одна из DLP-систем не является стопроцентным гарантом защиты от утечек, система классификации документов может стать базой для внедрения систем класса Information Rights Management (IRM). Документы, проклассифицированные определенным образом, должны быть упакованы в криптоконтейнер с разграничением прав доступа. Документы, защищенные при помощи IRM-систем, невозможно открыть, не имея доступа к серверу, ключей расшифрования и соответствующих прав доступа, наложенных на документ.

* * *

Таким образом система классификации электронных документов позволит не переплачивать за защиту информации, не имеющей ценность, а сфокусироваться на защите действительно критичной информации, послужит фундаментом для построения и гранулированной настройки систем контроля утечек данных и обеспечения конфиденциальности информации.



Георгий КАРАЕВ
руководитель
направления
исследования
данных компании
«Перспективный
мониторинг»

ПРОВОДНИК ДЛЯ ВОСХОЖДЕНИЯ НА ГОССОПКА

ЗАКАЗЧИК НЕ ДОЛЖЕН ПОКУПАТЬ
«КОТА В МЕШКЕ»

В октябре 2017 года компания «Перспективный мониторинг» (ГК «ИнфоТеКС») и ФСБ России заключили соглашение о взаимодействии в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагировании на компьютерные инциденты. С весны 2018 года подключаем заказчиков к ГосСОПКА.

НАЧАЛО СОТРУДНИЧЕСТВА

Главная задача, которую мы решаем в рамках услуги подключения к ГосСОПКА — передать данные об инцидентах информационной безопасности по вертикали иерархической структуры ГосСОПКА в форматах, отвечающих актуальным требованиям регулятора, и в установленные сроки. Но как мы узнаём об инциденте?

С технической (не процессной) точки зрения подключение к ГосСОПКА начинается с построения системы мониторинга ИБ. На стороне заказчика размещаются сетевые и хостовые средства обнаружения компьютерных атак. Данные с этих сенсоров могут поступать напрямую к нам в Центр мониторинга либо предварительно регистрироваться и анализироваться на стороне заказчика. Успешное выполнение условий правил корреляции событий приводит к фиксации инцидента информационной безопасности, в системе управления инцидентами заводится карточка инцидента, с которой происходит вся дальнейшая работа. Именно постоянный мониторинг и обработка (идентификация, классификация, информирование, сдерживание, расследование и

устранение последствий) инцидентов помогают успешно выявлять компьютерные атаки и своевременно на них реагировать.

Когда мы общаемся с потенциальными заказчиками, нам часто задают вопрос в духе: «Мы субъект КИИ, похоже нам придётся подключиться к ГосСОПКА. Но с мониторингом у нас... не очень... Нет ни средств, ни людей. Что делать?». Увы, пока ответ один — комплекс средств мониторинга нужно будет приобрести (или взять в аренду при аутсорсинге) и развернуть.

АКТУАЛЬНОЕ СОСТОЯНИЕ

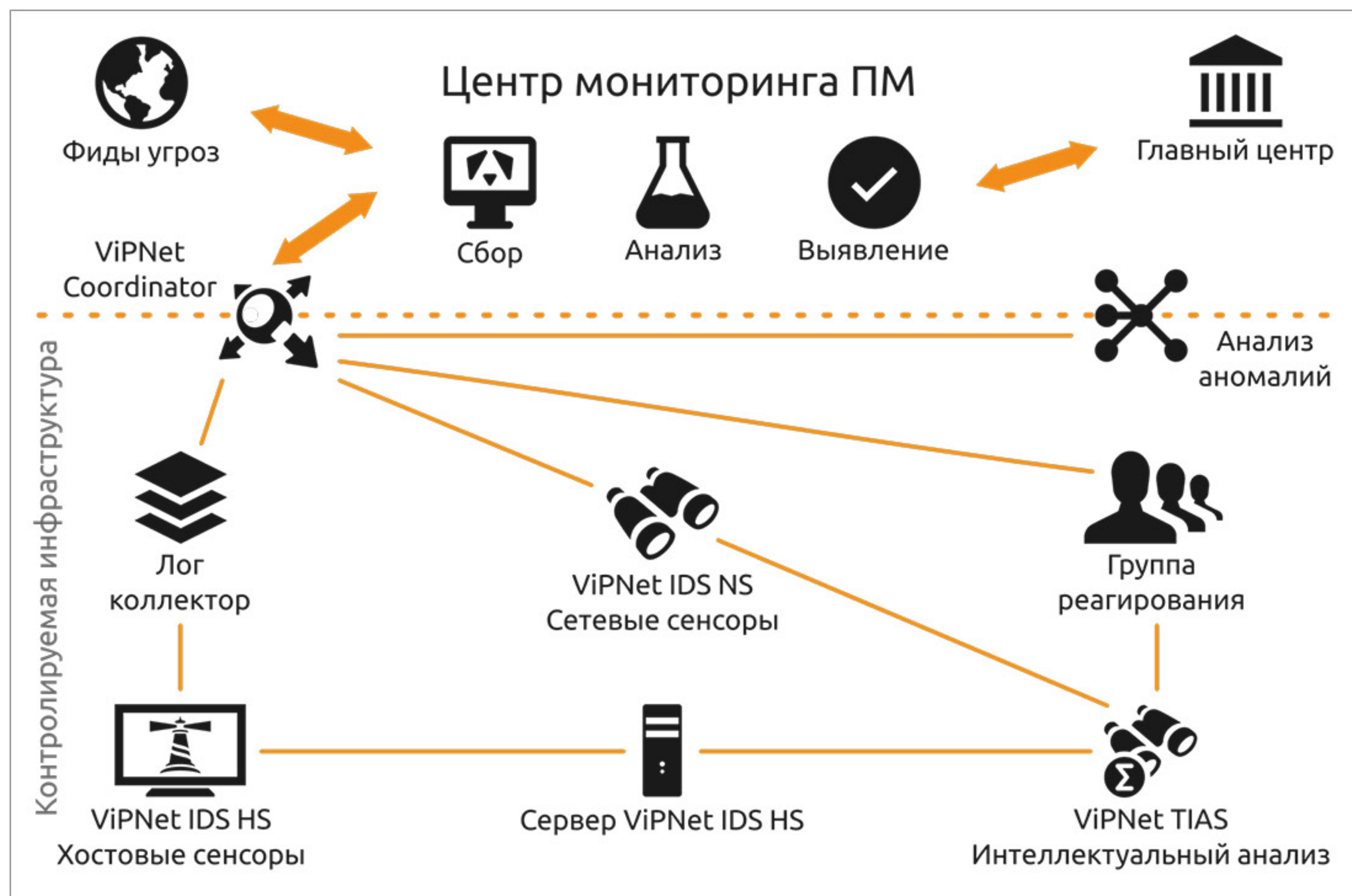
Вторая задача, определённая регулятором, — сформировать и поддерживать в актуальном состоянии информацию о контролируемых ресурсах. Эту задачу мы решаем двумя способами, которые дополняют друг друга. Сначала мы вместе с заказчиком определяем пул контролируемых ресурсов: от информационных систем (включая АСУ ТП) до конкретных сетевых узлов (АРМов, серверов, контроллеров, маршрутизаторов и т.д.). После этого мы получаем перечень установленно-го программного обеспечения на каждом из контролируемых узлов. Состав ПО загружается в нашу систему управления уязвимостями, которая отслеживает появление новых уязвимостей в публичном поле. Если версия установленных и зарегистрированных в системе программных пакетов совпадает с той, где есть уязвимость, владельцу информационного ресурса приходит уведомление с рекомендациями по устранению данной уязви-

мости или необходимыми компенсационными мерами.

По рекомендациям регулятора, контроль сведений об уязвимостях информационных ресурсов носит периодический и системный характер. Например, ежемесячно проводятся сетевое и системное сканирование ресурсов автоматизированными средствами и контроль выполнения требований безопасности. Пройгнорировать найденные слабости в защите тоже не получится — раз в квартал нужно будет контролировать устранение ранее выявленных уязвимостей. А тестирование на проникновение проводится не реже одного раза в год, чтобы оценить эффективность системы защиты. Его мы тоже можем провести и смоделировать действия злоумышленника, дать оценку, сколько ресурсов и времени потребуется для успешной кибератаки на заказчика. Знание векторов атак даёт возможность подготовиться к ним и снизить негативные последствия.

ОТКУДА АТАКА?

Часто к нам обращаются заказчики с просьбой расследовать инцидент информационной безопасности и выяснить откуда «пришла» атака, каковы цели и мотивация атакующего, кто был вовлечён в проведение атаки со стороны жертвы, какие методы, уязвимости и инструменты использовал атакующий. Эти данные пригодятся для передачи информации об инциденте в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).



Анализ событий и обнаружение компьютерных атак

В случае выявления инцидента наш заказчик не останется один на один с проблемой. Мы поможем среагировать на инцидент, дадим рекомендации, что нужно сделать в первую очередь, чтобы снизить негативное влияние атаки, и как ликвидировать последствия. Мы также проанализируем результаты устранения последствий инцидентов.

СИЛЫ ГОССОПКА

Если посмотреть в нормативные документы, то там встречается понятие «силы ГосСОПКА». «Силы» — это кадровое обеспечение. Опыт общения с заказчиками наглядно показывает, что люди — одна из острых проблем. Их

или нет, или их недостаточно, или у них недостаточно знаний и опыта. Мы обучаем и информируем заинтересованных лиц по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак, помогаем повысить осведомлённость пользователей в вопросах обеспечения безопасности информации.

В случае самостоятельного подключения к ГосСОПКА субъекту будет необходимо обеспечить взаимодействие с 8 Центром ФСБ России, выполнить организационные и технические требования в соответствии с нормативными правовыми актами и методическими рекомендациями, раз-

вернуть специализированные системы взаимодействия с технической инфраструктурой НКЦКИ (только для значимых объектов КИИ). В случае подключения через корпоративный центр ГосСОПКА «Перспективного мониторинга» — заключить с нами соглашение и уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности корпоративного центра.

Мы не хотим, чтобы потенциальные заказчики покупали «кота в мешке», поэтому даём возможность протестировать услуги Центра мониторинга во время месячного пилотного проекта. За это время мы вместе с заказчиком сможем оценить готовность инфраструктуры к подключению и понять необходимый на постоянной основе объём работ.

Остались вопросы? Пишите на info@amonitoring.ru.

ОПЫТ ОБЩЕНИЯ С ЗАКАЗЧИКАМИ НАГЛЯДНО ПОКАЗЫВАЕТ, ЧТО ЛЮДИ — ОДНА ИЗ ОСТРЫХ ПРОБЛЕМ. ИХ ИЛИ НЕТ, ИЛИ ИХ НЕДОСТАТОЧНО, ИЛИ У НИХ НЕДОСТАТОЧНО ЗНАНИЙ И ОПЫТА



Денис КАЛЕМБЕРГ
генеральный директор
компании SafeTech

ОБЛАЧНАЯ ПОДПИСЬ НА СМАРТФОНЕ

КАК ЗАЩИТИТЬ ЦИФРОВОЕ ВЗАИМОДЕЙСТВИЕ ЧЕЛОВЕКА С БИЗНЕСОМ И ГОСУДАРСТВОМ?

В век цифровой экономики технологии позволяют нам общаться, делать финансовые проводки и подписывать электронные документы, не видя друг друга. Это очень удобно и позволяет сэкономить огромное количество времени, однако требуется обеспечить безопасность личности и организаций, надежно защитить их транзакции от компьютерных мошенников и при этом сохранить удобство цифрового взаимодействия граждан с государством и бизнесом. Одним из наиболее подходящих решений этой задачи могла бы стать квалифицированная облачная подпись на смартфоне — мобильном устройстве, ставшем в последние годы нашим верным спутником.

ДОСТУП К ОБЛАКУ — КАКОЙ ВАРИАНТ ВЫБРАТЬ?

Камнем преткновения для реализации квалифицированной «облачной» электронной подписи долгое время было сохранение уровня безопасности при удаленном акцептовании (подтверждении) операции подписи, ключ которой находится, например, в HSM, Hardware Security Module.

В качестве способа доступа к ключам пользователей, хранящимся в облаке, уже давно было предложено на выбор несколько вариантов: многоразовый пароль, одноразовый пароль, включая от-

правку кода через SMS, аутентификация с использованием токена, подключаемого к компьютеру. При этом доступ к ключам при помощи одноразовых и/или многоразовых паролей не обеспечивает приемлемого уровня безопасности и, соответственно, противоречит требованиям регулирующих органов. А использование аппаратных смарт-карт и токенов «убивает» саму идею облачной подписи. Ввиду технологических и логистических ограничений до сих пор не получила значимого развития и электронная подпись на специальных SIM-картах, которые фактически должны были стать носителями ключей пользователей и самим средством электронной подписи. Обойти описанные выше ограничения позволила технология аутентификации владельца облачных ключей подписи при помощи специального приложения для смартфона КриптоПро myDSS — продукта партнерского взаимодействия компаний SafeTech и КриптоПро.

КРИПТОПРО myDSS. КВАЛИФИЦИРОВАННАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ ПРИ ПОМОЩИ СМАРТФОНА

Мобильное приложение КриптоПро myDSS позволяет пользователю при помощи буквально двух «тапов» по экрану смартфона подтверждать операции подписи любых электронных транзакций, вырабатывая код подтверждения транзакции, который зависит от

четырех составляющих: времени, содержания подписываемого документа, уникальных признаков смартфона, а также уникального ключа, который хранится в смартфоне пользователя в защищенной области. Эта схема существенно более безопасна, чем использование одноразовых или многоразовых паролей, так как обеспечивает неизменность электронного документа в процессе передачи на сервер подписи, кроме того, в ней не используется недоверенный SMS-канал.

Совсем недавно, 14 февраля 2018 года, комплекс «облачной подписи» КриптоПро DSS с модулем аутентификации myDSS получил положительное заключение Федеральной службы безопасности Российской Федерации, в ближайшее время ожидается получение сертификата на данное решение.

Итак, использование комплексного решения КриптоПро DSS с модулем аутентификации myDSS позволит просто и удобно подтверждать любые документы и операции квалифицированной электронной подписью при помощи смартфона, получая доступ к электронному документообороту и государственным услугам, а также в системы дистанционного банкинга в любом месте и в любое время, совершенно не проигрывая в удобстве.



КриптоПро myDSS



Квалифицированная электронная подпись в системах электронного документооборота при помощи смартфона.

Мобильное приложение myDSS является частью решения КриптоПро DSS и позволяет обеспечить строгую аутентификацию пользователя и контроль подписываемых документов.

myDSS проще, дешевле и удобнее, чем токены, смарт-карты или программные криптопровайдеры.

Что такое myDSS

КриптоПро myDSS – это приложение для смартфона, которое позволяет подписывать квалифицированной электронной подписью документы и контролировать действия пользователя в системах дистанционного банкинга, порталах госуслуг, системах ЭДО, электронных торговых площадках и т.д.

В основе myDSS лежит технология PayControl, которая обеспечивает строгую криптографическую аутентификацию пользователей, безопасное online-взаимодействие, отображение документа и подтверждение операций. Это позволяет сервису облачной электронной подписи КриптоПро DSS выполнить требования, предъявляемые регулятором к средствам электронной подписи.

Безопасность

Приложение myDSS выполняет визуализацию электронного документа и формирование подтверждения на его подписание в КриптоПро DSS.

Криптографическая аутентификация и защищенный обмен между приложением и сервером КриптоПро DSS гарантируют, что только легальный пользователь сможет воспользоваться ключами подписи.

Ключи электронной подписи пользователей хранятся в сертифицированном КриптоПро HSM в неизвлекаемом виде.

Юридическая значимость подписи

Документ и другие действия пользователя заверяются квалифицированной электронной подписью, что обеспечивает неотказуемость действий. Пользователь не только подтверждает содержание документа, но и в дальнейшем не имеет возможности отказаться от совершенного действия.

КриптоПро myDSS

Совместная разработка компаний КриптоПро и SafeTech на базе сертифицированного программно-аппаратного средства криптографической защиты информации КриптоПро HSM, КриптоПро DSS и системы подтверждения электронных транзакций PayControl.



Александр МАХНОВСКИЙ
руководитель Департамента
разработки компании «Аванпост»

ТОП-5 ВЫЗОВОВ ДЛЯ СИСТЕМЫ IGA

Автоматизация процессов управления доступом и жизненным циклом учетных записей, которую обеспечивают классические IDM-системы, приносит большую пользу организации: устраняет задержки между кадровыми событиями и их адекватным отражением в настройках доступа инфраструктурного и прикладного ПО, позволяет проводить аудиты ИБ, разгружает ИБ-персонал от рутинной работы, делает невозможными многие виды компьютерных преступлений.

Это особенно важно в период быстрых изменений бизнес-среды и ИТ-ландшафта, связанных с импортозамещением ИТ, предстоящей цифровизацией всех сторон нашей жизни, растущими потребностями предприятий в переходе на более совершенные системы менеджмента, появлением новых классов перспективных ИТ-систем (роботизация процессов, Big Data и др.). Именно поэтому в России популярность IDM-решений быстро растет, а стратегически мыслящие организации изначально встраивают IDM в картину будущего состояния своих информационных систем (ИС) в качестве обязательного элемента.

Однако все эти изменения имеют общий побочный эффект, создавая новые риски и уязвимости, которые не могут быть закрыты средствами классических IDM-систем. Справиться с новыми рисками и уязвимостями позволяет новое поколение IDM — системы класса IGA.

Сохраняя все ценности автоматизации для ИТ-подразделений и бизнеса, они предоставляют дополнительную бизнес-ценность для подразделений, отвечающих за информационную безопасность предприятия.

В этой статье мы рассмотрим наиболее опасные риски и уязвимости, которые позволяют устранить именно IGA-решения, но не классические системы IDM.

«МЕРТВЫЕ ДУШИ»

Чем больше учетных записей (УЗ) в ИС, тем выше риск компрометации каких-либо из них и использования в компьютерных преступлениях. Причем наибольший интерес для злоумышленника представляют учетные записи уволенных сотрудников и работников, ушедших в долгосрочный отпуск. Ведь активность такой учетной записи почти наверняка не будет замечена её владельцем. А поскольку пароли таких аккаунтов долгое время не меняются, то однажды получив такой пароль, можно долго пользоваться им и даже менять его, не опасаясь реакции пользователя.

Это один из главных рисков, который классические IDM-решения успешно закрывают за счёт управления жизненным циклом УЗ на основании данных, поступающих из кадровой системы. Например, при увольнении пользователя его учетная запись будет автоматически заблокирована или удалена, а в будущем ее состояние будет контролироваться.

IGA-решения идут значительно дальше: отслеживая активность учетной записи (с помощью прямой интеграции, интеграции с решениями класса Web SSO или через SIEM), они выявляют неиспользуемые учетные записи действующих работников, обладающие схожими рисками, и позволяют — автоматически или с привлечением ответственных лиц — принять решение об изменении состояния каждой такой УЗ. Иными словами, они проактивно работают с группами риска, которые динамически возникают, меняются и исчезают в ходе работы предприятия.

ПРЕВЫШЕНИЕ ПОЛНОМОЧИЙ

Полномочия пользователей в ИС должны строго соответствовать их должностным обязанностям. Это очевидно, но выполняется крайне редко, что создаёт риски утечки информации, нарушение процессов и функционирования системы (по злому умыслу или по неосторожности пользователя). Есть и другие нежелательные последствия, хотя и менее значимые.

Корректная ролевая модель, которую предлагают IDM-решения, во многом снимает эту проблему, однако IGA-системы предлагают целый ряд дополнительных инструментов, как использующих ролевые модели, так и не связанные с ними.

Так, значительно сокращают рассматриваемые риски процессы аттестации и сертификации прав доступа пользователей и ролевой модели. Их цель —

поддерживать актуальные наборы прав в точном соответствии с меняющимися бизнес-процессами и ИТ-ландшафтом организации.

Сертификация «легитимизирует» доступ, полученный до внедрения IDM, либо в обход неё. В процесс вовлечены ответственные лица, подтверждающие или отвергающие необходимость и правомерность наличия таких прав у пользователя. Права, прошедшие сертификацию, в будущем считаются разрешенными для их владельца. Но значительная часть полномочий, исторически накопленных пользователем, отсекается на этапах рассмотрения и автоматически отзывается у пользователя, что позволяет в автоматизированном режиме навести порядок уже при внедрении IGA. Ценность данного процесса ещё возрастает благодаря тому, что для его запуска не требуется дорогостоящий этап анализа и построения ролевой модели. Более того, наиболее продвинутые IGA-решения могут обучаться в процессе сертификации и затем, на основе собранных данных, предлагать элементы для добавления в ролевую модель.

Аттестация предполагает плановый пересмотр доступов пользователя ответственными лицами по гибкому расписанию, зависящему от разных факторов. Так, повышение частоты аттестации может использоваться как эффективная компенсационная мера для пользователей, обладающих привилегированными или конфликтными полномочиями, либо попавших под внимание офицеров ИБ или системы по какой-то другой причине.

Кроме этого, в IGA решениях классический механизм аудита прав доступа, как правило, дополняется набором политик. Они, в частности, позволяют либо автоматически устранить превышающие полномочия пользователя в ИС, либо организовать бизнес-процесс оценки их обоснованности, в котором участвуют специалисты в ИБ и представители бизнеса, что практически нивелирует риск.

НЕСОВМЕСТИМЫЕ ПОЛНОМОЧИЯ

Сегодня одним из основных рисков становится нарушение принципа разде-

НАИБОЛЕЕ ПРОДВИНУТЫЕ IGA-РЕШЕНИЯ МОГУТ ОБУЧАТЬСЯ В ПРОЦЕССЕ СЕРТИФИКАЦИИ И ЗАТЕМ, НА ОСНОВЕ СОБРАННЫХ ДАННЫХ, ПРЕДЛАГАТЬ ЭЛЕМЕНТЫ ДЛЯ ДОБАВЛЕНИЯ В РОЛЕВУЮ МОДЕЛЬ

ления ответственности (SoD), т.е. запретов на совмещение определенных ролей/прав у одного человека. В финансовой сфере хорошо знакомы с этим риском: здесь невнимание к нему позволяет злоумышленнику, например, единолично выполнить финансовую операцию. Однако данному риску подвержены любые ИС, управляющие сколько-нибудь значимыми для бизнеса активами.

Без специальных инструментов своевременно выявлять и предотвращать такие конфликты полномочий (на фоне меняющейся системы запретов совмещения и часто меняющихся прав пользователей) в большой организации крайне затруднительно. И если на уровне отдельных ИС (например, в автоматизированных банковских системах) вопрос достаточно часто решается средствами самой ИС, то межсистемные SoD-конфликты контролировать без IGA практически невозможно. Причем, современный подход к разработке корпоративных информационных систем (включая SOA, микросервисную архитектуру и другие тенденции) делает практически незаменимым внешнее по отношению к прикладным ИС средство контроля и управления полномочиями пользователей.

Механизм контроля SoD-конфликтов, являющийся обязательным атрибутом решений класса IGA, позволяет создать модель, определяющую отношения между множествами полномочий. Такая модель позволяет выявить несовместимые полномочия у работников, разрешить конфликты и предотвратить их появление в будущем, либо определить строгие компенсационные меры для такого лица. Причем всё это можно сделать как для отдельных ИС, так и для групп взаимосвязан-

ных ИС — вплоть до масштабов всей корпоративной информационной системы территориально распределенной организации.

Наиболее продвинутые реализации механизма предотвращения SoD-конфликтов позволяют не только проанализировать уже имеющийся у пользователя набор доступов, но и в режиме реального времени проверить запрашиваемый пользователем доступ и, при выявлении конфликтов, предложить самому пользователю варианты решения. Среди них могут быть: временный или постоянный отказ от какого-либо из запрашиваемых или имеющихся доступов, что устраняет конфликт; дополнительное согласование запроса представителями ИБ или другими должностными лицами, в компетенции которых находится принятие решения о допущении риска; другие меры по компенсации риска, которые либо накладывают ограничения на пользователя, либо создают предписание соответствующим должностным лицам.

Кроме того, IGA-решения, как правило, предлагают гибкие политики, позволяющие автоматически устранить превышающее полномочие пользователя в ИС, уведомить ответственных, либо организовать бизнес-процесс по их рассмотрению с оперативным привлечением как специалистов ИБ, так и бизнеса.

КОМПРОМЕТАЦИЯ ПРИВИЛЕГИРОВАННЫХ УЗ

Особого внимания требуют учетные записи администраторов (как системных, так и прикладных), а также пользователей, суммарный набор полномочий которых позволяет выполнить действия, чувствительные для бизнеса организации. В крупной организа-

ции таких аккаунтов может быть очень много. Для их выявления IGA-системы предлагают модель, основанную на оценке рисков. Эта сложная гибко настраиваемая математическая модель позволяет выявить и ранжировать потенциально опасных пользователей, которые имеют техническую возможность нанести ощутимый вред своей организации (по злому умыслу или в результате компрометации их аккаунтов). А упомянутые ранее процессы сертификации и аттестации, совместно с гибкими политиками управления паролями, позволяют определить компенсационные меры, достаточные для значительного снижения данных рисков.

НЕОСВЕДОМЛЕННОСТЬ БИЗНЕСА

Нередко в организациях, особенно с невысокой культурой ИБ, руководители бизнеса, на который ориентирована ролевая модель, и их подчиненные относятся к процессу управления доступом «спустя рукава». В такой ситуации главная задача ответственных от бизнеса сводится к обеспечению «невмешательства» и устранения препятствий «нормальной работе», которые, по их мнению, только и создают подразделения ИБ. А это приводит не только к избыточности прав, но и к отсутствию естественного процесса актуализации ролевой модели. При этом бизнес-подразделения не понимают и не учитывают свои риски, возникающие благодаря их поведению. В свою очередь, офицеры ИБ, не будучи непосредственными участниками основных бизнес-процессов организации, в принципе не могут представить себе полную картину рисков. Именно поэтому просто необходимо вовлечение бизнеса в процессы ИБ и, в первую очередь, в процесс

управления доступом. Но как это сделать?

IGA-системы существенно помогают не только вовлечь бизнес в процесс управления доступом, но и сделать его ответственным за значительную часть принимаемых решений. Этому способствуют упомянутые ранее процессы аттестации и сертификации, а также возможность самостоятельного формирования бизнес-ролей и наборов доступов проектных команд, которую предлагают большинство решений. Использование этих инструментов существенно повышает культуру ИБ в компании, а необходимость ставить свою визу на правах доступа своих работников вынуждает руководителя любого уровня задуматься над их необходимостью, что благотворно влияет на весь процесс поддержания актуальности ролевых моделей.

ПОДВЕДЕМ ИТОГ

Системы класса IGA существенно расширяют возможности IDM-решений, причем в тех направлениях, которые отвечают уже произошедшим или только намечающимся, но практически неизбежным изменениям в работе российских организаций практически любого масштаба. Причем это одинаково относится как к коммерческим структурам, так и к системе госуправления, госкорпорациям, силовым ведомствам. Что же делать заказчику, задумавшему внедрение IDM, в этих условиях?

Решая этот действительно непростой вопрос, стоит учесть несколько обстоятельств.

Во-первых, значимость вышеперечисленных и ряда не включенных в данную статью возможностей IGA-систем, лежащих за пределами классических IDM-решений, будет только возрастать, поскольку отсутствие IGA-

функций, когда они стали нужны организации, означает для неё невозможность их качественной автоматизации и, как следствие, возврат ко всем хорошо знакомым недостаткам управления доступом вручную.

Во-вторых, трансформация IDM в IGA требует коренной переработки всей системы: изменения модели предметной области; реализации алгоритмов IGA, опирающихся сразу на несколько функций IDM и дополняющих их сложной логикой взаимодействия; изменения архитектуры ядра системы, чтобы получить возможность эффективно реализовывать такие «трансграничные» межсервисные алгоритмы; наличия гибкой системы workflow, с помощью которой можно реализовать и поддерживать все необходимые процессы (о некоторых из них мы говорили в данной статье). С этой задачей справятся не все поставщики IDM-систем.

В-третьих, выбрав сегодня IDM-систему, которая не сможет своевременно трансформироваться в IGA-решение, заказчик столкнется с необходимостью или примириться с растущим набором практически неустраняемых проблем, либо мигрировать на другое решение. Для интенсивно работающей и развивающейся организации оба варианта мучительны и, пожалуй, неприемлемы.

Таким образом, даже если заказчик видит ценность для себя IGA-функций лишь в отдаленной перспективе, разумнее сразу выбрать IDM-систему, где уже реализован базовый набор IGA-функций (например, предотвращение SoD-конфликтов), где уже есть необходимая технологическая основа для создания комплексных процессов, а разработчик сделал их реализацию основой своей стратегии.

Именно такой предусмотрительный подход гарантирует, что организация всегда будет готова встретить любые изменения, не снижая, а повышая степень автоматизации процесса управления правами доступа.

**IGA-СИСТЕМЫ СУЩЕСТВЕННО
ПОМОГАЮТ НЕ ТОЛЬКО ВОВЛЕЧЬ
БИЗНЕС В ПРОЦЕСС УПРАВЛЕНИЯ
ДОСТУПОМ, НО И СДЕЛАТЬ ЕГО
ОТВЕТСТВЕННЫМ ЗА ЗНАЧИТЕЛЬНУЮ
ЧАСТЬ ПРИНИМАЕМЫХ РЕШЕНИЙ**



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

VII ФОРУМ АЗИ

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Поскольку институт государства с некоторых пор пребывает в состоянии поиска своего места и роли в жизни общества, то организацией обмена опытом в сфере кибербезопасности занимаются общественные организации, одна из которых — Ассоциация защиты информации (АЗИ), образованная в 2002 году по инициативе ФАПСИ и Гостехкомиссии РФ.

Внимание участников VII Форума АЗИ было сосредоточено на нескольких актуальных темах, которые в ближайшей перспективе могут стать причиной новых забот «ибэшников». Ну и какой же «обмен премудростями» без итогов и умеренной похвалы?

Если структурировать проблематику мероприятия не организационно («планка» и секции), а тематически, то можно выделить такие темы:

- ♦ Цифровая экономика «вообще» и частности этой экономики в лице технологии блокчейн и создания т.н. криптовалют (майнинг, говоря по-иноземному).
- ♦ Квантовая криптография и технологии Больших Данных (Big Data) для обеспечения информационной безопасности.
- ♦ Практика обеспечения безопасности КИИ, в т.ч. с учётом требований федерального законодательства.
- ♦ Проблемы подготовки кадров и повышения квалификации в сфере ИБ.
- ♦ Итоги 2017 года и тенденции развития рынка ИБ в России.

ИБ 2017: СТАБИЛЬНОСТЬ И ИННОВАЦИИ

Подведение итогов 2017 года в формате АЗИ показало, что информационная безопасность имеет свою стабильную «десятину» в бюджетах регионов и ведомств. Удельный вес расходов на ИБ может в единичных случаях достигать до 40–50% (и в регионах и в ведомствах), но, как правило, он находится в преде-

лах 10+%. При этом сопоставление абсолютных величин расходов на ИБ по годам показывает, что в последние несколько лет даже в кризис на безопасности не экономят, что не может не радовать. Правда и при таком подходе ибэшники не жируют.

Определённая стабильность рынка ИБ благотворно сказывается на развитии отечественного инструментария ИБ. Например, компания «Код безопасности» представила на суд межсетевые экраны «Континент», которые существенно (в разы) превосходят по базовым характеристикам неназванных конкурента 1 и конкурента 2. Сама за себя говорит информация на слайде компании «Информзащита», озаглавленном «Технологический потенциал» (рис. 1).

Если перейти к будущему технологий ИБ, то в части перспектив практического использования квантовой криптографии представитель компании «ИнфоТеКС» в своем выступле-

нии был академически оптимистичен и осторожен (цитата со слайда): «Современный уровень развития науки и технологии квантового распределения ключей (КРК) позволяет переходить к коммерциализации и практическому внедрению при условии, что обеспечиваются доказуемая стойкость квантового протокола; аппаратные методы генерации случайных чисел; доказуемая стойкость квантового ключа; защиты от атак на реализацию».

При этом ещё в одном докладе — «Развитие цифровой экономики. Новые угрозы информационной безопасности» — было упомянуто, что только в 2016 году удалось соотнести уровни безопасности в квантовой и классической криптографии, а большинство нынешних квантовых криптографических систем крайне уязвимы к атакам в силу несовершенства элементной базы.

Исходя из информации, представленной компанией «ИнфоТеКС», «на низком старте» в части коммерциали-

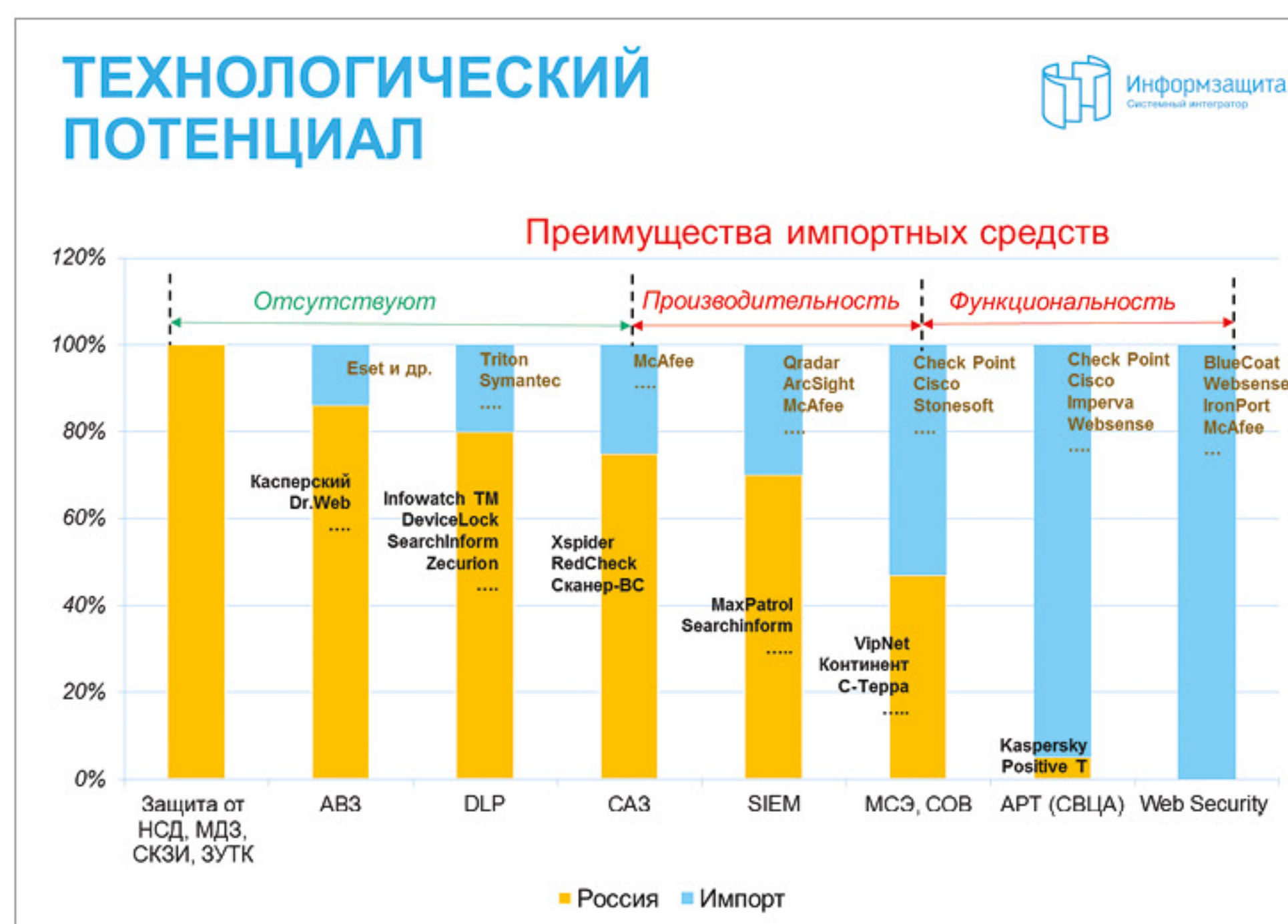


Рисунок 1. Технологический потенциал (из презентации вице-президента НИП «Информзащита» О.В. Чутова)

зации и практического внедрения квантовой «крипты» стоят США и Китай: есть оборудование (номинально китайское обладает лучшими характеристиками, опережая не только США, но и Швейцарию и Францию), есть проекты «квантовых» сетей (тут Япония и Европа «дышат в спину» США и Китаю). Россия формально представлена «лабораторными установками». Однако в нашей стране появляются «драфты» нормативной документации; компанией «Гроссмейстер» создан генератор случайных чисел, использующий свойства случайного физического процесса. Новинка может использоваться в средствах криптографической защиты информации в качестве источника случайных двоичных последовательностей. Напомним также, что на февральском Инфофоруме 2018 ГУ развития информационных и телекоммуникационных технологий МО РФ уверенно доложило о готовности к появлению квантовых компьютеров и квантовой криптографии.

Так что в целом Россия «держит руку на пульсе» квантовой криптографии, головокращения от успехов нет, но есть понимание проблем и необходимости и путей их решения.

ТОРОПИТЬСЯ НЕ НАДО. МЫ ДОЛЖНЫ ПРЕДЛОЖИТЬ ОБЩЕСТВУ ПОЛНОЦЕННУЮ ЭКОНОМИКУ

Столь же трезвый, как и на квантовую криптографию, взгляд на цифровую экономику «вообще» с частностями этой экономики в виде блокчейнов представил уже упомянутый доклад «Развитие цифровой экономики. Новые угрозы информационной безопасности». Общий настрой профессионалов в отличие от чиновников: поспешать не торопясь.

И это не боязнь нового, а трезвая оценка уже набитых мировым сообществом шишек. Информация об этих шишках хорошо известна, в их числе: уязвимости криптовалют на уровне валидации транзакций, на сетевом уровне (DDoS-атаки, атаки Sybil и Eclipse), при генерации и хранении ключей, при авторизации пользователя (напрямую или через посредников).

Было отмечено, что, например, в сеть майнеров биткоинов напрямую под-

МЕРОПРИЯТИЕ В ОЧЕРЕДНОЙ РАЗ ПРОДЕМОНСТРИРОВАЛО, ЧТО ОТРАСЛЬ ИБ В НАШЕЙ СТРАНЕ — ОДНА ИЗ НЕМНОГИХ (ЕЩЁ ОДИН ПРИМЕР — КОСМОНАВТИКА), ИМЕЮЩИХ СВОЁ ЛИЦО НА МИРОВОМ РЫНКЕ РАЗДЕЛЕНИЯ ТРУДА

ключается лишь около 11500 пользователей, остальные 99,9% используют посредников, которые никем не уполномочены, не сертифицированы и не имеют отношения к создателям криптовалюты. Контроль над аккаунтом может быть перехвачен как при регистрации, так и в процессе использования, в т.ч. самими посредниками.

Недобросовестность работы в блокчейне возможна на основе существенной разницы в мощности вычислительных ресурсов участников сети. При этом, как отмечалось в докладе, на февраль 2018 года более 65% физических ресурсов находилось в Китае, около 55% всех мощностей — под контролем трех крупнейших пулов, около 90% мощностей — под контролем 7 пулов.

ЗАКОН ЕСТЬ ЗАКОН: ПОМНИ О ФЗ-187 И GDPR

В части традиционного внимания ибэшников к «нормативке», Елена Торбенко, заместитель начальника управления ФСТЭК России, продолжила свою подвижническую деятельность по разъяснению массам особенностей внедрения Федерального закона от 26 июля 2017 г. № 187 «О безопасности критической информационной инфраструктуры Российской Федерации», который с 1 января 2018 года добавил новые оттенки в симфоническое звучание кибербезопасности в нашей стране.

На форуме также был проведен мастер-класс на тему «Мониторинг и анализ медиaprостранства с целью выявления предпосылок к различного рода негативным проявлениям». Тема выглядит несколько «перпендикулярной» по отношению к вопросам защиты информации при её [информации] появлении в киберпространстве. Скорее

это из области дополнительных возможностей контроля благонадежности сотрудников благодаря ИТ. При этом сразу возникает вопрос о наличии точных критериев благонадежности, если посмотреть на эту проблему со стороны социальных медиа. Право, «выявление более 20 подтверждений взаимного общения между сотрудниками различных банков» вряд ли может считаться таким критерием. Сразу вспоминается реклама 90-х: «Кормить надо лучше, они и не улетят!».

В то же время и мастер-класс и упоминание об использовании машинного обучения для построения политик безопасности — это все примеры того, как тема Больших Данных была затронута на форуме.

На фоне растущего осознания необходимости отказа от понятия экономической эффективности в сфере ИБ в пользу понятия безусловной безопасности неким диссонансом отдают идеи информационной безопасности как сервиса, которые, тем не менее, также нашли своё отражение в повестке дня VII Форума АЗИ.

В целом мероприятие в очередной раз продемонстрировало, что отрасль ИБ в нашей стране — одна из немногих (ещё один пример — космонавтика), имеющих своё лицо на мировом рынке разделения труда. И, возможно, в связи с этим простые русские слова «конференция», «совещание», «семинар» смогут в ближайшем будущем разбавить бесконечную череду фонетически безликих «форумов», добавив гуманитарную изюминку в их оригинальную технологическую канву.



POSITIVE HACK DAYS 2018

КАЛОРИЙНОЕ МЕРОПРИЯТИЕ ОБ ИЗНАНКЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Хакерская группировка «нагрела» примерно сотню финансовых организаций по всему миру на более чем 1 млрд евро. Около 800 DDoS-атак на ресурсы «Ростелекома» и клиентов компании регистрируется ежедневно. Около половины компаний в мире подверглись в 2017 году целенаправленным кибератакам. Эти и другие цифры и факты настораживают, но не новы. И не они стали изюминками Международного форума Positive Hack Days 2018, проходившего в ЦМТ на Красной Пресне.

Лишь 5 % компаний, заказывавших когда-либо Positive Technologies — организатору PHDays 2018 — пентестинг своей ИТ-инфраструктуры, замечают сам факт попыток вторжения.

Но ещё ни разу специалистам Positive Technologies не пришлось потерпеть фиаско в этой области. «Нужно сделать три простые вещи: везде установить антивирусы, устранить критически опасные уязвимости хотя бы на внешнем периметре и — поскольку с большой долей вероятности вы уже взломаны — нужно целенаправленно искать следы взлома», — утверждает Борис Симис, заместитель генерального директора компании.

Эта информация уже более эксклюзивна, но и она не шокирует. «Если дела идут плохо, в ближайшем будущем они пойдут ещё хуже». «Если ситуация улучшается, значит, вы чего-то не заметили». Эти так называемые законы Мерфи были выведены задолго до появления термина «кибербезопасность», но труд-

но придумать что-то более актуальное для нынешней эпохи цифровой трансформации.

ИЗЮМ ПОШЕЛ

Настоящей же изюминкой PHDays 2018 стала синергия прикладной безопасности и дискуссий на концептуальные темы. Именно так сформулировал главное о форуме Александр Бондаренко, генеральный директор компании R-Vision. На площадке форума срежиссировали действие, названное «Цифровая изнанка». Пространство было организовано так, что входящий оказывался во вместительном холле для личного общения в режиме peer-to-peer, а естественный путь дальше выводил его на площадку, где бились команды «хакеров» и «безопасников». Ну а для

академичных пленарных заседаний и мастер-классов были отведены многочисленные залы ЦМТ.

Масштабное хакерское соревнование позволило наяву ощутить атмосферу угроз, витающих над «цифровой экономикой». Панорама напоминала армейский штаб во время боевых учений. За тем лишь исключением, что макет поля боя представлял собой кибермодель цифровой инфраструктуры хозяйственного субъекта: АСУ ТП промышленных объектов, фрагменты автоматизированной транспортной инфраструктуры, «умные» дома, банки, поддерживающие услуги удалённого банкинга, сеть сотовой связи, оплётённая онлайн-сервисами.

Тут вживую проводился перехват трафика в каналах смоделированного сотового оператора, взлом банкоматов, манипуляции с «умными» счётчиками электроэнергии, DDoS-атаки на камеры наблюдения «умного» города, взлом SCADA-систем промышленных предприятий. Все эти невинные кибершалости осуществлялись что называется «с колёс». Нетрудно экстраполировать, сколько дров способны наломать в цифровой «лавке» атакующие, обладающие значительно большими ресурсами, когда ставки измеряются не в «публях» — специальной валюте PHDays 2018, а в реальных рублях, долларах и евро.

«...новые технологии сулят людям качественное улучшение жизни. Но пока весь мир охвачен идеей цифровой трансформации, хакеры решают: кто станет жертвой этого процесса, а кто получит от него выгоду...». (© Positive Technologies).

«Уми, Денис, лучше не напишешь!» (© Григорий Потёмкин).

Но было бы несправедливым утверждать, что единственной целью PHDays 2018 было запугивание.

НЕ СТРАХОМ ЕДИНЫМ

На мастер-классах участники осваивали приёмы защиты корпоративных сетей от вредоносных программ, настраивали SELinux, строили threat-hunting-инфраструктуру для поиска и расследования сложных современных атак.

А на пленарных заседаниях и в ходе панельных дискуссий обсуждалась ситуация с безопасностью нынешней

предтечи «цифровой экономики», которую иначе как аховой назвать трудно. Шоры сиюминутных интересов бизнеса чаще, чем хотелось бы, затмевают риски киберугроз. Даже в материальном производстве. И это в условиях, когда всё большее число кибератак носит деструктивный характер и имеет целью уничтожить цифровую инфраструктуру, а наши англосаксонские партнёры, чуть что не по ним, начинают размахивать жупелом кибервойны. Но как показал PHDays 2018, некоторым отечественным бизнесменам, получившим при делёжке хозяйства СССР оборудованием массой в сотни тонн и температурами рабочих процессов в тысячи градусов, важнее выявлять мошенничество партнёров, а кибербезопасность отдать на аутсорсинг. Запредельная раскрутка ядерных центрифуг Ирана их ничему, похоже, не научила.

Но в целом ещё одной приятной изюминкой форума стало, если не превалирование, то, по крайней мере, необычно громкое звучание трезвых оценок ситуации, не принимающих такой аргументации, как «прогресс не остановить», «за рубежом тоже всё плохо с кибербезопасностью», «мы не успеем вскочить в уходящий поезд».

Уже сегодня в результате анархического внедрения «цифры» под небезопасным прессом оказались мелкообразные Акакии Акакиевичи, справившие себе смартфоны и получившие доступ в магазины мобильных приложений. Эти неопиты сразу же теряют, как минимум, самое дорогое, что у них осталось после покупки смартфона — персональные данные. Получая взамен потоки рекламы.

На «пленарке» с названием в стиле Сидни Люмета и Геннадия Хазанова «Шесть разгневанных заказчиков, или чего не хватает российской ИТ-индустрии» как бы вскользь было упомянуто, что «самый незащищённый в современном цифровом мире — простой человек». Именно так был сформулирован тезис Александра Баранова (ГНИВЦ ФНС), который сразу же сорвал бурные аплодисменты, что означает попадание в «десятку». Народ знает ситуацию не понаслышке! И в качестве теста на зрелость цифрового общества Александр Павлович предложил разра-

ботать для начала хотя бы удобную и защищённую систему управления паролем для народа.

Уместно заметить, что не в лучшем положении и та пара-тройка миллиардов жителей планеты Земля, что запланирована в «золотой» миллиард и на его службу. Именно они в первую очередь должны будут, по идее, по полной упаковаться цифровыми «приблудами» с искусственным смарт-интеллектом. По прогнозу Gartner к 2020 году под каток хакерских атак будут брошены 250 млн автомобилей, подключённых к Интернету. А беззащитность такой техники мы уже наблюдали на упомянутом хакерском соревновании.

ВМЕСТО ЭПИЛОГА

И ещё об одной изюминке PHDays 2018: демонстрация наличия в нашей стране достаточного числа потенциальных технократов. Тех, кто на деле, а не в связи с искусственно прилепленным СМИ ярлыком, являются Инженерами и могут стать лидерами «объединённой» отрасли ИТ&ИБ в правительстве России.

И не обязательно технократом молодым. Цифровые дела в ближайшие шесть лет могли бы возглавлять люди с опытом руководства такими компаниями и организациями, как Positive Technologies, Лаборатория Касперского, InfoWatch, Информзащита, ГНИВЦ ФНС и другими подобными. Для них ИТ и ИБ синергетически едины, а внедрение ИТ рассматривается ими как средство, а не как цель.

* * *

С точки зрения единого образа форум Positive Hack Days 2018 оказался полновесной калорийной булочкой, буквально напичканной изюмом. Место проведения — уютный и удобный ЦМТ; организаторы — компетентная компания, к тому же с хорошим вкусом в том, что называется внешними коммуникациями; увлечённые, компетентные и доброжелательные партнёры и гости Форума; хорошая майская погода! Что ещё надо, чтобы на два дня погрузиться в атмосферу Знаний на технических сессиях, Мнений на круглых столах и Виртуальных битв в киберпространстве «умных» городов.

«Current Trends in Cryptology» has proved a place where everyone can take a look at results of the researches conducted by foreign specialists and, moreover, ask them questions. Lightweight cryptography – one of the most of modern cryptography – is the subject to be delivered by Thomas Peyrin. Phillip the «provable security» founders, will speak on encryption, another equally discussed issue. Shayev's disciple Oleg Kozlitsin, invited speaker of Cryptography of the Russian Federation – organizers of the Workshop – will share his research on mathematical problems in cryptography.



СТCRYPT 2018

VII СИМПОЗИУМ «СОВРЕМЕННЫЕ ТЕНДЕНЦИИ
В КРИПТОГРАФИИ» ЗАФИКСИРОВАЛ ПЕРЕХОДНЫЙ
ПЕРИОД В ИСТОРИИ ОТЕЧЕСТВЕННОЙ
КРИПТОГРАФИИ

В Суздале в конце мая состоялся VII симпозиум «Современные тенденции в криптографии» (СТCrypt'18), участие в котором приняли более 100 исследователей в области криптографии из 9 стран мира, включая Вьетнам, Сингапур, США, Финляндию. Организаторами симпозиума выступили Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), Академия криптографии Российской Федерации и Математический институт им. В.А. Стеклова РАН.

Симпозиум STCrypt проводится в сотрудничестве с Международной ассоциацией криптологических исследований (IACR) и при поддержке Фонда содействия развитию безопасных информационных технологий (ФСРБИТ). Организационную поддержку мероприятию оказала Медиа Группа «Авангард».

STCrypt 2018 стал главным международным научным событием в России, посвященным теоретическим и практическим аспектам криптографии в современном мире. С приглашенными докладами выступили крупные ученые, сделавшие значительный вклад в разработку международных криптографических стандартов — в их числе профессор Калифорнийского университета в Дэвисе (США) Филлип Рогауэй, адъюнкт-профессор Наньянского технологического университета (Сингапур) Томас Пейрин. Кроме того, были проведены телемосты с зарубежными исследователями — Филиппом Джовановичем (Швейцария) и коллективом исследователей из Ирана.

В программе симпозиума прозвучали около тридцати докладов, представивших результаты российских и зарубежных исследований в области криптографии. На тематическом заседании были рассмотрены перспективные разработки с применением технологии блокчейн. В связи с планами развития цифровой экономики Российской Федерации участники обсудили на круглом столе перспективы и препятствия на пути распространения программных продуктов и сервисов на базе отечественной криптографии среди широких слоев пользователей.

Модератором круглого стола «Криптография и цифровая экономика»,



Президент Академии криптографии РФ Александр Шойтов



Профессор Калифорнийского университета в Дэвисе (США) Филлип Рогауэй

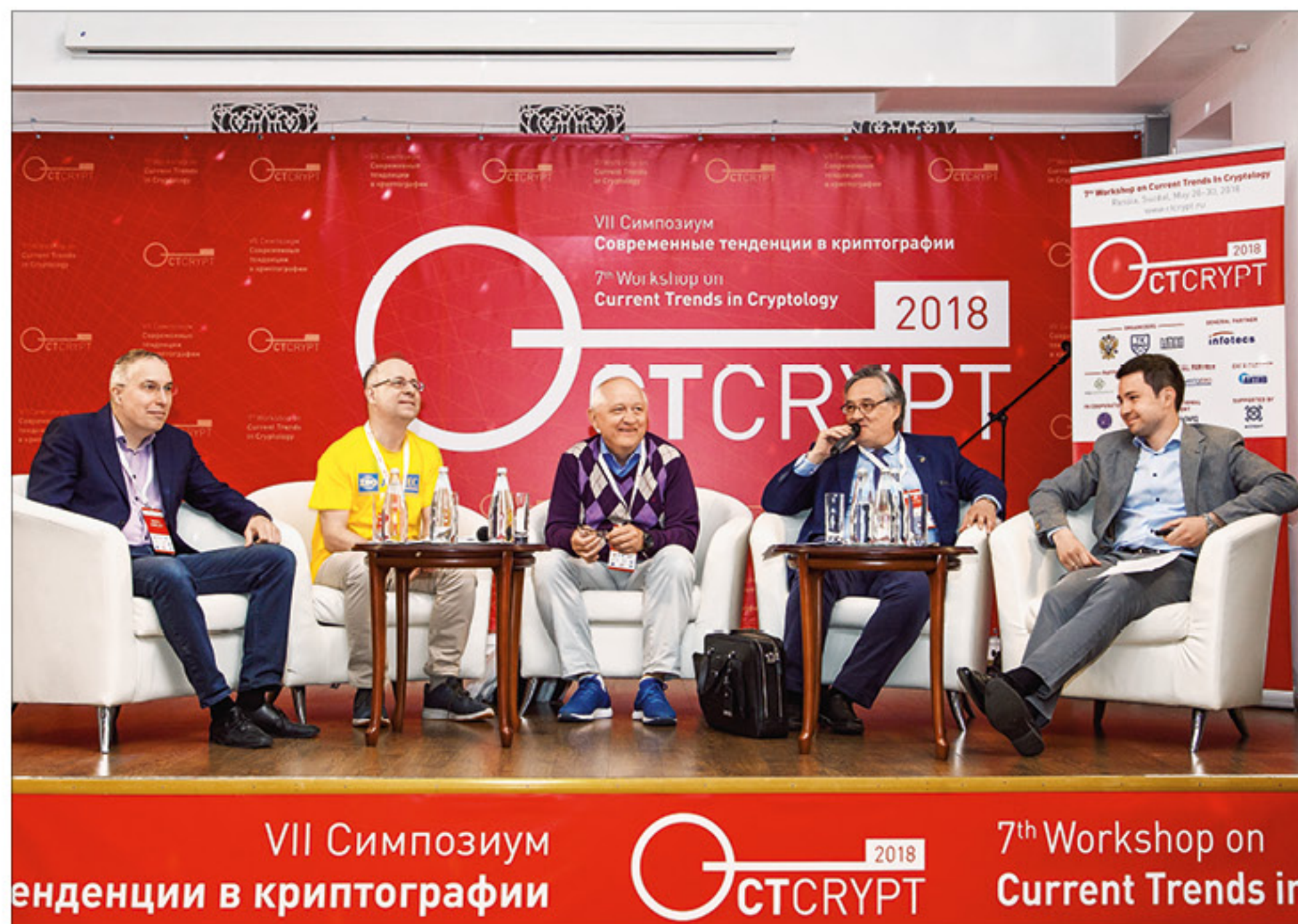


Председатель ТК 26 Игорь Качалин

в котором активно участвовали представители ТК 26, выступил генеральный директор компании «ИнфоТеКС» Андрей Чапчаев. Один из выводов дискуссии он сформулировал следующим образом: «С точки зрения научной базы, стандартов и технологических заделов у нас есть если не все, то многое для массового внедрения отечественной криптографии. При наличии поэтапного плана можно поступательно наращивать процент ее использования, и тут программа «Цифровая экономика РФ» является серьезным подспорьем. Самый большой вопрос — это мотивация потребителей сделать такой переход,

что весьма проблематично, поскольку удобство пользования СКЗИ пока не в нашу пользу. И тут большую роль играют разрешительно-регуляторные моменты, которые пока еще не очень помогают на этом пути».

Заместитель председателя Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) Дмитрий Матюхин зафиксировал текущую ситуацию как поворотную в истории криптографии: «Сегодня мы все являемся участниками перехода от «криптографии как защиты государственных интересов» к «криптографии везде», вплоть, как го-



Круглый стол «Криптография и цифровая экономика»

ворится, до утюгов. Процесс цифровизации общества, как и любой процесс обновления, — во многом болезненный и не во всем понятный, поэтому государству не так просто определить, какое место в нем занимает, какую роль играет тот или иной институт, в данном случае — криптография. На мой взгляд, государство должно взять на себя ответственность за совершение юридически значимых действий, и именно исходя из этого оно должно внедрять отечественную криптографию, причем, не только алгоритмы, но и СКЗИ. Другого пути для регулирования этого процесса нет. Иначе мы в массовом порядке столкнемся с ситуацией, как в прошлом году, когда через смарт-контракт «Эфириум» за один раз утекло 23 млн долларов, и никто за это не взял на себя ответственность».

DLTREG 2018. БЛОКЧЕЙН В РОССИИ

Ассоциация ФинТех и Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) провели в конце мая международную конференцию по регулированию распределённых реестров DLTReg 2018. Конференция проходила в Высшей школе экономики и включала в себя четыре сессии: Смарт-контракты, Цифровые финансовые активы, RegTech и Практическое применение распределённых реестров в рамках российского законодательства. Каждая сессия сопровождалась бурным обсуждением докладов участниками-спикерами и приглашенными экспертами.

Яркое развитие получила тема права в применении к технологии блокчейн. Участники дискуссии отметили, что в России существует проблема создания законов «на будущее». По мнению Максима



Выступление профессора Гамбургского института прикладных систем Фолькера Скварека

Генеральным партнёром STCrypt 2018 стала компания «ИнфоТеКС», официальным партнёром — ООО «КриптоПро». Партнёрами симпозиума выступили компании «Код Безопасности» и НПП «Гамма», партнёром выставки — компания «Актив».

Широкий перечень рассмотренных вопросов, глубина научной проработки проблем и высокий профессионализм участников подтвердили статус симпозиума STCrypt как ведущего российского научного мероприятия в области криптографии. По решению программного комитета, летом 2019 года будет проведён следующий — VIII симпозиум «Современные тенденции в криптографии».



Участники симпозиума STCrypt 2018



Роман Янковский, преподаватель кафедры предпринимательского права юрфака МГУ

Башкатова, ведущего научного сотрудника ВШЭ-Сколково, это закономерно связано с исторической ситуацией, сложившейся в российском законодательстве.

Роман Янковский, преподаватель кафедры предпринимательского права юридического факультета МГУ, высказался следующим образом: «В нашей стране большие проблемы с законодательным процессом, инициати-

вы бизнеса с большим трудом доходят до органов, принимающих решения. Суть в том, что каждый орган хочет захватить себе больше власти, а не решить важную проблему. Тем не менее ситуация с распределёнными реестрами имеет позитивную динамику. Несмотря на то, что регуляторы законов занимают консервативную позицию, блокчейн в скором времени войдет в

обыденную жизнь людей. Например, в принятых платёжных системах банков технология блокчейн уже постепенно внедряется. И если сейчас транзакция может осуществляться несколько часов даже в рамках одного банка, то блокчейн позволит существенно оптимизировать и ускорить этот процесс».

Кроме того, все участники отметили большое количество рисков, связанных с недостаточной конкретизацией закона. Например, в рамках проблемы анонимности обсуждался парадокс бесповоротности реестра, когда становится непонятным, как перевести электронные права на другое лицо в случае соответствующего решения суда. А пока все ждут внятных комментариев Министерства финансов по поводу налогообложения сделок на основе технологии блокчейн, ведь на все вопросы оно отвечает лишь общими фразами.

Материалы подготовила
Валерия Мещерякова,
корреспондент BIS Journal

МЕЖДУ СЦИЛЛОЙ И ХАРИБДОЙ

КОНФЕРЕНЦИЯ «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТЬЮ В СОВРЕМЕННОМ ОБЩЕСТВЕ»

VI Международная научно-практическая конференция «Управление информационной безопасностью в современном обществе» действительно оказалась и научной и практической. Не слишком международной, но это скорее достоинство. У России есть свои проблемы и по части ИТ и по части кибербезопасности, которые, как бы ни усмехались глобалофилы, «аршином общим не измерить».

Ключевой особенностью конференции оказался специфический «классовый» состав участников. Это существенная прослойка старшего поколения, умудрённая не только знаниями и опытом, но и привыкшая чётко фиксировать эти параметры официальными показателями. Пальцев на руке не хватит, чтобы пересчитать докторов наук, выступивших с трибуны. Общее же их число вкупе с кандидатами наук на полях форума проще охарактеризовать словом «множество».

Методы и результаты изучения проблем ИБ, представленные на конференции, являются удачным дополнением чапаевскому стилю, которого придерживаются участники квазихакерских хакатонов с англоязычными названиями.

ЛЕД ТРОНУЛСЯ

Хакатоны с показательными кибервзломами банков и АСУТП сильны лишь в визуализации проблем ИБ, тогда как наука способна предложить решения этих проблем. И тут особо следует отметить доклад «Конвергентная эволюция задач информационной безопасности в условиях цифровой трансформации». Пётр Зегжда, питерский доктор, профессор и отраслевой академик, а также научный руководитель компании «НеоБИТ», презентовал возможность созда-

ния ИТ-систем с врождённым ИБ-иммунитетом. Возможность безусловно необходимая, но пока непривычная уху тех гостей конференции, которые попытались выступить в ответ в терминах «модели угроз ИБ». Добрая, но жёсткая улыбка матёрого питерского интеллигента и возмущённое мысленное шиканье зала мгновенно охолодили ретроградов и вывели их на зады технического прогресса.

Стоит отметить, что конференция представила весьма разноплановые взгляды на проблемы обеспечения ИБ и в классическом понимании (конфиденциальность, целостность, доступность), и с точки зрения безопасности общества в условиях манипулирования информацией с помощью социальных сетей и технологий Больших Данных. В связи с широкой вовлечённостью общества в т.н. цифровую трансформацию на конференции были детально рассмотрены юридические аспекты работы с данными в условиях «цифровизирующих» экономики, госуправления и социальных контактов.

Проблемы ИБ рассматривались и под углом зрения разных отраслей (телеком, финансово-кредитная сфера, торговля, госуправление) и в разных технологических срезах (софт, железо, эксплуатация, с особым акцентом на безопасность работы в интернете).

Наряду с юриспруденцией, стоит особо отметить внимание конференции к элементной базе вычислительных систем как к одному из ключевых элементов обеспечения ИБ. На пленарном заседании, а также в ходе работы специальной секции под руководством д.т.н., профессора НИУ ВШЭ Андрея Чеповского были рассмотрены различные аспекты создания высокопроизводительных многоядерных процессоров

и их применения в системах анализа данных. Работа этой секции и настрой её участников весьма полезны в плане противодействия многочисленным стереотипам, в числе которых и тот, что мы якобы не успели «вскочить на поезд» в том, что касается разработки «железа» для ИТ.

На конференции предпринималась попытка системного анализа достижений отечественных компаний, разрабатывающих операционные системы т.н. общего назначения (т.е. без поддержки технологий реального времени). Речь идёт о круглом столе «Научное содержание понятия информационная безопасность отечественных операционных систем (ОС)». Удалось ли раскрыть заявленную тему? Скорее нет.

ИГРЫ РАЗУМА

Нет оснований сомневаться в компетенции участников круглого стола по отечественным ОС, но очевидна объективная причина, мешающая им легко и непринуждённо, без оглядки на «быт», обсуждать высокие материи своей работы. Это непредсказуемость социально-экономической среды (а хуже того, её предсказуемая «вязкость»), в которой приходится работать вследствие своеобразия мышления государственных мужей, которое никак не назовёшь косным. Скорее дилетантски идеалистичным. Госмужики предпочитают рассуждать и официально поддерживать исследования с широкими, расплывчатыми и слабо контролируемыми толкованиями: Большие Данные, квантовые технологии, новые производственные технологии, технологии виртуальной и дополненной реальности — см. программу «Цифровая экономика РФ». А вот первоочередные нужды российского сектора ИТ, в числе которых

производство базового софта, — это в лучшем случае остаётся за кадром, а то и вообще зачисляется «экспертами» в упущенные возможности.

Пока идеи профессора П.Д. Зегжды о возможностях создания врождённо безопасных ИТ-систем не реализованы в полной мере на практике, острым вопросом при обеспечении ИБ остаётся поиск и выявление т.н. недекларированных возможностей (НДВ) в программном обеспечении. Эта тема затрагивалась в разных докладах, и озвученная ситуация не располагает к оптимизму. Во-первых, в качестве сухого остатка от прослушанных выступлений можно сделать вывод, что решения этой проблемы развиваются скорее в плоскости искусства и эпистолярного жанра общих рекомендаций, чем науки, инженерии и чётких алгоритмов. А, во-вторых, и это главное, общественность, похоже, готова принести в жертву скорости написания программ их качество, а также принять избыточность кода и перетекание багов из одного программного продукта в другой (как и программных багов вообще) в качестве неизбежности.

И при этом общественность, естественно, не слишком доверяет результатам официальных экспертиз на отсутствие НДВ. Например, как следовало из доклада директора по информационной безопасности Microsoft Rus, ряд продуктов этой компании успешно прошли российские проверки на возможность обработки совершенно секретной информации. Компания обеспечила проведение этих работ по отечественным методикам, отечественными экспертами без каких-либо обязательств по части дальнейших коммерческих контрактов.

Но понимающие ухмылки на лицах слушателей конференции, как и отсутствие контрактов, были лучшей оценкой доверия результатам упомянутой экспертизы.

МОЛЧАНИЕ ЯГНЯТ

Лучшей оценкой за неимением иной. А иной не имеется вследствие соглашательской позиции тех, кого общество по инерции относит к научно-технической элите. Соглашательской — с несистемным хаотичным (как организационно, так и с точки зрения выбира-

ОСТЕПЕНЁННАЯ НАУЧНО-ТЕХНИЧЕСКАЯ ЭЛИТА ПРЕДПОЧИТАЕТ НЕ ВСТУПАТЬ В ОТКРЫТУЮ ПОЛЕМИКУ С НОВАЯВЛЕННЫМИ ИТ-ГУРУ

емых технологий и платформ) «внедрением» ИТ в нашей стране и тотальным навязыванием сомнительных стереотипов. Сомнительных как в части места и роли «цифровизации» в экономике, так и приоритетов развития технологий в ходе обретения суверенитета России в сфере собственно ИТ.

В числе таких стереотипов, например, утверждение о том, что «...пройдет какое-то время, и любой товар будет так оцифрован и будет находиться в таких информационных цифровых платформах, что без использования информации из этих платформ вообще нельзя будет ничего построить и модернизировать. И те, кто будут обладать этими платформами, будут хозяевами мира». Это, на минуточку, цитата из ответов президента на встрече с руководством ряда СМИ в начале 2018 года.

Столь категоричные высказывания, предлагаемые президенту в качестве экспертного мнения, свидетельствуют о том, что на пути формирования культуры восприятия цифровой экономики есть чем заняться.

Но остепенённая научно-техническая элита предпочитает не вступать в открытую полемику с новоявленными ИТ-гуру, по совместительству ещё и власть придержащими (академик Жорес Алфёров — это скорее исключение, хотя и замалчивание со стороны СМИ исключить нельзя). Язвительно ухмыляться безопаснее. А лучше вообще не выражать эмоций и помнить уроки мудрого Ходжи Насреддина. За спиной большинства выживших, увешанных академическими регалиями мужей — небольшие коммерческие организации или даже целые группы компаний. На худой конец — кафедры учебных заведений. И «Цифровая экономика РФ» — это тот надёжный ишак, который может позволить им жить вполне сносно.

КТО ВИНОВАТ И ЧТО ДЕЛАТЬ?

Среднеазиатская мудрость вкупе с толерантной осторожностью шварцев-

ского короля, культивируемые отечественной наукой, и нахрапистые интересы глобального бизнеса привели к тому, что хотя т.н. ИТ имеют уже приблизительно четвертьвековую историю внедрения (я не включаю сюда период становления кибернетики и больших ЭВМ), но до сего момента это больше похоже на масштабную обкатку идей НИОКР, финансируемую за счёт населения. Расходы бизнеса на ИТ в конечном счёте оплачиваются тем же населением. При этом ИТ и ИБ существуют фактически как две разные «отрасли», а их проблемы в государственном аппарате курируют «молодые технократы» с дипломами юристов, экономистов, возможно инженеров, но инженеров ни дня не работавших «в технике». В то время, когда этим должны заниматься те, кто имеет опыт, похожий на опыт руководителей компаний Positive Technologies, Лаборатория Касперского, InfoWatch, Информзащита или, по крайней мере, опыт оставшихся пока в обойме руководителей, «родившихся в СССР», возраста 60+. В результате возникающие из-за техники проблемы улаживают страховщики и юристы.

* * *

В этих условиях простой человек вынужден лавировать между Сциллой и Харибдой ИТ и кибербезопасности. Ведь в некотором смысле многие т.н. электронные сервисы — это навязываемая услуга, доступ к которой с кнопочного сотового телефона просто невозможен. Персональный ПК в доме, приобретённый для игр и работы в соцсетях — личное дело каждого, как и доверие его ремонта компьютерному мастеру по объявлению. Но если ПК-клиент навязан в качестве средства общения с государством, то кто должен обеспечить его доверенную работу и сервис?

ЦИФРОВАЯ ГОНКА

НИКТО В МИРЕ НЕ ХОЧЕТ СТАТЬ АУТСАЙДЕРОМ
ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ

В последние месяцы словосочетание «Цифровая экономика» стало весьма популярным. О XXI веке как «веке цифры» говорят на правительственном уровне, вместо Минкомсвязи в новом правительстве создано Министерство цифрового развития, связи и массовых коммуникаций РФ, появилась и должность вице-премьера по цифровой экономике. На местах в срочном порядке готовят региональные концепции и программы цифровой трансформации. Сотни местных экспертов из разных сфер деятельности судорожно сочиняют планы по никому неведомым направлениям (умный город, цифровая трансформация госсектора, производства, региона... стратегия региональных IT-кластеров и т.д. и т.п.). Как утверждают чиновники, переход на «цифру» каждого отдельно взятого региона позволит кардинально изменить и улучшить жизнь населения всей страны.

Но не стоит забывать, что и в других странах идут аналогичные процессы.

РОССИЯ

Начнем обзор с России. Программа «Цифровая экономика РФ» была утверждена 28 июля 2017 г. Она определяет цели, задачи, направления и сроки по созданию условий для развития в России экономики, в которой данные в цифровом виде являются ключевым фактором во всех сферах социально-экономической деятельности. В марте 2018 г. на финансирование трех направлений программы, включая ИБ,

Минкомсвязи выделил 3040,4 млн рублей. Остальное — из внебюджетных средств.

О достижениях в реализации программы чиновники и представители компаний рассказывали уже в апреле на первом «Петербургском цифровом форуме 2018». По их словам, лучше всего программа реализуется в нефтегазовой отрасли, где активно используются (в тестовом или коммерческом режиме) «блокчейн, беспилотные летательные аппараты, автотранспорт с элементами искусственного интеллекта, промышленный Интернет вещей и роботов, включая программных агентов» (по материалам онлайн-издания D-russia.ru).

Есть потенциал и в «цифровой трансформации промышленности». Тут цифровые технологии уже, похоже, скоро сократят издержки производства на протяжении всего жизненного цикла изделия — от концепции до эксплуатации и утилизации продукции. А развитие онлайн-торговли, как оказалось, — это чуть ли не последний шанс для выживания и развития малого и среднего бизнеса, тем более, что интернет-магазины представляют «целый комплекс технических и информационных систем, обеспечивающих взаимодействие с потребителем». Безусловно перспективная отрасль — строительство и ЖКХ.

И, конечно, финансовый сектор. Тут и блокчейн, и большие данные, и маркетплейсы, где на одной платформе будут соперничать и гиганты и маленькие банки, и искусственный интеллект, уже готовый сменить живого кассира и всяких прочих менеджеров.

Отдельные вопросы — ИБ и подготовка кадров для цифровой экономики. С кадрами пока проблема, так как невозможно вычленивать основные требования и подготовить образовательные стандарты, поскольку «предметная область находится в развитии». Не определены и сами «организационные механизмы цифровых трансформаций образовательной среды».

В части ИБ глава компании InfoWatch Наталья Касперская и многочисленные эксперты полагают, что направление ИБ в программе «Цифровая экономика РФ» может стать плацдармом «для рывка на зарубежные рынки с лучшей в мире экспертизой в программировании и инструментах искусственного интеллекта (ИИ)».

Среди других на Петербургском цифровом форуме поднимались вопросы развития цифровых городов, логистики и управления транспортными потоками, перехода на безбумажный электронный документооборот, развития телемедицины и создания единой базы пациентов, обмена большими данными и ресурсами сетевой инфраструктуры.

Так понимают цифровую экономику в России. Энтузиазм есть, но аргументов пока все же больше, чем фактов.

Стоит также отметить, что Росстат не выделяет вклад цифровой экономики в ВВП, выделяя только информационно-телекоммуникационную отрасль, рост которой в 2017 г. составил 3,6%. А вот по оценкам Российской ассоциации электронных коммуникаций, вклад цифровой экономики в ВВП России на конец 2017 г. составил 2,1%, вместе с мобильным сегментом — 5,06%. Влияние интернет-рынков на экономику растет на 11% в год, и к 2021 г. вклад «чистых» интернет-рынков в ВВП составит 4,7%. В интернет-отрасли работают порядка 2,3 млн человек, включая самозанятых.

Так к чему все-таки идем? В рамках развития цифровой экономики в Рос-

**ВКЛАД ЦИФРОВОЙ ЭКОНОМИКИ
В ВВП РОССИИ НА КОНЕЦ
2017 Г. СОСТАВИЛ 2,1%, ВМЕСТЕ
С МОБИЛЬНЫМ СЕГМЕНТОМ — 5,06%**



Китайская система распознавания лиц Yitu Technology

сии планируется создать 50 «умных городов», в которых будет проживать 50 млн человек. Каждый горожанин сможет вносить свой вклад в управление, высказывая мнение на специальных информационных площадках. Благодаря комплексу технических и организационных мероприятий «умные города» создадут комфортные условия для проживания и бизнеса.

Кроме того, в городах с населением более 300 тыс. планируется развернуть сеть 5G. К 2024 г. таких населенных пунктов должно быть не менее десяти. Количество госуслуг, предоставляемых в онлайн-режиме, к 2025 г. должно составить 80%. В 25 городах России будет работать беспилотный общественный транспорт.

КИТАЙ

Тут тоже голова кружится от успехов. В 2015 г. Китай обнародовал стратегию Internet Plus, в которой заявил о планах по выводу страны в лидеры Четвертой промышленной революции. Власти КНР планировали совместить современное производство и мобильный интернет, облачные технологии больших данных и Интернет вещей, а

также развивать электронную торговлю, промышленные сети, интернет-банкинг и вывести китайские IT-компании на мировой рынок как достойных конкурентов западным интернет-гигантам. Китай должен был стать лидером в робототехнике, системах ИИ и создании беспилотных летательных аппаратов. По расчетам специалистов, в 2018 г. расходы на новые технологии должны вырасти до \$ 234 млрд. Эти деньги идут на компьютерное и телекоммуникационное оборудование, разнообразное ПО.

Позднее к стратегии Internet Plus добавил план «Сделано в Китае 2025». Глава КПК Си Цзиньпин провозгласил искусственный интеллект одним из центральных пунктов этого плана. К 2025 г. план должен быть реализован, чтобы преобразовать экономику страны, а к 2030 г. Китай должен стать мировым лидером в области искусственного интеллекта. К слову, искусственный интеллект в понимании китайцев — это не роботы или беспилотники, а системы машинного обучения.

Уже сегодня компьютеры заменили стенографистов в более чем 6 тыс. ки-

тайских судах, они выявляют опухоли у пациентов в больницах, а на станциях метро Шанхая можно купить билеты, поговорив с машиной... Китайские руководители рассказывают о схеме регулирования дорожного движения, при которой «Скорая помощь», переключая поток трафика и светофоров, добирается до пациента вдвое быстрее.

Среди других достижений — система распознавания лиц Yitu Technology, в БД которой хранятся образы 1,5 млрд человек. Она была создана по заказу правоохранительных органов Китая и получила мировое признание на профильных соревнованиях в США. Теперь создатели системы ищут клиентов и в других странах. Эта система позволяет контролировать толпу, искать в ней пропавших детей и пожилых людей...

Другой стартап — Malong Technologies — работает в области моды и на основе анализа данных с многочисленных дефиле определяет модные тенденции для швейной промышленности.

В рамках Плана развития индустрии робототехники, к 2020 г. Китай планирует создать не менее 1 млн роботов в год, что, по подсчетам Международной федерации робототехники, соста-

вит 40% мировых продаж промышленных роботов. В последние годы в Китае появилось более 3 тыс. фирм по производству робототехники. Китайские компании активно скупают акции предприятий иностранных конкурентов, создают препятствия для развития их филиалов в стране и мире.

Правительство КНР поставило перед предприятиями цель сократить импорт компьютерных чипов, который составляет около \$200 млрд в год, уменьшить его вдвое к 2020 г. и стать мировым лидером в области создания полупроводников к 2030 г. На производство микросхем правительство выделило \$150 млрд инвестиций.

Западные эксперты отмечают, что во многом достижения китайцев в области ИИ, робототехники, дронов или 3D-реальности зависят от действий шпионов — реальных и хакеров. Совместные китайские компании требуют от иностранных партнеров делиться новыми технологиями, при этом сами не допускают посторонних к своим разработкам.

Офис представителя США в ВТО создал 200-страничный доклад о недопустимых действиях КНР в рамках этой организации. Однако многие компании сообщают о притеснениях со стороны китайских партнеров неофициально, и аргументов для открытого скандала в ВТО нет. Преференции национальным компаниям — налоговые или финансовые — дает и правительство Китая, опять же нарушая правила ВТО. Все крупные технологические игроки имеют совместные с правительством КНР исследовательские лаборатории.

Все разработки Китая, как отмечают иностранные эксперты, имеют не столько гражданское, сколько военное назначение. И если сегодня ставка в КНР сделана на программирование, в то время как в США предпочитают фундаментальные исследования, то вскоре и этот пробел будет закрыт — работы китайских исследователей и научно-исследовательских институтов получают признание на международной арене.

В 2017 г. цифровая экономика Китая принесла \$4,31 трлн, что на 20% больше, чем десять лет назад. Вклад цифровой экономики в ВВП превысил 33%. Ожидается, что рост продолжится

СОВМЕСТНЫЕ КИТАЙСКИЕ КОМПАНИИ ТРЕБУЮТ ОТ ИНОСТРАННЫХ ПАРТНЕРОВ ДЕЛИТЬСЯ НОВЫМИ ТЕХНОЛОГИЯМИ, ПРИ ЭТОМ САМИ НЕ ДОПУСКАЮТ ПОСТОРОННИХ К СВОИМ РАЗРАБОТКАМ

и в будущем. Тем более, что цифровая экономика позволила создать новые рабочие места. В этой сфере работает 171 млн человек, что составляет 22% от всех работающих в стране. Правительственный аналитический центр Китайской академии информационных и коммуникационных технологий уже заявил, что цифровая экономика страны вступила в «золотую эру» и стала новым двигателем экономического прогресса.

ИНДИЯ

Китай уже давно не считает своего южного соседа конкурентом в борьбе за цифровое превосходство на мировом рынке, его цель — «догнать и перегнать Америку». Между тем, в Индии принята программа «The \$250 Billion Digital Volcano: Dormant No More». Ожидается, что доля интернет-экономики в ВВП страны вырастет с 5% (\$100–120 млрд) до 7,5% (\$215–265 млрд) к 2020 г. Из них электронная коммерция и финансовые услуги составят \$40–50 млрд, продукты электронной коммерции — \$45–50 млрд, цифровые медиа и реклама — \$5–8 млрд.

Технологическое отставание Индии возникло не столько из-за геополитического противостояния с Китаем, сколько потому, что развитию таких направлений, как ИИ, Интернет вещей или 3D-печать, не уделялось достаточно внимания ни правительством, ни инвесторами. Слабо развита в стране и робототехника, хотя спрос на нее со стороны покупателей очевиден.

Рост цифрового сектора ожидается за счет частных и государственных вливаний (\$50–60 млрд), увеличения числа подключений к мобильному интернету (\$45–55 млрд) и покупки гаджетов (\$30–40 млрд).

Имея второе по численности население в мире и наличие 391 млн по-

требителей мобильной связи, Индия стала второй страной мира по числу пользователей мобильным интернетом. К 2020 г. их будет уже 650 млн чел. Одновременно планируется рост трафика в 10–14 раз, средний объем скачанного контента достигнет 7–10 Гб в месяц. Сегодня он не превышает 4 Гб в месяц.

Для роста этого сектора экономики предполагается развивать сети 4G и надежный высокоскоростной доступ в интернет, увеличить число продаж смартфонов и заманить в глобальную сеть новых пользователей, предложив им интересный цифровой контент. Как показывает опыт местных телекоммуникационных компаний, владельцы смартфонов с льготными тарифами, включающими бесплатные услуги, очень быстро начинают активно пользоваться электронной коммерцией и совершать онлайн-платежи.

Ожидается, что эти шаги увеличат время, проведенное онлайн, в 3–4 раза. Более того, количество видео, потребляемого в интернете, вырастет за счет онлайн-медиа и развлечений, а также собственного видео-вещания пользователей. Массовый переход на 4G и развитие точек WiFi-доступа создаст огромные возможности во всех сферах жизни и затронет практически все отрасли, включая финансовые услуги, розничную торговлю, СМИ, туризм, транспорт и здравоохранение.

Из существующих проблем, помимо слабо развитых 4G сетей, специалисты отмечают плохую техническую базу большинства малых и средних предприятий; популярность дешевых смартфонов с ограниченным набором функций, не обеспечивающих беспрепятственный доступ в Интернет; нехватку квалифицированных кадров в сфере IT и безграмотность пользователей.

На фоне этих перспектив правительство страны уделяет особое внимание «оцифровке всего и вся» и переходу на безналичную экономику. Д-р Гулшан Раи, координатор направления национальной кибербезопасности в правительстве страны, отмечает, что Индия как быстроразвивающаяся страна в области цифровой экономики старается уделять больше внимания вопросам ИБ. Для этого надо объединяться не только разработчикам и производителям ПО, тесно сотрудничать с правительством, но и создавать SOC-центры, в том числе на национальном уровне, а для этого нужна законодательная база.

Гулшан Раи считает, что следует инвестировать больше средств в сферы ИИ и машинного обучения. Крупные компании Индии уже установили системы для защиты своих данных от любых кибератак, но им сложно защищаться от целенаправленных атак. Системы ИИ и машинного обучения — технологии двусторонние, которые при правильном подходе и интерпретации результатов помогут повысить устойчивость цифровых систем и сведут к минимуму целевые атаки и их последствия. В развитии таких технологий заинтересованы Резервный банк Индии и Индийский Совет по ценным бумагам и биржам (SEBI), которые сегодня контролируют все подозрительные транзакции и изучают различные методы слежения в рамках политики кибербезопасности.

США

Если каждая отрасль США будет расти так же быстро, как цифровой сектор, экономика страны будет расти огромными темпами. Согласно данным Бюро экономического анализа Министерства торговли США, с 2005 по 2016 г. цифровая экономика росла в среднем на 5,6% в год по сравнению с 1,5% роста экономики в целом. Сектор, в который вхо-



Индия стала второй страной мира по числу пользователей мобильным интернетом.

дят сетевая инфраструктура, электронная коммерция и цифровые медиа, в 2016 г. принес \$ 1,2 трлн или 6,5% ВВП. В 2016 г. в секторе было 5,9 млн рабочих мест, что равно 3,9% от общей занятости в США. Средняя зарплата в отрасли \$ 114 275 в год, что на 72% выше средней компенсации на одного работника в стране. В секторе работает 231 тыс. предприятий.

Достоинства США — независимость штатов от федерального центра. Штаты, и, главным образом, города формируют свою повестку дня для развития цифровой экономики. Местные органы власти создают условия для процветания интернет-экосистемы, в результате чего появляются новые предприятия, технологические центры, которые учитывают уникальные культурные и исторические черты каждой местности и сочетают их с инновационными политическими подходами.

По данным доклада, подготовленного Национальной лигой городов и Интернет-ассоциацией, местные инновации

позволили возродить некогда процветающие, а в последнее время депрессивные города. В Колумбусе (штат Огайо, второй по величине город на Среднем Западе) местные технические фирмы при содействии властей создали благоприятную деловую среду для развития технопарков. Благодаря этому в город перебираются жители с побережья. Город пожинает плоды победы в национальной программе Минтранса США Smart City Challenge за созданный технологически интегрированный план транспортной системы, ориентированной на быстрое перемещение пассажиров и грузов по региону.

Канзас-Сити активно развивался в области технологических инноваций в начале 2000-х и теперь концентрация интернет-сектора и служащих STEM сектора (Science, Technology, Engineering and Mathematics) тут выше, чем в Нью-Йорке, Лос-Анджелесе или Чикаго. В городе есть представительства высокотехнологичных компаний, например, Garmin и Google, в регион переехали несколько крупных компаний из района залива Сан-Франциско.

Власти позаботились о разработке планов экономической интеграции интернет-сектора в инфраструктуру города, чтобы выгоды от сотрудничества получали все жители. Совместно с Cisco был реализован проект умного городского транспорта стоимостью \$ 15 млн

**СОГЛАСНО ДАННЫМ МИНИСТЕРСТВА
ТОРГОВЛИ США, С 2005 ПО 2016 Г.
ЦИФРОВАЯ ЭКОНОМИКА РОСЛА
В СРЕДНЕМ НА 5,6% В ГОД ПО СРАВНЕНИЮ
С 1,5% РОСТА ЭКОНОМИКИ В ЦЕЛОМ**

который облегчил перемещение жителей удаленных кварталов в коммерческий центр. Город сделал максимум для улучшения доступа к высокоскоростному интернету и принял план цифрового подключения Digital Equity.

В районе Crossroads создан Art Incubator, который предлагает инновационную программу для начинающих художников и выпускников художественных школ города для оттачивания художественных и деловых навыков. Помимо занятий, художники используют различные цифровые платформы для продажи работ, рекламы выставок и т.д.

В пятом по численности городе США Фениксе (штат Аризона) расположены штаб-квартиры нескольких компаний из списка Fortune 500 и Fortune 1000. Здесь и ранее процветали технологические гиганты, а сегодня власти уделяют особое внимание кооперации цифровых технологий с городом. Так, Uber выбрал эти места для тестирования беспилотных транспортных средств. В 2014 г. Феникс принял политику открытых данных для повышения прозрачности и предоставления сведений общественности.

Эта политика касается и разработчиков приложений. С тех пор в свободном доступе находятся гигантские массивы данных. Муниципалитет заключил соглашение с Open Gov на запуск нового открытого портала данных, чтобы обеспечить простой и быстрый доступ к информации с помощью улучшенных файловых систем и визуализации данных. Активно поддерживаются стартапы в рамках программы Phoenix home.

Город вкладывает свободные средства не в недвижимость, а в сферу инноваций и внедрения цифровых технологий, находя им применение в «традиционных» секторах экономики.

ГОРОД ВКЛАДЫВАЕТ СВОБОДНЫЕ СРЕДСТВА НЕ В НЕДВИЖИМОСТЬ, А В СФЕРУ ИННОВАЦИЙ И ВНЕДРЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ, НАХОДЯ ИМ ПРИМЕНЕНИЕ В «ТРАДИЦИОННЫХ» СЕКТОРАХ ЭКОНОМИКИ



Генеральный директор Uber Дара Хосровшахи в офисе компании в Питтсбурге (США)

Так, компания LinkedIn провела обучение 6 тыс. человек и запустила Training Finder. Этот инструмент призван упростить поиск работы и обучения, чтобы найти лучшее краткосрочное обучение по специальности в регионе. Участники тренингов могут искать программы по отраслям, навыкам, школам или учителям, а также информацию о стартовых зарплатах, работодателях и выпускниках для каждого сертификата или программы.

Цель этих партнерств и проектов — создать экономические возможности и повысить эффективность услуг и улучшить жизнь жителей района.

В последней трети XX в. Питтсбург потерял 40% своего населения, безработица превышала 17%. Но город не умер, а его власти нашли пути возрождения.

Сегодня в городе и его окрестностях живут более 2,3 млн жителей. Питтсбург вошел в число семи финалистов программы Smart City Challenge и заслужил репутацию ведущего центра технологического образования. В городе есть несколько всемирно известных университетов, включая Университет Питтсбурга, Университет Чатем и Университет Карнеги-Меллона, работают офисы Google, General Motors, Uber и других ведущих технических фирм, активно поддерживаются стартапы. Город стремится улучшить свою вовлеченность в «технологические» программы, о чем свидетельствует работа Управления по реорганизации г. Питтсбурга в поддержку «Дорожной карты для инклюзивных инноваций».

В рамках поддержки инноваций разработана программа PGH Lab, которая предоставляет возможность местным стартапам совместно с городом и муниципальными властями получать опыт внедрения продуктов в реальный сектор экономики через партнерские отношения с организациями-клиентами. Использование системы закупок и быстрых пилотных программ для новых технологий — один из подходов, который может привести к заключению

долгосрочных контрактов и обеспечить стабилизацию в реализации стартапов.

На примере городов авторы доклада делают выводы, что цифровая экономика так или иначе придет в города и регионы, и надо быть готовыми к ее экспансии. Лучше всего задействовать транспортные системы, работу с большими данными, развивать электронную коммерцию и партнерские программы, которые могут принести пользу городу, при этом следует учитывать уникальные культурные и исторические особенности региона. Города должны оценить, как они могут объединить уникальное историческое наследие с современными технологиями. Не стоит бояться экспериментов и небольших пилотных проектов — это способ тестирования идей для местных стартапов, у которых пока нет возможности для полномасштабной реализации. Все эти меры приведут к появлению новых рабочих мест, повышению образовательного уровня населения и росту экономики региона или города в целом.

ЕВРОСОЮЗ

Переход на «цифру» экономики ЕС — огромный потенциал роста для Европы. Европейская промышленность и сегодня является лидером в традиционных секторах экономики и может использовать свои наработки для развития таких технологий, как Интернет вещей, большие данные, робототехника и производства, 3D-печать, блокчейн и ИИ. В будущем эти достижения позволят занять свою нишу на рынках развивающихся стран.

Цифровая трансформация характеризуется слиянием передовых технологий и интеграцией физических и цифровых систем, преобладанием инновационных бизнес-моделей и новых процессов, а также созданием интеллектуальных продуктов и услуг.

В настоящее время предприятия ЕС не в полной мере используют передовые технологии и инновационные бизнес-модели. Развитие отраслей во многом зависит от страны ЕС, величины бизнеса или предприятия и того, к какой области они относятся. Для выравнивания положения Еврокомиссия отметила перспективные направления цифровой трансформации:

СРЕДИ ЛИДЕРОВ ОБЩЕГО РЕЙТИНГА В ОБЛАСТИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭКОНОМИКИ — СТРАНЫ СКАНДИНАВИИ, БЕНИЛЮКС, ГЕРМАНИЯ И ИСЛАНДИЯ, В ОТСТАЮЩИХ — РУМЫНИЯ, ЛАТВИЯ, БОЛГАРИЯ И ХОРВАТИЯ

◆ **Большие данные и цифровые платформы.** Это направление активно развивалось последние 10 лет. Большие объемы данных, создаваемые оборудованием, машинами и людьми предоставляют возможности для инноваций, новых бизнес-моделей и создания интеллектуальных продуктов и услуг.

◆ **Новые цифровые навыки.** Новые технологии высвобождают огромное количество занятых на производстве человек, которых необходимо переучить и найти им новое применение в современных условиях. Расширение разрыва в цифровых технологиях будет влиять на способность предприятий и правительств ЕС извлекать выгоду из возможностей нового производства.

◆ **Города и регионы.** Они являются основными факторами цифровой трансформации в Европе, создают динамичные инновационные экосистемы путем объединения местных ресурсов и всех заинтересованных сторон. Представители госсектора или коммерческих компаний, гражданского общества или местных властей должны понимать социальные и экономические последствия передовых технологий и встать во главе изменений. Программа Digital Cities Challenge — это инициатива Комиссии, которая поможет городам пойти по пути цифровых преобразований.

◆ **Стандартизация и функциональная совместимость** информационно-коммуникационных технологий являются предпосылкой для внедрения цифровых инноваций. Необходимо разрабатывать и внедрить евростандарты, которые обеспечат совместимость систем и повысят конкурентоспособность европейской промышленности и открытость рынков ИКТ.

В связи с этим Еврокомиссия разработала ряд мер и мониторингов для

определения основных тенденций при переходе к цифровой экономике и оценке достижений на национальном и отраслевом уровнях. Мониторинг отражает статистические и фактические данные о темпах цифровых преобразований в конкретных секторах и во всех странах ЕС, анализирует основные инициативы национальной политики и поддерживает развитие этой политики.

По данным мониторинга 2017 г., наиболее перспективными областями считаются: мобильные сервисы, облачные технологии, социальные медиа, робототехника и автоматизированные системы, Интернет вещей, Большие данные и их анализ, сфера ИБ. Из традиционных областей цифровая экономика найдет применение в здравоохранении, машино- и автомобилестроении. Среди лидеров общего рейтинга в области цифровой трансформации экономики — страны Скандинавии, Бенилюкс, Германия и Исландия, в отстающих — Румыния, Латвия, Болгария и Хорватия.

* * *

Подводя итог. Многие страны разрабатывали стратегии по цифровой трансформации экономики к 2020–2030 гг. с учетом существующего сегодня положения вещей. Кто-то уже идет к своей цели семимильными шагами, кто-то действует медленно, но упорно. Кто-то строит сети 5G для Интернета вещей и «умных домов», кто-то развивает давно известные в мире сети 4G. Кто-то создает реальные стратегии и реализует их, а кто-то плодит национальные проекты и программы, от которых через несколько лет остаются воспоминания и суммы потраченных впустую денег.



Александр БОДРИК

вице-президент по информационной безопасности
ISACA Moscow, CISA, ITIL Expert

ТОП-РАБОТОДАТЕЛИ ДЛЯ ТОП-КАРЬЕР

Традиционно государственный бюджет наполняется в первую очередь за счет нефтегазовых гигантов — Газпрома, Роснефти и других. Как ни странно, на рынке труда в кибербезопасности позиции компаний топливно-энергетического сектора не столь заметны. Тут действуют свои закономерности. Рассмотрим текущих и перспективных (в горизонте пяти лет) крупнейших работодателей в сфере ИБ.

ТЕКУЩИЕ ЛИДЕРЫ (ТОП-12)¹

Сбербанк. Крупнейший банк страны содержит и одну из крупнейших служб информационной безопасности. В ее штате есть всевозможные подразделения и центры компетенций, причем банк формирует спрос не только и не столько в Москве — его ИБ-ареал распространяется еще как минимум на Санкт-Петербург, Самару и Новосибирск. Оценка ИБ-штата — 1000+ человек.

Министерство обороны. В силу закрытости ведомства информации о его службе ИБ немного. Однако с учетом штата в 1,4 млн военнослужащих и гражданских служащих счет на специалистов по ИБ идет в тысячах. Правда, остается вопрос: считать ли специфические задачи по защите государственной тайны частью информационной безопасности или выделять в отдельную парافизию?

Министерство внутренних дел. Аналогичная Министерству обороны ситуация: штат ведомства превышает 800 тыс. человек. Публичные закупки ведомства показывают эксплуатацию известных на рынке вендоров — Kaspersky, Positive, Инфотекс — в крупнейших в России масштабах (сотни миллионов рублей при поставке и внедрении только одной подсистемы), так что границ профессионального роста в ведомстве практически нет. Уже по закупкам видно, что кроме государственной тайны в ведомстве хватает подлежащей защите конфиденциальной информации — они в открытом доступе.

Федеральная служба безопасности. Мало кто знает, что штат ФСБ составляет миллион человек. Задачи ФСБ разнообразны: обеспечение экономической безопасности ключевых отраслей, противодействие террору, регулирование определенных аспектов сферы ИБ... и все это — не считая охраны государственной границы РФ. Аналогично другим силовым ведомствам штат Службы ИБ тут превышает тысячу специалистов, но имеет свою специфику — попасть в ФСБ проще всего, окончив ИКСИ Академии ФСБ или аналогичный факультет Бауманки, где частенько преподают одни и те же лица.

Федеральная налоговая служба. Несколько лет назад на одной из конференций ФНС раскрыла численность службы ИБ — порядка 1 тыс. специалистов. Учитывая масштаб и географический разброс подразделений службы, возможно

ожидать, что ФНС создает минимум 80 вакансией ежегодно по всей России (8% текучести персонала в год). В Правительстве РФ высоко оценивают успехи ФНС по повышению качества администрирования налогов, в следствие чего вероятно передача ФНС новых функций с соответствующим ростом штата службы в целом и ИБ в частности.

Пенсионный фонд России. Пенсионный Фонд уже несколько лет как стал крупнейшей в стране организацией по оказанию социальных услуг (в частности, отвечает еще и за выплату материнского капитала). Другие его функции, например, обеспечение инвестиционных процессов, не менее значимы. Учитывая присутствие фонда как минимум в каждом райцентре (более 2,5 тыс. точек), специалистов по ИБ в нем много — сотни, а с «оцифровкой» все новых процессов Фонда и выпуском новых версий его автоматизированной информационной системы (АИС ПФР) спрос на них будет только расти.

Федеральное казначейство. Известная практически каждому чиновнику крупнейшая государственная информационная система «Электронный бюджет» управляется Федеральным казначейством, а значит, её миллион пользователей (как и сотня тысяч пользователей самой «Казны») потребуют заботы сотен специалистов по ИБ.

В целом у служб ИБ федеральных структур две особенности:

♦ В центре они поощряют специализацию, что дает возможность стать

¹ Статья была подготовлена до того, как Ростелеком объявил о покупке Solar Security и анонсировал план найма более 100 специалистов по ИБ.

глубоким профессионалом в конкретной области.

♦ В регионах есть потребность в универсальных специалистах, что дает возможность попробовать себя на разных участках процессов ИБ, не меняя должности.

Газпром. Самая доходная компания России обладает и самыми большими бюджетами на ИБ, что открывает возможности получения интересного проектного опыта. Однако оценка размера штата специалистов по ИБ Газпрома может быть только приблизительной — в силу размера, малой публичности и большого разнообразия направлений деятельности концерна. В первом приближении это 500–1000 специалистов, в том числе учитывая занятых в Газпромнефти, ключевых ДЗО (дочерних зависимых обществах), ИТ-дочках (Газпромавтоматизация, ИТСК, Газпром-информ и др.), различных проектных институтах, где разрабатываются в том числе разделы по ИБ проектной документации на информационные системы. Газпром велик и в нем, словно в отдельном государстве, есть любые перспективы, но внутри него те же, что и в большой стране, проблемы — «дураки» (бизнес не понимает зачем нужна ИБ) и «дороги» (подразделения мало связаны между собой, а различные юридические лица тем более).

Росатом. Будучи сопоставимой по численности персонала с Газпромом Госкорпорация Росатом в разы уступает ему по выручке. Это связано с историческими особенностями и спецификой бизнеса, но вследствие этого бюджеты и размеры службы ИБ Росатома так же в разы уступают возможностям Газпрома. Сильны и позиции службы защиты государственной тайны, соответствующий департамент в управляющей компании так и называется «Департамент защиты государственной тайны и информации». Внутри корпорации интересны подразделения ИБ управляющих компаний крупнейших дивизионов (Росэнергоатом, ТВЭЛ, АРМЗ) и центры компетенций по ИТ и ИБ (Гринатом, Консист-ОС) — там будет возможность фокусироваться на информационной безопасности, во многих других случаях придется время от времени следить и за вопросами физической и экономической безопасности.



СЛУЖБА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГРУППЫ ВТБ ПО ВСЕМ КОСВЕННЫМ ПРИЗНАКАМ ГОРАЗДО БОЛЕЕ КОМПАКТНА, ЧЕМ В СРАВНИМОМ ПО АКТИВАМ СБЕРБАНКЕ, А ЗНАЧИТ НЕИЗБЕЖНО РАСШИРЕНИЕ

Ростех. 700 предприятий этой Госкорпорации мало чем объединены, но там имеется свой ИТ-стандарт. В области ИТ центром компетенции выступает РТ-информ, однако тамошняя ИБ-служба относительно немногочисленна. Интересными для безопасника могут быть в первую очередь подразделения крупнейших холдингов внутри Ростеха — «Вертолеты России», Росэлектроника, Технодинамика, Швабе, ОДК, КРЭТ и ранее упомянутый РТ-информ.

Софтлайн. Многопрофильный ИТ-холдинг Софтлайн (Softline) сделал большую ставку на информационную безопасность: расширил штат до более чем сотни выделенных ИБ-специалистов, а потом еще и приобрел фокусную компанию Infosecurity services. Итого в активе уже сотни специалистов и амбициозные планы по покорению российского и зарубежных рынков, в частности регионов Латинской Америки и Азиатско-Тихоокеанского региона. Впрочем, кандидатам нужно понимать, что добрая половина позиций так или иначе связана с управлением продуктами и продажами. Однако позиция руководителя службы ИБ (да и любого руководителя в принципе) подразумевает определенный уро-

вень продаж своей функции внутри организации, поэтому такой опыт работы может быть стратегически полезен.

ПЕРСПЕКТИВНЫЕ ЛИДЕРЫ (ТОП-5)

ВТБ. Группа ВТБ за последние 10 лет нарастила свои активы в разы, а в последнее время появляются новости о возможной ее консолидации с санируемым Банком России ФК «Открытие» и Бинбанком. В любом случае служба информационной безопасности Группы по всем косвенным признакам гораздо более компактна, чем в сравнимом по активам Сбербанке, а значит, неизбежно расширение. Оценочный целевой размер штата — 400 специалистов самых разных специализаций: инфраструктурная безопасность, application security, security management и т.д.

Ростелеком. Переживающий цифровую трансформацию Ростелеком нанимает специалистов по ИБ практически в каждом федеральном округе. Это и технические специалисты, и специалисты по управлению продуктами информационной безопасности, и специалисты с большим фокусом на продажи — совокупно у Ростелекома никак не меньше

полтора сотен специалистов, а будет очевидно минимум сотни три. Внутри службы удивительное разнообразие позиций и обязанностей, ведь «оператор» (а правильнее сказать, цифровой холдинг) на самом деле уже и сервис-провайдер, и вендор, и Центр обработки данных — только под государственные услуги у него в свое время было пять ЦОДов, а ведь потом была приобретена компания Safedata. Учитывая размер коммерческого блока компании («силу продаж») и ее государственный статус, будущее у ее службы ИБ будет ярким, но надо понимать внутренние особенности — исторически повышенную бюрократию и высокую конкуренцию за инвестиционный ресурс между подразделениями, а значит просто не будет.

Роскосмос. Роскосмос — практически как Росатом, только в прошлом. Сильный фокус на государственную тайну, в пару раз меньший размер, экономические проблемы у ряда предприятий. Однако аэрокосмическая отрасль России — одна из сильнейших в мире, заказы на космические технологии у частного и военного секторов есть, аэрокосмическая отрасль мира стремительно развивается, так что в ближайшие 5–10 лет Роскосмос и его служба ИБ будут подниматься и интересных задач будет становиться все больше. Относительно небольшая зрелость представляет отдельный интерес: еще есть что строить и развивать, а вот, например, в филиалах международных компаний в России все наоборот, процессы выстроены из глобальных штаб-квартир и им остается только банально следовать.

Федеральная служба охраны. Федеральная служба управляет закрытым сегментом Рунета — «госнетом». Ввиду продолжающихся геополитических штормов и санкций «госнет» будет только расти и задачи по его защите и защите подключений к нему тоже. Размер задач фактически неограничен, в случае реаль-

ных проблем в «госнет» может переехать очень большое количество сервисов — вплоть до государственной системы межведомственного электронного документооборота (СМЭВ) и иных сервисов оказания государственных услуг.

Роснефть. Отраслевые стандарты Росатома и Газпрома на рынке ИБ хорошо известны (ЕОСИБ Росатома, СТО Газпром), а вот про сопоставимого уровня детализации стандарты Роснефти пока не слышать. А значит все впереди, и компания с многотриллионной выручкой будет системно и последовательно инвестировать в ИБ, тем более, что ввиду физических и экологических свойств процесс добычи, транспортировки, переработки и перевалки нефти неразрывно связан и фактически непрерывен — и эту непрерывность нужно обеспечивать в том числе и специалистам по ИБ. А учитывая глобальные амбиции и масштаб деятельности НК Роснефть, обеспечивать придется в глобальном масштабе, принимая во внимание зарубежные нормативные документы и технологические особенности приобретаемых за рубежом активов.

«МЕДОВЫЕ ЛОВУШКИ» ИЛИ ЛИДЕРЫ БЕЗ ПЕРСПЕКТИВ

Кроме текущих и потенциальных лидеров существует ряд компаний, которые, с одной стороны, на слуху, а с другой, вряд ли разовьют у себя сообразные размеру своего бренда и выручки подразделения информационной безопасности. Для большинства специалистов по ИБ такие компании представляют собой «медовые ловушки» и о них лучше знать заранее.

Интернет-компании. Будучи открытыми и во многом публичными, интернет-компании регулярно публикуют вакансии по информационной безопасности и выступают на конференциях. Из этих и других подобных материалов видно, что даже бизнесы с многомиллиардной оценкой в долларах имеют все-

го-навсего отделы ИБ. Ситуация понятна: прозрачный бизнес таких компаний имеет не так много требований по конфиденциальности, вопросы целостности закрываются во многом высокой степенью контроля за сервисами в целях обеспечения качества услуг, вопросы доступности решаются с многочисленными и одними из лучших в России R&D и департаментами эксплуатации. Другие особенности служб ИБ ИТ-компаний (связанные с фундаментально высокой тиражируемостью ИТ-сервисов) раскроем в следующем описании.

ЦОДы. Высокая степень тиражируемости сервисов Центров обработки данных скорее сформирует спрос на программистов, чем на специалистов по информационной безопасности. Таковых даже для гигантского ЦОДа понадобится всего несколько десятков — обслуживать мощные специализированные средства защиты, консультировать службы эксплуатации ИТ по отражению атак и формировать требования для разработчиков.

Металлургические гиганты. Металлургические гиганты вряд ли станут гигантами с точки зрения ИБ — в процессах поиска и разработки месторождений с последующими обогащением и переработкой руды в металл банально не так много места информационным активам и их безопасности. Менее остро, чем в нефтегазе стоит проблема непрерывности производственной цепочки (руды намного проще и безопаснее для экологии транспортировать, чем нефть или газ), менее остро стоит и политический вопрос — спецслужбам иностранных государств выгоднее атаковать в первую очередь государственные структуры и ТЭК.

Специалисту по информационной безопасности в России есть и будет куда податься — выбор крайне широк: от атомной отрасли и космоса до банкинга и федеральных служб. Главное, прислушаться к чему душа лежит, ведь если заниматься обеспечением безопасности значимого для себя крупного дела, то и работа будет спориться, и стрессовые ситуации будут восприниматься не так остро.

СУЩЕСТВУЕТ РЯД КОМПАНИЙ, КОТОРЫЕ, С ОДНОЙ СТОРОНЫ, НА СЛУХУ, А С ДРУГОЙ, ВЯД ЛИ РАЗОВЬЮТ У СЕБЯ СООБРАЗНЫЕ РАЗМЕРУ СВОЕГО БРЕНДА И ВЫРУЧКИ ПОДРАЗДЕЛЕНИЯ ИБ

ОЛИМПИАДЫ ПО ИБ 2018

В БОЙ РВУТСЯ ШКОЛЬНИКИ
И СТУДЕНТЫ КОЛЛЕДЖЕЙ



Марина БРОДСКАЯ
обозреватель
BIS Journal

Готовя очередной ежегодный обзор школьных и студенческих олимпиад, я не надеялась увидеть что-то новое в организации мероприятий: решение задач или соревнования в формате CTF идут по давно проложенным рельсам. Но оказалось, в 2017/2018 учебном году список соревнований расширился, а предлагаемые в них задачи стали разнообразнее.

МЕЖРЕГИОНАЛЬНЫЕ ОЛИМПИАДЫ ШКОЛЬНИКОВ

Традиционно итоги этих олимпиад подводятся в начале календарного года. Межрегиональная олимпиада школьников по математике и криптографии и олимпиада по информатике и компьютерной безопасности ежегодно проводятся Академией ФСБ России, Академией криптографии РФ, УМО ИБ при участии входящих в его состав вузов, других образовательных учреждений,

при содействии иных юридических лиц. Координацию организационного обеспечения олимпиад осуществляет Институт криптографии, связи и информатики Академии ФСБ России.

Олимпиады проводятся для школьников 8–11/9–11 классов школ и студентов колледжей. Соревнования проходят в два тура — отборочный (в дистанционной форме) и заключительный (в очной форме). Работы всех участников заключительного (очного) тура олимпиады пересылаются в ИКСИ Академии ФСБ России. Проверка и определение победителей (призеров) проводится централизованно по единым критериям.

Второй этап олимпиады школьников по информатике и компьютерной безопасности прошел в 12 регионах России, он собрал 280 человек, победителями и призерами стали 26 школьников. В очном этапе XXVII олимпиады по матема-

тике и криптографии приняли участие около 2000 человек из 45 городов страны.

ВСЕРОССИЙСКАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА ПО ИБ

В конце апреля в НИЯУ МИФИ при поддержке Минобрнауки России, ФСТЭК России, а также УМО вузов по информационной безопасности прошел финал VI Всероссийской студенческой олимпиады по информационной безопасности. Отборочный тур проходил с начала марта, его университеты проводили самостоятельно.

В олимпиаде приняли участие студенты вузов, обучающиеся по программам бакалавриата, специалитета и магистратуры укрупненных направлений подготовки 10.00.00 и 09.00.00, в том числе начинающие молодые ученые, проводящие изыскания по специальности ВАК 05.13.19.



Победители XXVII Межрегиональной олимпиады по математике и криптографии и XII Межрегиональной олимпиады по информатике и компьютерной безопасности



Участники III Всероссийского кейс-чемпионата для молодых специалистов по ИБ

Победители, призеры и лауреаты Олимпиады были награждены дипломами и ценными подарками. Лауреаты Олимпиады получают льготы при поступлении в магистратуру по направлениям подготовки «Информатика и вычислительная техника» и «Информационная безопасность» Института интеллектуальных кибернетических систем НИЯУ МИФИ. Победители (участники, занявшие 1, 2, 3 места) зачисляются в магистратуру НИЯУ МИФИ без вступительных экзаменов на направления инженерной подготовки. По традиции победители получили полезные и ценные призы от организаторов и спонсоров мероприятия, в том числе сертификаты на бесплатное обучение на курсе «003. Тестирование на проникновение: технологии хакеров для аудита информационной безопасности».

III ВСЕРОССИЙСКИЙ КЕЙС-ЧЕМПИОНАТ ДЛЯ МОЛОДЫХ СПЕЦИАЛИСТОВ ПО ИБ

Организаторы мероприятия получили 114 заявок на участие в соревнованиях от команд из 11 городов России. По сравнению с прошлыми годами география чемпионата расширилась, что отметили сами организаторы. В финале кейс-чемпионата по ИБ RISC-2018 приняли участие 7 команд из российских вузов, в том числе Сыктывкарско-

го университета им. Питирима Сорокина, Сибирского государственного университета телекоммуникаций и информатики, Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (ИТМО), Санкт-Петербургского государственного экономического университета (СПбГЭУ) и др.

Финал кейс-чемпионата прошел в апреле в Конгресс-центре Московского технического университета связи и информатики (МТУСИ). По итогам двух этапов конкурса победителями чемпионата стала команда Bread Hunting — сборная аспирантов и студентов старших курсов НИУ ВШЭ, НИЯУ МИФИ и Московского Политеха. Второе место заняла команда KirPitch из НИУ ВШЭ. Третье — команда InfoSec, МТУСИ.

На первом этапе командам предлагалось подготовиться к Чемпионату мира по футболу с учетом принятого ФЗ-187 «О безопасности критической информационной инфраструктуры РФ». В итоговой презентации надо было провести оценку возможной компрометации ИТ-инфраструктуры и составить план мероприятий по защите от кибератаки государственной организации.

В финале командам предстояло за 50 минут решить кейс и подготовить презентацию, а затем выступить с её защитой перед жюри. Это удалось сделать

не всем финалистам. Строгое жюри на всех этапах чемпионата оценивало не только техническую реализацию предложенного решения и глубину его проработки, но и точность ответов на поставленные вопросы. Из-за невнимательности и неправильного прочтения задания на первом этапе были отсеяны большинство участников. По этой же причине потеряли столь важные баллы и те, кто прошел в финал соревнований.

Конкурсные задания на первом и втором этапах были разработаны специалистами-практиками из крупнейших российских компаний. И, вопреки ожиданиям экспертов, в ходе решения задач студенты предлагали не только типовые решения, но и оригинальные, учитывающие последние веяния на рынке средств ИБ. Победители Кейс-чемпионата были награждены почетными кубками и медалями, а также специальными призами от организаторов и партнеров конкурса. А также приглашены на стажировку и собеседования в ведущие ИТ, ИБ и телекоммуникационные компании страны.

QCTF SCHOOL 2018

Соревнования по правилам QCTF для школьников старших классов проводятся с 2013 года (как Ural SchoolCTF), в 2014 г. они проходят в разных городах России, организаторами выступают студенты Уральского федерального университета.

CTF (Capture The Flag) — это командные соревнования, цель которых — «захватить флаг», достичь некоего результата, поставленного организаторами соревнований. На QCTF School 2018 команда школьников должна выполнить набор заданий из разных областей знаний любым доступным способом. Результатом решения является некоторая строка, которую и необходимо отправить на проверку. Финальные соревнования, в которых участвовали 159 команд, прошли в середине мая сразу на 26 точках проведения QCTF School 2018 по всей стране и за ее пределами.

Общий рейтинг команд школьников представлен на сайте организаторов QCTF. В списке — более 350 команд, которые хотя бы один раз приняли участие в соревнованиях для новичков и набрали очки.

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ПРОФЕССИОНАЛЬНОГО МАСТЕРСТВА

Итоги Всероссийской олимпиады профессионального мастерства по укрупненной группе специальностей 10.00.00 «Информационная безопасность» в этом году подвели в Уфе. В конце апреля в Уфимском колледже радиоэлектроники, телекоммуникаций и безопасности прошел заключительный этап соревнований, на который приехали 28 участников из 27 регионов России. Все они стали победителями региональных этапов, выполнили тестовое задание и задания по организации работы коллектива, а также перевели профессиональный текст.

Второй этап включал профессиональное задание с учетом специфики специальности ИБ: участники на протяжении трех дней выполняли комплексные многоуровневые задания с использованием специализированного оборудования и программного обеспечения. Победителем соревнований стал Дмитрий Салаткин, студент Аэрокосмического колледжа, Сибирский государственный аэрокосмический университет имени академика Решетнева. Второе место занял Александр Аксентьев (Челябинский радиотехнический техникум). Третьим стал Константин Кисенко из Краснодарского колледжа электронного приборостроения.

Одновременно в рамках деловой программы олимпиады прошел III Пленум Федерального учебно-методического объединения в системе среднего профессионального образования по укрупненной группе специальностей 10.00.00 «Информационная безопасность». Также организованы КПК по теме «Технологии проведения демонстрационного экзамена и разработки контрольно-измерительных материалов для государственной итоговой аттестации по специальностям в области ИБ» и научно-практическая конференция «Пути совершенствования подготовки кадров по специальностям СПО в области ИБ». В работе Пленума приняли участие представители образовательных организаций среднего и высшего образования (из них четыре, реализующих ФГОС СПО), представители регуляторов, региональных и федеральных органов исполнительной власти.

CTF GENESIS-2018

В марте в Тихоокеанском государственном университете (ТОГУ) впервые прошла Олимпиада для «белых хакеров» CTF Genesis-2018, в которой могли участвовать только школьные команды.

Организаторами выступили студенты кафедры Компьютерная безопасность ТОГУ и ученики 11-х классов. Участниками CTF Genesis-2018 стали старшеклассники общеобразовательных школ, лицеев, гимназий города Хабаровска. Среди них были как новички, так и опытные игроки, уже принимавшие участие в соревнованиях в декабре 2017 г. В течение восьми часов команды решали задачи, среди которых были криптография, реверс, веб, стеганография, поиск информации, PPS-программирование.

Победители CTF Genesis-2018 получили награды, сертификаты участников олимпиады и подарки от ТОГУ и спонсоров проекта — Министерства информационных технологий и связи Хабаровского края и компании Мегафон.

Одновременно с CTF Genesis-2018 в ТОГУ проходила конференция по защите компьютерных программ «ПоИБ», которая открыла серию мероприятий по ИБ в Хабаровске. Среди планов организаторов — открытие школы для студентов и школьников по изучению прикладных практических вопросов в области ИБ и проведение олимпиады CTF для студентов и школьников в формате «attack-defence».

INNO CTF JUNIOR 2018

В конце апреля в АНО ВО «Университет Иннополис» (Татарстан) завершился первый Турнир по компьютерной безопасности для школьников Inno CTF Junior 2018. В отборочных соревнованиях, предшествовавших очной встрече, командам предлагалось решить 25 задач из семи категорий: admin, crypto, forensic, network, pps, web, joy. Задания были представлены в виде виртуальной карты города, который команды должны были захватить. В финал прошли участники, набравшие максимальное число баллов.

В финале участвовали 60 школьников из 12 регионов России. В течение двух дней они решали задания по криптографии, стеганографии, уязви-

мости веб-приложений и другим аспектам кибербезопасности. Первый день был посвящен Task-based (jeopardy). Команды получили набор заданий, к которым требовалось найти ответ и отправить его жюри. Ответом мог быть набор символов или произвольная фраза. Второй этап соревнования — Classic (attack-defense). Каждая команда получила выделенный сервер или небольшую сеть для поддержания её функционирования и защиты. Очки зачислялись за корректную работу сервисов своего сервера и за украденную информацию с серверов соперников.

Победителем Inno CTF Junior 2018 стала команда учеников 11-х классов из Москвы, Мытищ и Королёва, в числе призеров — московские команды Ugan dan Web Force и EVA.

TYUMEN CTF 2018

В начале апреля команда Тюменского государственного университета провела III соревнования по ИБ Tyumen CTF. Это открытый онлайн-CTF для начинающих команд школьников и студентов в формате task-based. Как отметили организаторы, на онлайн-соревнования зарегистрировалось рекордное количество участников: более 170 школьных и студенческих команд из России, Украины, Тайваня, Испании, Индонезии и Японии. Во время соревнований был преодолен порог в 10000 попыток сдачи флага и 500 полученных флагов. Победителями среди студентов стала команда Lunary из НИУ ВШЭ (Москва), среди школьников — сборная команда Twinklewing Firefly из Лицей ДВГУПС, ЛИТ, МБОУ СОШ № 12 г. Хабаровска.

В планах у организаторов — провести в октябре 2018 г. межрегиональные соревнования в формате CTF по Уральскому федеральному округу среди школьников и студентов.

* * *

Летом студентов и школьников ждут соревнования Altay CTF 2018, Летняя школа «Развитие CTF движения в России». Завершится год в декабре, когда в битве за II Кубок CTF России встретятся победители крупнейших CTF-соревнований среди школ, университетов и колледжей 2018 г.



Евгения КОЛОДИНА
директор по развитию ООО «ЦИБИТ»

ЗАКРЫВ ГЛАЗА, ЛЮБОВЬ НЕ ПОВСТРЕЧАТЬ

СОЦИАЛЬНЫЙ ПРОЕКТ «ТРИ ШАГА К УСПЕХУ»

Каждый раз, когда я принимаю участие в различных форумах, конференциях, круглых столах, посвященных вопросам и проблемам современной информационной безопасности, я неизбежно сталкиваюсь с темой дефицита кадров. Об этом говорят много, громко и как-то безнадежно. Вопросы так и остаются вопросами, а ответы не находят отклика в сердцах тех, кто эти вопросы задает. Работодатели, словно с закрытыми глазами, не видят путей выхода из сложившейся ситуации и лишь разводят руками, в то же время стремясь переманить друг у друга более-менее подходящих специалистов. «А что делать?» — негодуют они.

ГДЕ ВЗЯТЬ КЛАССНЫХ СПЕЦИАЛИСТОВ?

Перелистываю программы различных отраслевых мероприятий, таких как Уральский Форум, РКІ-Форум, КЗИ, SOC-Форум и др. Тема звучит всё громче:

«Где найти квалифицированного специалиста по ИБ для финансовой сферы? Как соединить интересы вузов

и работодателей?» (Уральский Форум, февраль 2018)

«Кадровый голод. Не секрет, что хороших специалистов не хватает на все SOC-и. Поэтому вопрос, откуда брать специалистов, один из самых острых». (SOC-Форум, ноябрь 2017)

«Кадры решают все!» (Научно-практическая конференция «Комплексная защита информации», май 2018)

Острый дефицит кадров в отрасли растет подобно снежному кому, находясь в прямой зависимости от роста киберугроз, ужесточения требований регуляторов и т.п., несмотря на то, что ежегодно вузы выпускают тысячи специалистов, получивших высшее образование по информационной безопасности. Почему? Работодатели, клиенты кадрового агентства «ЦИБИТ», отвечают: «Вузы выпускают теоретиков, а нам нужны практики с опытом работы».

Опыт работы! Вернее, его отсутствие. Вот что становится камнем преткновения при принятии решения о найме выпускника. И решение, как правило, принимается не в его пользу.

Иногда, задавая вопрос кандидату, ищущему работу, почему он никак не может трудоустроиться, мы получаем ответ, что работы на рынке практически нет, а те работодатели, которые есть, предлагают рабский труд с грошовой зарплатой. А если спросить работодателей, в чём причина столь долгого поиска персонала, то зачастую можно услышать такой ответ: «На рынке только неучи и бездельники с высокими зарплатными ожиданиями».

Каждый из них прав и неправ по-своему.

«МЫ ВЫБИРАЕМ, НАС ВЫБИРАЮТ. КАК ЭТО ЧАСТО НЕ СОВПАДАЕТ...»

Занимаясь профессионально вопросами поиска и трудоустройства кадров в отрасли ИБ, мы зачастую становимся свидетелями того, что работодатели и специалисты не могут друг друга найти. Не хотят. Не умеют. Нет времени. А если речь идет о молодом специалисте, о выпускнике института, то тут еще добавляется и отсутствие опыта, и стеснительность, и многие другие факторы.

Работодатели ищут готовых специалистов с высоким уровнем подготовки, подтвержденным различными дипломами, сертификатами, свидетельствами, которые сумеют моментально вникнуть в работу. И никто не хочет вкладываться в выпускников вузов, т.к. считается, что дело это неблагодарное

ОСТРЫЙ ДЕФИЦИТ КАДРОВ В ОТРАСЛИ РАСТЕТ ПОДОБНО СНЕЖНОМУ КОМУ, НАХОДЯСЬ В ПРЯМОЙ ЗАВИСИМОСТИ ОТ РОСТА КИБЕРУГРОЗ, УЖЕСТОЧЕНИЯ ТРЕБОВАНИЙ РЕГУЛЯТОРОВ И Т.П.

и бесполезное. Среди наших клиентов многие так откровенно и говорят, при этом выдвигают требование к соискателям на вакансии по информационной безопасности — опыт работы не менее 1 года. А где же выпускник получит этот опыт, если его никуда не берут? Замкнутый круг!

В то же время готовых суперспециалистов мало, они в большинстве своем благополучно трудоустроены, найти их трудно без специальных навыков. На помощь приходит кадровое агентство «ЦИБИТ», сотрудники которого являются экспертами в области подбора персонала, связанного с защитой информации, и помогают компаниям утолить кадровый голод.

История поиска сотрудника и развития трудовых отношений с ним подобна истории любви. Сначала мы присматриваемся к партнеру, формулируем свои требования к нему, пытаемся понравиться друг другу, тем не менее обозначая границы, и оцениваем, как он на эти требования и границы реагирует. Конфеты, букеты в личных отношениях сродни предложению соцпакета в трудовых.

ЗАКРЫВ ГЛАЗА, ЛЮБОВЬ НЕ ПОВСТРЕЧАТЬ

Вот только с закрытыми глазами эти отношения построить не удастся. Пришла пора открыть глаза навстречу реалиям современного мира. Опытных зубров на всех не хватит. Работодателям

НЕ БОЙТЕСЬ ТОГО, ЧТО ВЫ ВЛОЖИТЕ В НИХ СИЛЫ, А ОНИ ПОТОМ УЙДУТ. ЕСЛИ ВСЁ ВЫШЕПЕРЕЧИСЛЕННОЕ СДЕЛАТЬ В КОМПЛЕКСЕ, ИМ НЕЗАЧЕМ БУДЕТ УХОДИТЬ

пора, наконец, понять, что будущее их бизнеса, будущее отрасли, и даже будущее страны, зависит от того, готовы ли они сегодня взять на себя ношу по практическому обучению молодых специалистов. Пора растить свои молодые кадры!

Разработать мотивационные программы, сформировать институт наставничества, научить студентов на практике, как должны работать профессионалы, на каких принципах основывать свою деятельность, какие инструменты использовать для того, чтобы минимизировать угрозы, существующие в каждой организации, прочертить вместе с ними вектор их карьерного развития, роста на долгосрочную перспективу.

Не бойтесь того, что вы вложите в них силы, а они потом уйдут. Если всё вышеперечисленное сделать в комплексе, им незачем будет уходить. Они полюбят свою работу. А любовь — это сильный мотиватор.

Именно с этой целью мы разработали социальный проект для студентов и выпускников вузов, который заключа-

ется в возможности получения грантов на бесплатное дополнительное профессиональное образование и последующей помощи в трудоустройстве.

СОЦИАЛЬНЫЙ ПРОЕКТ «ТРИ ШАГА К УСПЕХУ»

- ♦ Шаг 1: Прохождение тестирования
- ♦ Шаг 2: Получение грантов, прохождение обучения

- ♦ Шаг 3: Трудоустройство

У «ЦИБИТ» налажены хорошие связи со многими высшими учебными заведениями. Один раз в год на конкурсной основе по итогам специального тестирования мы производим отбор лучших студентов и выпускников вузов по профильным и смежным специальностям для получения грантов на бесплатное обучение в отраслевом учебном центре «ЦИБИТ» по программам профпереподготовки по информационной безопасности, согласованным с ФСБ России и ФСТЭК России. Это обучение позволит молодым специалистам повысить уровень своих знаний и понимания проблематики ИБ. После прохождения обучения кадровое агентство «ЦИБИТ» будет содействовать трудоустройству таких студентов, будет развивать их профессиональную траекторию, способствовать становлению их карьеры, будет готовить кадровый резерв для работодателей, которые захотят открыть глаза навстречу пониманию пути решения кадровой проблемы и будут готовы открыть двери своих компаний молодым перспективным специалистам.

«ЦИБИТ» приглашает к сотрудничеству компании, испытывающие дефицит кадров, которые готовы открыть вакансии для молодежи и принять участие в социальном проекте.

ПРЕИМУЩЕСТВА НАЙМА ВЫПУСКНИКОВ

- ♦ Выпускник — как чистый лист. То, как он будет в дальнейшем трудиться, зависит от того, что и как вы на этом листе напишете. Воспитайте его под себя, и тогда лучшего сотрудника вам не найти.

- ♦ Выпускник открыт для всего нового. Формируйте с ним вместе его функционал, предупредив, что он со временем будет меняться, и вы не услышите от него те слова, которые частенько слышите от опытных сотрудников — «Это не моя работа».

- ♦ Выпускник свеж умом. Его работоспособность в разы выше, чем у его более взрослых коллег. Он способен впитывать огромный объем новой информации и генерировать новые идеи. Уделяйте ему внимание, и вы получите новые, подчас нестандартные решения.

- ♦ Любой новый сотрудник — это всегда кот в мешке. Никогда не знаешь, какие угрозы он может принести в организацию. Выпускник еще не «отравлен» увольнениями с предыдущих мест работы, а значит, не столь изощрен в способах мести и вредительства.



Артем ЗУБКОВ
директор Фонда
содействия развитию
безопасных
информационных
технологий (ФСРБИТ)

СИСТЕМА СТАБИЛЬНА, НО НЕПОВОРОТЛИВА

МЕЖДУНАРОДНЫЙ И ОТЕЧЕСТВЕННЫЙ
ОПЫТ ОБРАЗОВАНИЯ В СФЕРЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На научно-практической конференции «Комплексная защита информации» активно обсуждался вопрос образования и подготовки кадров в сфере ИБ. Неподдельный интерес участников вызвал доклад «Международный и отечественный опыт образования в сфере информационной безопасности», прочитанный в рамках «Школы молодых ученых» директором Фонда содействия развитию безопасных информационных технологий (ФСРБИТ) Артемом Зубковым. В докладе исчерпывающе представлена картина базовой подготовки кадров в сфере ИБ и обозначены ее основные болевые точки. Публикуется с сокращениями.

Не секрет, что число хакерских атак год от года растет. Ежегодно эксперты фиксируют их кратный рост, распространение новых вирусов-шифровальщиков, эксплуатацию различных уязвимостей. Аналитики отмечают, что во многом процветанию киберпреступности способствуют сами пользователи. Причина — низкая осведомленность в сфере информационной безопасности.

Учитывая все большее проникновение интернета в жизнь, проблема осведомленности (а правильнее все же назвать ее проблемой образования в сфере ИБ) приобретает глобальный характер. Хакеров сегодня интересуют и банковские счета, и системы жизнеобеспечения, и узлы связи, и объекты топливно-энергетических комплексов, и Интернет вещей — все, до чего можно дотянуться через глобальную сеть. И они не собираются останавливаться.

Почему? Потому что это выгодно. На Финополисе-2017 в Сочи были приведены шокирующие данные: совокупный рынок киберпреступности на планете сегодня оценивается в 2–3 триллиона долларов и продолжает расти. Для сравнения: рынок наркотиков уже много лет стабильно оценивается в 1 триллион долларов.

Понятно, что бороться с таким злом в глобальном масштабе можно только всем миром. И одной из главных, если не главной составляющей успеха в этой войне является повышение всеобщего уровня образования в сфере ИБ.

ШКОЛА

Естественно, начинать надо с раннего детства. И если воспитанникам детских садов сведения об информационной безопасности еще не требуются, то школьникам необходимо осваивать азы кибербезопасности уже с первого класса. И тут происходит первое столкновение с представлениями об информационной безопасности российских чиновников разного уровня.

Как проходит просвещение и профориентация школьников в сфере ИБ в России? Если исключить специализированные классы с уклоном в информатику и ИКТ, то согласно Федеральным государственным образовательным стандартам, информационной безопасности уделяется по 1–2 часа в год (!) в 7 и 9 классах. Часть информации по кибербезопасности дается в виде дополнительных сведений при изучении других тем или предметов в формате — внимание! — общения с учителями через соцсети и электронную почту. То

есть подразумевается, что такая работа для учителя является чем-то вроде общественной нагрузки, а значит, не обязательна к выполнению.

Основная же часть так называемой просветительской работы проходит в виде «акций». Беда этих акций заключается в том, что они оттягивают на себя немалые средства и создают видимость активной работы по этому важному направлению. Например, многочисленные околообразовательные структуры проводят разовые акции в формате Единого урока кибербезопасности в сети или сетевой викторины для дошкольников и учащихся 1–11 классов. На этом знакомство детей с темой информационной безопасности чаще всего и заканчивается. Честно говоря, я интересовался, но так и не встретил ни одного школьника, который участвовал бы в такой викторине. Это не говорит о том, что такие мероприятия проводятся исключительно для галочки, но и популярными среди молодежи, привычными, системными они не являются.

Конечно, многое зависит от школьных учителей. Есть педагоги, которые сами включают материал по ИБ в рамки предмета «Окружающий мир» в начальной школе. Старшеклассникам в рамках курса «Информатика» предлагают обсудить такие вопросы, как кража личных данных и утечка информации; вирусы, черви, трояны; спам; хакерские атаки; мошенничество; дезинформация; авторское право и нелицензионное программное обеспечение. Это, конечно, здорово и заслуживает всяческих похвал, но это также не системный подход, это — из области «просто повезло с учителем».

Безусловно, учащиеся профильных классов и те дети, которые в рамках дополнительного образования выбрали в качестве будущей профессии информационную безопасность, знают о ней намного больше. Такие школьные команды участвуют в олимпиадах и соревнованиях типа CTF, организуемых федеральными университетами на местном и региональном уровнях.

Но, акцентирую, единой программы по знакомству с информационной безопасностью на базовом, даже бытовом, уровне в системе начального и среднего образования в наших школах нет.

А КАК У НИХ?

Поскольку мы ищем положительные примеры обучения школьников азам ИБ, стоит обратиться к опыту Великобритании. В феврале прошлого года королева Елизавета II открыла новый Центр национальной кибербезопасности Великобритании в Лондоне. Отметим само словосочетание — *национальная кибербезопасность*, что говорит о понимании проблемы и стремлении ее решить на государственном уровне.

Фактически Центр заработал еще в октябре 2016 г., он был образован путем слияния трех ведомств — Группы безопасности в электронике и связи, CERT-UK (что-то вроде нашей ГосСОПКи) и Центра кибероценки. Возглавил его Кириан Мартин, который определил цели и задачи ведомства так: снижение числа кибератак на британские компании и решение проблемы нехватки квалифицированных кадров в сфере информационной безопасности. По инициативе Центра в британских школах проводятся уроки кибербезопасности, на которых ищут будущих экспертов для защиты королевства от хакерских атак.

На пятилетнюю Национальную школьную программу правительство Великобритании планирует потратить до 20 млн фунтов. В рамках этой программы будут отобраны несколько тысяч учеников в возрасте от 14 до 18 лет, которые хотят связать свою жизнь с информационной безопасностью, а остальные, прошедшие обучение, станут просто гражданами, но уже образованными в сфере ИБ.

Центр национальной кибербезопасности предлагает 11–14-летним школь-



Соревнования CyberFirst Girls Competition в Lancaster House в Лондоне (фото: www.ncsc.gov.uk)

никам и их родителям, опекунам и учителям записаться на однодневные курсы, 14–15-летним подросткам — на пятидневный вводный курс по ИБ, где они получают базовые знания и понятия по защите компьютеров и небольших сетей. А для ребят 15–16 лет, желающих в перспективе углубленно изучать информатику, разработаны пятидневные курсы, на которых студенты узнают об основных угрозах кибербезопасности для устройств, приложений и программного обеспечения, а также о способах их защиты. Курсы бесплатные и проходят в летний период в учебных заведениях по всей стране. Записаться могут как мальчики, так и девочки, но для девочек, кстати, есть специализированные женские курсы.

Любопытно, что привлечение женщин в сферу ИБ — это отдельный пункт программы. В Великобритании проводятся конкурсы для девушек 13–15 лет CyberFirst Girls Competition. Девичьи команды в составе четырех человек по всей стране решают тесты на логику, кодирование, создание сетей и криптографию. Десять самых сильных команд встречаются в очном поединке в Лондоне. Победители получают компьютерное оборудование для своей школы стоимостью 1000 фунтов, а каждая из девушек награждается ценным призом. Таким образом Центр хочет привлечь девушек на работу в сферу ИБ. По оценкам экспертов, среди специалистов ИБ, например, в США уже работают до 10% женщин.

Англичане, предлагая ввести кибербезопасность в Национальную школьную программу, не стали первооткрывателями ИБ-направления в средних учебных заведениях. Подобные программы давно работают в Израиле, однако в Европе они все же мало распространены.

Очень интересны инициативы на местах. Например, государственная общеобразовательная школа «Академия Кайл» в шотландском городе Эйр в сотрудничестве с Полицией Шотландии организовала курс информационной безопасности. Полицейские, предоставляя школьникам реальные исследования в области киберпреступности и рассказывая о конкретных случаях интернет-вымогательства в регионе, десять недель учили детей как со всем этим бороться. Главным условием занятий было то, что дети обо всем, что узнали, рассказывают дома, а по результатам обучения экзаменуют своих родственников. Так папы, мамы, дедушки и бабушки в городе Эйр и его окрестностях узнали, что пароли к сетевым ресурсам интересны не только друзьям. За счет того, что школьники познакомились с правилами кибербезопасности родных и знакомых, эффект от курса многократно увеличился. А учитывая тот факт, что это малонаселенный район, где нет отделений банков и жители пользуются исключительно онлайн-банкингом, польза от таких занятий была значительной.

Как тут не вспомнить регулярные SMS и звонки мошенников нашим пен-

сионерам, после которых старики сами открывают киберпреступникам доступ к своим банковским счетам. Если бы внуки рассказали им о том, чему их учат на уроках по защите информации, таких случаев могло быть меньше. Но, к сожалению, у нас нет таких уроков и тем более таких домашних заданий.

КОЛЛЕДЖИ

Следующая ступень образования — колледжи — наследники ПТУ и техникумов. С некоторых пор в них появилось новое направление обучения: «информационная безопасность». Разработаны Федеральные государственные образовательные стандарты. В зависимости от того, после какого класса абитуриент поступает в колледж, он учится 3 или 4 года и по окончании получает специальность «техник по защите информации». Многие колледжи предлагают очную, очно-заочную и заочную формы обучения.

Помимо базовых предметов школьной программы (для тех, кто пошел в колледж после 9 класса) студенты изучают основы многих технических и экономических дисциплин. В целом программа обучения по специальностям среднего профессионального образования в ИБ во многом схожа с программой подготовки инженерных кадров в вузах. Студентов учат эксплуатировать подсистемы безопасности автоматизированных систем, применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах, применять инженерно-технические средства обеспечения информационной безопасности.

В отличие от бесплатного обязательного среднего образования, среднее профессиональное может обойтись родителям студента в приличную сумму, если абитуриент не пройдет по конкурсу на бюджетное место. Число поданных заявлений зависит от популярности колледжа, в некоторых конкурсах составляет 2–3 человека на место. Стоимость обучения по программам Среднего профессионального образования по направлениям ИБ на коммерческой основе в ряде колледжей не на много отличается от стоимости образования в ведущих вузах и составляет до 120 тыс. рублей в год при дневной



Получатели стипендии по кибербезопасности US Bank (фото: nkytribune.com)

форме обучения или порядка 35–60 тыс. для заочников.

И самое поразительное. Несмотря на спрос со стороны студентов, не все колледжи, имеющие лицензию на направление ИБ (а таких порядка 90), открывают прием абитуриентов. Многие фактически не рекламируют кибербезопасность как направление обучения. И второе: спрос на технику со стороны работодателей минимален, несмотря на то, что учебные программы подготовки специалистов среднего звена создавались с участием профильных компаний и госструктур.

Среди вариантов продолжения образования для техников по защите информации — обучение в вузе по профильной специальности. Тем более, что многие колледжи являются факультетами университетов или работают в тесном сотрудничестве с ними.

А КАК У НИХ?

Схожие программы подготовки есть и в западных колледжах. Так, в США широко распространена система двухлетней подготовки (от 4 до 7 семестров) специалистов в области ИБ по различным направлениям — от базовых основ кибербезопасности и сетевой безопасности до подготовки в специфических областях, например, в области компьютерной или судебной криминалистики. Как правило, первый год посвящается теоретической подготовке, а второй — наработке практических навыков со

специализацией в более узком направлении деятельности. Итогом обучения становится сертификационный экзамен, многие колледжи предлагают продолжение обучения на степень бакалавра в дружественном университете, дополнительную стажировку для наработки навыков практической работы в крупных компаниях.

Главное требование к претенденту — законченное среднее образование. Некоторые колледжи проводят вступительные экзамены, многие ведут круглогодичный прием абитуриентов и обучают онлайн. В некоторых колледжах есть и ограничения: претенденты на будущую работу в области кибербезопасности систем здравоохранения должны пройти проверку на благонадежность и иметь базовые знания в области IT.

Как указывают разные источники, в США подготовку младших специалистов по компьютерной безопасности или обеспечению сохранности информации ведут около 100 колледжей. Выпускники продолжают учебу в университетах или идут работать по специальности: спецслужбы и профильные министерства и ведомства активно нанимают на работу таких специалистов.

ВЫСШЕЕ ОБРАЗОВАНИЕ

В начале 2000 г. российские вузы готовили 2000 специалистов в области ИБ, в 2019 г. — более 7000. Только в 2016 г. по всем направлениям ИБ в госуниверситеты на бюджет было принято поч-

ти 4400 студентов, средний проходной балл превысил 70. Еще порядка 1450 человек подали документы на обучение на коммерческой основе.

По данным на 2018 г. в России лицензии на обучение по семи профессиональным образовательным стандартам по направлению «информационная безопасность» имеют 170 университетов.

Образовательные профстандарты удовлетворяют потребности значительной части индустрии ИБ, учитывая как государственные, так и коммерческие интересы. По запросам банковского сообщества Федеральное учебно-методическое объединение организует обсуждения новых образовательных программ, способствует их оптимизации и выносит на утверждение в министерство. Для бакалавриата выделен профиль «информационно-аналитические системы финансового мониторинга», который напрямую связан с кредитно-финансовой сферой, нормативы стандартов позволяют специализироваться на конкретных профессиональных областях по многим «широким» профилям образования в области информационной безопасности.

Одновременно с актуализацией образовательных стандартов идет развитие базовых кафедр. Такую работу в ряде ведущих университетов ведет Банк России, будет создавать свои кафедры Сбербанк и другие крупные организации. Многие компании, мировые эксперты в области защиты информации, открывают свои кафедры в региональных и федеральных университетах или приглашают студентов на практику. Например, по этому пути пошли Лаборатория Касперского, InfoWatch, Mail.Ru Group... Свои Академии открыли или планируют открыть Yandex, Центробанк, Сбербанк...

Лидерами в области подготовки кадров по направлениям информационной безопасности в России являются МГУ им. Ломоносова, МФТИ, Санкт-Петербургский ИТМО, МИФИ, МГТУ им. Баумана, Уральский федеральный и Ярославский госуниверситеты.

А КАК У НИХ?

В мире признанными лидерами среди технических университетов, где из-

учают компьютерные дисциплины, в т.ч. и информационную безопасность, считаются университеты США, Европы, Китая, Южной Кореи, Австралии, Японии. По данным рейтинга Times Higher Education 2016 г., пятерку лучших возглавляет Швейцарская высшая техническая школа Цюриха, далее следуют Калифорнийский Технологический университет в Пасадене, известный как лидер в области математики и компьютерных технологий, Университет Оксфорда, Массачусетский Технологический институт и Технологический институт Джорджии. В сотне лучших есть и два российских университета: МГУ (43 место) и Санкт-Петербургский ИТМО (56 место).

Казалось бы, имея в активе 170 университетов и систему среднего профобразования, за 4–6 лет можно получить несколько тысяч хорошо подготовленных молодых специалистов. Однако на различных конференциях по кибербезопасности мне не раз приходилось слышать жалобы работодателей на слабо подготовленные и не всегда профпригодные молодые кадры. Это связано и с общими проблемами в области образования, и с трудностями в профориентации молодежи, которая представляет свою будущую работу, не исходя из реальности, а скорее по кинофильмам — как лихо закрученный приключенческий боевик. И потому сегодня крупные работодатели предпочитают брать на работу уже опытных сотрудников, пусть и с непрофильным образованием.

ПОВЫШЕНИЕ КВАЛИФИКАЦИИ

Помимо университетов в России действуют более 40 учебных центров по подготовке и переподготовке специалистов по защите информации. Часто они кооперируются с университетами или созданы на базе крупных компаний-интеграторов. Постоянное повышение квалификации — это требования нового законодательства и профстандартов. Программы дополнительного образования согласуются с регуляторами и в отличие от университетских программ, что вполне закономерно и оправдано, быстрее и чаще актуализируются.

При желании специалист может сам или на курсах подготовиться к сдаче эк-

заменов на международные сертификаты. С принятием федерального закона процесс создания центров национальной сертификации заметно активизировался.

А КАК У НИХ?

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

* * *

Подводя итоги, хочу отметить, что в России к вопросам обучения и подготовки кадров в области информационной безопасности подошли основательно. Система построена с участием профессионального сообщества. Как любая структура государственного масштаба она неповоротлива, работает с некоторым запаздыванием, однако она действительно сомасштабна стоящим перед ней задачам, стабильна и готовит новые кадры безопасников для всех отраслей народного хозяйства. Есть все основания надеяться, что как только будет определено оптимальное время реагирования на изменившуюся ситуацию в области кибербезопасности, будет обеспечена и быстрая адаптация к новым требованиям учебных программ. И никто больше не сравнит наше образование в сфере ИБ с человеком, бегущим за уходящим трамваем.

Вопрос за малым — правильно ориентировать и заинтересовывать молодежь, начиная со средней школы.

КТО ДЕЛИТСЯ ЗНАНИЯМИ?

КАФЕДРЫ ИБ ПО ПРЯМЫМ ДОГОВОРАМ
РАСТУТ КАК ГРИБЫ ПОСЛЕ ДОЖДЯ

Часто, выступая на конференциях по информационной безопасности, представители компаний жалуются на нехватку квалифицированных кадров и рассказывают, что их организации вынуждены заключать прямые договоры с профильными кафедрами вузов. Ректоры вузов обычно поддерживают такие предложения, рамочные соглашения действительно заключаются, все счастливы... Но как на самом деле обстоят дела в этой сфере? Ведь иногда в частной беседе руководители компаний и вспомнить не могут, где они читают лекции или ведут семинары, а в службах по работе с персоналом понятия не имеют, сколько подготовленных специально для их компании молодых специалистов пришли к ним на работу.

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Академическая партнерская сеть «Лаборатории Касперского» охватывает традиционно сильные в области подготовки специалистов по ИБ московские и петербургские вузы, а также крупные федеральные университеты в Казани, на Дальнем Востоке, Южном Урале, а также университеты в Казахстане.

К этому ЛК постоянно открывает свои базовые кафедры в региональных вузах. Из последних новостей: появилась информация о намерении ЛК открыть базовую кафедру на факультете математики и информационных технологий Северо-Осетинского государственного университета (СОГУ) им. Коста Хетагурова. Открытие планируется в рамках соглашения о сотрудничестве в сфере

образования, подписанного Евгением Касперским и ректором университета Аланом Огоевым. Основными задачами новой структуры станут подготовка специалистов и реализация научно-исследовательских проектов в области защиты информации. На кафедре будет вестись работа по учебной и научной деятельности, а также по внеклассной работе со студентами.

В ноябре 2017 г. ЛК открыла в Чувашском госуниверситете им. И. Н. Ульянова Научно-образовательный центр информационной безопасности в электроэнергетике. На базе центра осуществляется подготовка специалистов международного уровня, а также проводятся научные исследования в сфере ИБ. Теперь процесс обучения студентов технических специальностей университета дополнен дисциплинами, отражающими самые современные тенденции индустрии кибербезопасности.

Ранее аналогичные центры были открыты в Дальневосточном федеральном университете и в Московском техническом университете связи и информатики (МТУСИ), в Южно-Уральском госуниверситете в Челябинске. Ожидается, что в сентябре 2018 г. на базе центров начнется подготовка магистров по направлению ИБ.

В рамках просветительских акций во многих университетах проходят конференции Kaspersky Security Day, на которых представители компании знакомят студентов и всех заинтересованных с современными технологиями защиты информации и возможностями их применения для предотвращения негативных последствий кибератак. Также прово-

дятся командные стратегические бизнес-игры Kaspersky Interactive Protection Simulation, которые позволяют на практике смоделировать процессы управления ИБ в АСУ ТП Электростанции.

Для студентов этих вузов организованы стажировки KasperskySafeBoard, а выпускники бакалавриата могут принять участие в добровольном квалификационном экзамене выпускников по ИБ, который проводит Рособрнадзор совместно с ЛК и IT-компаниями.

Но ЛК — это не только защита информации, но и крупный бизнес. В мае 2018 г. в Москве при поддержке бизнес-инкубатора НИУ ВШЭ прошла весенняя школа HSE Start Up School. Участниками проекта стали школьники, студенты и специалисты в области интернет-предпринимательства. За 11 дней экспресс-подготовки в HSE Start Up School студенты получили знания и навыки работы в области интернет-предпринимательства, маркетинга и медиакоммуникаций и теперь знают многое о важных этапах, которые необходимо пройти стартапу: от бизнес-идеи до реальных инвестиций.

Практическим результатом обучения стали прототипы работающего продукта в сфере интернет-предпринимательства (приложение, веб-сервис и т.д.), а победители соревнования по итогам презентации проекта получили возможность заработать первые средства для его реализации, резидентство в бизнес-инкубаторе ВШЭ и консультации с трекерами инкубатора.

INFOWATCH

В Высшей школе экономики работает и другая компания, специализирующаяся на ИБ. Базовая кафедра АО InfoWatch была создана в МИЭМ НИУ ВШЭ для организации и проведения занятий ведущими специалистами-практиками в сфере корпоративной защиты от внутренних угроз, защиты от хакерских атак на веб-ресурсы организаций, защиты в сфере Интернета вещей. Сотрудники

**МНОГИЕ КОМПАНИИ РАБОТАЮТ
В ОСНОВНОМ С МОЛОДЫМ
ПОКОЛЕНИЕМ, А INFOWATCH СОЗДАЛА
ЕЩЕ И СПЕЦИАЛЬНЫЙ КУРС ОБУЧЕНИЯ
ДЛЯ ПРЕПОДАВАТЕЛЕЙ ВУЗОВ**

компания, включая руководство, проводят занятия в целях профессиональной ориентации студентов; разрабатывают и читают специальные курсы, проводят семинары, в которых отражают последнюю информацию по наиболее актуальным вопросам направлений современных исследований в области ИБ.

Еще один вуз, где работает АО InfoWatch — Университет ИТМО, где в январе 2018 г. был открыт учебный центр «ИТМО–Инфовотч». В специализированном компьютерном классе студенты учатся работе с аналитическими системами ИБ-компаний.

Многие компании работают в основном с молодым поколением, а InfoWatch создала еще и специальный курс обучения для преподавателей вузов и других учебных заведений. В рамках курса слушатели узнают о методиках защиты корпоративной информации от внутренних угроз, применении решений компании для противодействия внутренним угрозам, получают практический опыт внедрения подобных решений в различных организациях и знакомятся с практикой правоприменения.

АКАДЕМИЯ CISCO

Cisco — еще одна компания, которая активно работает со студентами и школьниками и помогает готовить будущих специалистов в сфере ИТ и ИБ. Сегодня в России открыто 500 академий Cisco при школах, колледжах и вузах. Учебный процесс основан на смешанной модели обучения, где наряду с традиционной подачей материала учителями применяются технологии дистанционного обучения на базе системы Cisco NetAcad.

Примером удачного сотрудничества Cisco с региональными вузами является кафедра «Закрытые системы связи» Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича. Региональная сетевая академия Cisco на Северо-Западе России была открыта на базе этой кафедры в далеком 1999 г., а в 2012 г. в учебной программе появилось такое направление подготовки бакалавров как «Информационная безопасность». Студенты, обучающиеся на курсе, получают необходимые знания и умения, позволяющие им при желании сдать экзамен на международный сертификат Cisco.



Подписание положения о стипендиальной программе АО «ИнфоВотч» директором МИЭМ НИУ ВШЭ Круком Е.А. и президентом ГК «ИнфоВотч» Касперской Н.И. Источник: miem.hse.ru

И ДРУГИЕ...

Решить проблему качественной подготовки будущих специалистов в области ИБ стараются многие университеты. Недавно НИУ МАИ и компания «Выштех», представляющая в России израильскую школу ИБ и IT HackerU, заявили о запуске совместных образовательных программ по информационной безопасности. В рамках курса «Профессиональный пентестинг» эксперты HackerU расскажут студентам об этичном хакинге, поиске уязвимостей, безопасности приложений и др. А осенью в МАИ откроется магистерская программа «Кибербезопасность и инфокоммуникации», включающая в себя расширенные курсы в области пентестинга и компьютерной криминалистики.

В Тюменском госуниверситете открылась кафедра безопасности информационных технологий умного города. Кафедра создана в Институте математики и компьютерных наук совместно с компанией «Техносерв А/С», занимающейся научными исследованиями и разработками в области естественных и технических наук. К учебному процессу, который начнется осенью, привлекут ведущих преподавателей университета и специалистов компании-партнера, практиков из других организаций сферы науки и бизнеса, а также сертифицированных специалистов по ИТ и ИБ. Обучение на кафедре

будут вести по программам бакалавриата, специалитета, магистратуры и аспирантуры.

Для формирования и закрепления практических навыков на кафедре планируют создать специальную лабораторию. Студенты и аспиранты смогут заниматься проектной и производственной деятельностью, востребованной мегаполисом. Уже ведется работа над двумя проектами: экономия тепла в университете (при удачном решении опыт распространят на весь город) и телемедицина, профилактика здоровья человека и скрининг на расстоянии.

В этом году на направление информационной и компьютерной безопасности в ТюмГУ выделено 75 бюджетных мест, всего планируется набрать 150 студентов.

Ежегодно российские вузы выпускают несколько сотен молодых специалистов по ИБ. И не все они, получив диплом, понимают, чем будут заниматься в жизни. Хочется надеяться, что работа как перечисленных, так и не упомянутых в обзоре ИТ-компаний по созданию профильных кафедр и учебных центров принесет свои плоды, и проблема нехватки квалифицированных кадров в сфере ИБ будет решаться эффективнее.



Дмитрий ЛАРИН
кандидат технических наук, АО «Лаборатория «СКАТ»

ДРЕВНЕРУССКИЕ ШИФРЫ

ПЕРИОДИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В РОССИИ.
ЧАСТЬ 2

Продолжаем рассказ о первом периоде (IX век — 1549 год) отечественной истории криптографии. Эта статья посвящена системам шифрования, применявшимся в XIV–XVI веках.

ЛИТОРЕЯ — ЦАРИЦА ШИФРОВ

Основной русской системой шифрования стал шифр простой замены, называвшийся «литорея». Существовало две разновидности этого шифра: «простая литорея» и «мудрая». «Простая литорея» предполагает замену большинства согласных букв кириллицы на другие, взятые из того же алфавита, причем замену производят по определенному правилу. Гласные буквы и некоторые согласные (Й, Ъ, Ь) остаются без изменений. Самым простым и распространенным был следующий ключ. Выписывали в строку подряд все согласные в количестве 10 букв. Под этой строкой составляли вторую из последующих 10 согласных, но их записывали в обратном порядке, то есть справа налево:

Б В Г Д Ж З К Л М Н
Щ Ш Ч Ц Х Ф Т С Р П

Замена производилась следующим образом: буква из верхней строки заменялась на соответствующую ей букву из нижней строки, и наоборот. Расшифрование осуществлялось таким же образом.

Для примера воспользуемся фрагментом Ермолинской летописи, датированной 1463 годом, в нем рассказывается о некоем жестоком княжеском слуге: «А прочих его чудес великое множество, невозможно ни описать, ни исчислить — потому что он во плоти есть **ЦЪЯШОС** (выделено авт.)». Расшифровывая последнее слово по вышеприве-

денному ключу получаем: **ДЪЯВОЛ**. Летописец, очевидно, монах, зашифровал это слово, чтобы не поминать нечистого всуе. Замена только согласных букв, осуществлялась для упрощения использования шифра. Вообще согласные в русском языке несут больше информации, чем гласные. Приведем пример. Возьмем некоторое слово и выпишем только гласные, пропущенные согласные обозначим точками:

.А.Я..А

Понять что здесь написано весьма затруднительно, а теперь сделаем наоборот (оставим только согласные):

П.М.Т.К.

— очевидно, что это **ПАМЯТКА** или **ПОМЕТКА**.

Самый древний документ, содержащий зашифрованный простой литореей фрагмент, известный на сегодня, датируется 1229 годом. Наиболее широкое распространение этот шифр приобрел в XIV–XV веках, хотя продолжали использовать его еще и в XVIII веке. Су-

ществовали усложнения «простой литореи», когда буквы верхней и нижней строк располагались в случайном порядке.

В «мудрой литорее» замене подлежали все буквы алфавита и гласные и согласные. Таким образом, эта система представляла собой классический шифр простой замены [Бабаш, 2002], [Соболева, 2002].

НЕМНОГО АРИФМЕТИКИ

Также на Руси были распространены цифровые или счетные системы шифрования. Еще их называли «фиоть» или «хвиоть». Цифры в древней Руси записывались с помощью букв кириллицы и греческого алфавита (рис. 1). Чтобы указать, что буква означает цифру или число, а не звук над ней ставили особый знак ~, который назывался «титло».

Система основана на использовании определенных букв кириллицы, имеющих известное цифровое значение. Такие буквы-цифры для тайнопи-

ⷰ	ⷱ	ⷲ	ⷳ	ⷴ	ⷵ	ⷶ
аз	вѣди	глагѡль	добро	ѡсть	зѡло	земля
1	2	3	4	5	6	7
ⷷ	ⷸ	ⷹ	ⷺ	ⷻ	ⷼ	ⷽ
иже	фита	и	како	люди	мыслѣте	наш
8	9	10	20	30	40	50
ⷾ	ⷿ	ⷰ	ⷱ	ⷲ	ⷳ	ⷴ
кси	он	покой	червь	рцы	слово	твердо
60	70	80	90	100	200	300
ⷿ	ⷰ	ⷱ	ⷲ	ⷳ	ⷴ	
ук	ферт	ха	пси	от	цы	
400	500	600	700	800	900	

Рисунок 1. Буквенные обозначения цифр и чисел [Бабаш, 2002, с. 202]

си раскладывали на слагаемые, обычно «раздваивая», в результате чего вместо одной буквы-цифры записывали две. Например, буква «Д» имела известное значение «4», а после «раздвоения» записывалась двумя буквами, из которых каждая была равна точно половине преобразуемой буквы, например, писали рядом две буквы «ВВ», каждая из которых означала «2» (т.е. $2+2$). Так поступали при зашифровке четных букв-цифр.

Для нечетных применяли пары приближенных половинок. Например, вместо буквы «Е» (5) писали «ГВ» (т.е. $3+2$). При этом буквы, не имеющие числового значения, не шифровались. В последствии числовое значение буквы стали разбивать на произвольные слагаемые, причем не на два, а на большее количество. Например, буква С=6, помимо традиционного ГГ, могла представляться как АЕ ($1+5$), АВГ ($1+2+3$) и т.д. В результате получается простейшая система многозначной замены. При этом очевидно, что чем больше числовое значение буквы, тем большим количеством вариантов она может быть представлена в зашифрованном тексте [Бабаш, 2002, с. 204].

С помощью такого шифра увековечил свое имя в 1307 году писец Домид, приписав к написанной в Пскове книге «Апостол» зашифрованный текст (для удобства «титло» над буквами-цифрами опущено, а незашифрованное начало фразы переведено на современный русский язык): «а писал ВВ.МЛ.КК.ДД. ВВ.Ъ.рекше: двдъ, органъ, мысль, истина...» (последнее слово из-за порчи листа рукописи не читается) [Соболева, 2002, с. 37].

Ко второй части этой записи мы вернемся чуть позже, а пока расшифруем первую: $ВВ=2+2=4=Д$, $МЛ=40+30=70=О$, $КК=20+20=М$, $ДД=4+4=8=И$, $ВВ=2+2=4=Д$, таким образом мы получаем имя писца Апостола 1307 года: ДОМИДЪ. [Симон, 1977], [Соболева, 2002].

Другим вариантом цифровой тайнописи являлся так называемый описательный, примером его применения может служить текст XV века: «Аще хочещи уведати имя писавшего книгу сию, и то ти напишю: «Десятерица сугубая и пятерица четверицею и единъ; десятирица дващи и единъ, де-

сяття четыре сугубо и четырежди по пяти; дващи два с едином; единица с четверицею сугубо; в семь имени словъ седмирица, три столпы и три души, царь». И сего числа в семь имени РОЕ» [Бабаш, 2002, с. 205]. Расшифруем эту тайнопись. Слово «сугубо» в те времена было синонимом слова «дважды». Таким образом: «десятерица сугубая и пятерица четверицею» — это $10 \times 2 + 4 \times 5 = 40 = М$; «единъ» — это $1 = А$; «десятерица дващи» — $10 \times 2 = 20 = К$; «единъ» — это опять $1 = А$; «десяття четыре сугубо и четырежди по пяти» — $10 \times 4 \times 2 + 4 \times 5 = 100 = Р$; «дващи два с едином» — $2 \times 2 + 1 = 5 = Е$; единица с четверицею сугубо $(1 + 4) \times 2 = 10 = І$ (или в современной транскрипции Й). Тогда имя автора МАКАРЕЙ.

Далее следует своеобразный проверочный код: букв в слове 7 столпы и души, означают гласные и согласные, которых в слове по 3, а царь это гласная Й, и наконец РОЕ — это 175 — сумма букв-цифр в слове.

Иногда зашифрованные записи носили шуточный характер, как, например в обрывке берестяной грамоты XIII века, найденной в Новгороде [Бабаш, 2002, с. 205]:

Н В Ж П С Н Д М К З Л Т С Ц Т...
Е Ъ Я И А Е У А А А Х О Е И А...

Если прочитать это сообщение по колонкам, то получаем следующий текст: НЕВЪЖЯПИСАНЕДУМАКАЗАЛХТОСЕЦИТА... Если адаптировать эту фразу к современному русскому языку, получится:

НЕВЕЖДА ПИСАЛ НЕ ДУМАВ
СКАЗАЛ А КТО С ИЕ ЧИТА (Л)...

...далее очевидно следовал не лестный отзыв об умственных способностях читателя. Для нас этот фрагмент важен тем, что это один из первых случаев применения на Руси шифра перестановки, пусть и в самой примитивной форме.

ПОЭЗИЯ НА СЛУЖБЕ КРИПТОГРАФИИ

Самым древним способом сокрытия информации в текстах, использовавшимся на Руси был акростих. Акростих (от греч. *akros* — крайний и *stichos* — строка) — стихотворение, в котором первые буквы строк образуют слово или фразу. Примером акростиха может

служить стихотворение «Загадка акростишная» русского поэта Ю.А. Нелединского-Мелецкого (1752–1829):

*Довольно именем известна я своим;
Равно клянется плут и непорочный им;
Утехой в бедствии всего бываю боле;
Жизнь сладостней при мне и в самой
лучшей доле.*

Блаженству чистых душ могу служить одна;

А меж злодеями — не быть я создана.

Если прочитать первые буквы строк сверху вниз, то получится «секретное» слово ДРУЖБА. Изобретателем акростиха считается известный древнегреческий комедиограф, философ и врач Эпихарм Сиракузский (примерно 550–460 годы до н. э.). На Русь акростих пришел из Византии и начал широко применяться с XI века, получив множество наименований: началостроиче, началограние, краеграние, акростихиада, краеэстроиче, первобуквие и др. Акростих широко применялся поэтами, авторами и переписчиками книг, составителями надгробных эпитафий, в основном для увековечивания своего имени. В.И. Даль называл акростих именишием [Соболева, 2002].

Применялся акростих и как средство защиты информации. Фактически применение акростиха можно отнести к стеганографическим методам защиты информации. На слух акростихи не воспринимаются. Чтобы их обнаружить, нужно написанное читать. Читающий заранее знает о существовании в тексте тайнописи, хотя в принципе ее можно обнаружить и случайно.

Древнерусские акростихи отличаются большим разнообразием. Известны многочисленные варианты тех или иных разновидностей акростихов. Так, чаще всего записи проявляются при чтении снизу вверх. Встречаются акростихи, в которых к обычной вертикальной записи добавляется целое слово или даже вся горизонтальная (верхняя или нижняя) строка, написанная открытым текстом, — это угловые акростихи. Можно сказать, что у наших книжников акростихи были излюбленным видом тайнописи. Посредством акростихов велась тайная деловая и личная переписка.

Для защиты информации широко применялись «неправильные акро-

стихи». Такое название они получили потому, что записывались не только первыми буквами строк, но и двумя и более буквами, начинающими строки, и даже первыми слогами и словами строк. Ясно, что такая свобода действий существенно облегчала сочинителю составление весьма пространных тайнописных записей. Но вместе с тем такой произвольный подбор делает невозможным найти какую-то закономерность в чередовании читаемых букв, слогов и слов. Случайность чередования этих элементов исключает возможность правильно составить универсальный ключ. Иными словами, для каждой конкретной записи читающий должен иметь тот ключ, которым эта запись составлялась. То есть это уже криптографическая система защиты информации.

Приведем пример «неправильного акrostиха». Иоанн Величковский (XVII век) составил различные тайнописи с именем Девы Марии. Одна из них умещается на шести строках (имя Мария повторяется 2 раза и выделено заглавными буквами):

МАти блага,
РИза драга-
Я же нас крыет,
МАлодушных,
РИзо нужны,
Якъ руно греет.

Здесь выделенные буквы или слоги в строках читают слева направо и сверху вниз. При этом первая буква третьей строки (Я) является не началом, а окончанием слова (драга/я).

Авторству Величковского принадлежит и более сложная запись, когда буквы «секретного сообщения» располагаются в произвольном порядке и перемешаны между собой:

МногАя Из неСУщих Созда
сей
твоРенИЯ
даДЕ
ми ХеРуИмСкую
ТОму
пеСнь хВАления.

Здесь зашифрованы два имени: Мария Дева (выделено заглавными буквами и курсивом) и Иисус Христос (выделено заглавными буквами и жирным шрифтом). Очевидно, что прочесть такую тайнопись, не зная ключа, крайне сложно.

Помимо стихотворений для сокрытия сообщений использовались и обычные тексты (принципы тайнописи те же, что для стихотворений) и даже бессмысленные наборы слов.

Вернемся к зашифрованной приписке к Псковскому Апостолу 1307 года. Если взять первые буквы четырех последних слов, то получаем ДОМИ, последнее нечитаемое слово, совершенно очевидно начиналось на Д, таким образом, и здесь получаем имя Домид. Переписчик зашифровал свое имя двумя способами — цифровой тайнописью и акrostихом [Бабаш, 2002], [Гогешвили, 1991], [Панченко, 1973], [Соболева, 2002].

ЯМСКАЯ ГОНЬБА НА СЛУЖБЕ ОТЕЧЕСТВУ

Эффективная организация связи помогла одержать свои знаменитые победы Александру Невскому и Дмитрию Донскому.

В 1239 году новгородский князь Александр Ярославич, после описываемых событий получивший почетное прозвище Невский, организовал морские дозоры в Финском заливе и на реке Неве с целью предупреждения нападения с Запада. В начале июля 1240 года один из дозоров обнаружил в устье Невы шведские корабли, выяснил место высадки, состав сил врага и с помощью ямской гоньбы послал тайное сообщение в Новгород: «уведав силу ратных, иде против князя Александра, да скажет ему стань» [Кудрявцев, 2002, с. 75]. 15 июля 1240 года в месте впадения реки Ижоры в Неву произошла знаменитая Невская битва, в которой князь Александр наголову разгромил шведских агрессоров.

После поражения на Неве шведы прекратили на время атаки на Русь, но Новгородское княжество постоянно пробовали на прочность немецкие рыцари-крестоносцы, окопавшиеся в Прибалтике. После захвата немцами Пскова для Новгорода возникла реальная угроза. В начале 1242 года Александр Невский начал собирать войска для сражения с Тевтонским орденом и опять тайные вести о сборе войск передавались ямской гоньбой. Внезапным ударом Александр освободил Псков, однако главные силы крестоносцев еще не вступили в бой. Хорошо поставленная

разведка и надлежащим образом сработавшая система связи (ямская гоньба) предоставили Александру информацию о противнике, что позволило выработать наилучшую тактику для предстоящего сражения. Оно состоялось 5 апреля 1242 года на льду Чудского озера и получило название «Ледовое побоище». Крестоносцы потерпели тяжелое поражение. Эта победа на долгие годы приостановила экспансию крестоносцев на Восток [Астрахан, 1996], [Кудрявцев, 2002].

Важнейшую роль система разведки и связи сыграла во время подготовки Куликовской битвы. Московский князь Дмитрий Иванович (после победы на Куликовом поле ставший Дмитрием Донским) еще в начале 1370-х годов организовал целую систему защиты границы Московского государства (проходившую тогда по реке Оке) от нападений ордынцев. Она включала в себя «сторожи крепкие», «заставы», которые выдвигались далеко в степь для наблюдения за передвижениями ордынских войск, пограничные крепости (Коломна, Серпухов и др.), а также организацию связи с этими отрядами при помощи особых посыльных, а с крепостями при помощи ямской гоньбы. Для быстрой и эффективной мобилизации войска Д. Донской приказал учредить разрядные книги, «подробные росписи полков и воевод, благодаря которым были точно известны районы мобилизации, а также состав и численность участников похода» [Кудрявцев, 2002, с. 109].

23 июля 1380 года в Москву прискакал «сторож крепкий» Андрей Попов, сын Семенов, и сообщил: «Идет на тебя, государь, царь Мамай со всеми силами ордынскими, а ныне он на реке на Воронеже» [Кудрявцев, 2002, с. 109]. После получения этой информации по всей Руси по ямским трактам полетели гонцы с секретными грамотами Московского князя о сборе войск для отражения ордынского нашествия. С целью выяснить дальнейшие планы врага выиграть время для сбора войск князь Дмитрий послал к Мамаю «юношу, доволна суца разумом и смыслом, именем Захарию Тютышова» [Кудрявцев, 2002, с. 109]. Захарий должен был вручить Мамаю большие дары и начать переговоры с ордынцами, пытаясь

убедить их в покорности Московского князя хану. Для переговоров вместе с Тютчевым были посланы «два толмача, умеюща языкъ половециский» [Кудрявцев, 2002, с. 109]. По пути в Орду Тютчев получил информацию об измене рязанского князя Олега и союзе с Мамаем литовского князя Ягайло. Эта важнейшая информация была доведена до князя Дмитрия — Захарий «пославъ скоро вестника тайно к великому князю» [Кудрявцев, 2002, с. 109]¹.

Получив это сообщение, князь Дмитрий решает нанести удар по Мамаю до соединения его полчищ с войсками Олега и Ягайло. Тем временем передовая стража продолжала наблюдение за основными силами Мамаея, подтверждая, что хан не торопится идти на Москву, кочует у реки Воронеж, ожидая подхода союзников. В середине августа 1380 года русские войска собрались в Коломне и оттуда форсированным маршем двинулись на встречу врагу. Движение войска сопровождалось постоянным получением информации о противнике от «сторожи» и специально высланных для разведки передовых от-

рядов. Благодаря грамотной организации разведки и связи князю Дмитрию с войском удалось раньше Мамаея прибыть на место предполагаемого сражения и занять более выгодную тактическую позицию, а также не допустить соединения ордынцев с войсками Ягайло и Олега. 8 сентября 1380 года на Куликовом поле состоялось знаменитое сражение, которое закончилось полной победой русского войска. [Астрахан, 1996], [Кудрявцев, 2002, с. 110–112], [Очерки, 1999].

ШИФРЫ И ПОЛИТИКА

Одним из немногих общественно-политических документов, где имеются зашифрованные фрагменты является «Второе послание митрополита Киприана 23 июня 1378 года». После кончины митрополита Алексия Киприан стремился занять высокий духовный пост в Москве. Против Киприана выступал московский князь Дмитрий Иванович. Киприан искал поддержки у игумена Троицкого монастыря Сергия Радонежского и игумена Симонова монастыря Федора. Понимая, что содержание послания может стать известным князю, Киприан во избежание неприятностей зашифровал отдельные части текста. Были сокрыты имя одного из адресатов (Сергия) и духовный сан другого (Федора), а также некоторые слова и предложения. Этот документ интересен тем,



Выступление русского войска на Куликовскую битву (миниатюра XV века)

что в нем обнаружено восемь мест, зашифрованных простой литереей, при этом использовались разные ключи!

* * *

Подведем итоги. В IX–XIV вв. на Руси использовались различные системы шифрования. Надежно организованная передача тайных сообщений помогла выиграть два из важнейших сражений в нашей истории — Ледовое побоище и Куликовскую битву.

ЛИТЕРАТУРА

- [Астрахан, 1996] Астрахан В. И., Гусев В. В., Павлов В. В., Чернявский Б. Г. Становление и развитие правительственной связи в России, Орел: ВИПС, 1996.
- [Бабаш, 2002] Бабаш А. В., Шанкин Г. П. История криптографии. Часть I. М.: Гелиос, 2002.
- [Гогешвили, 1991] Гогешвили А. А. Акростих в «Слове о полку Игореве» и других памятниках русской письменности XI–XIII веков. М., 1991. М.: Воениздат, 1984.
- [Кан, 2004] Кан Д. Война кодов и шифров. М.: РИПОЛ КЛАССИК, 2004.
- [Кудрявцев, 2002] Кудрявцев Н. А. Государево Око. Тайная дипломатия и разведка на службе России. М., ОЛМА-ПРЕСС, 2002.
- [Очерки, 1999] Очерки истории внешней разведки в 5 томах, под ред. Е. М. Примакова и С. Н. Лебедева, М., «Международные отношения», 1999.
- [Панченко, 1973] Панченко А. М. Русская стихотворная культура XVII века. Л., 1973.
- [Симонов, 1977] Симонов Р. А. Математическая мысль Древней Руси. М., 1977.
- [Словарь, 1984] Советский энциклопедический словарь. М., Советская энциклопедия, 1984.
- [Соболева, 2002] Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.
- [Сперанский, 1929] Сперанский М. И. Тайнопись в юго-славянских и русских памятниках письма. Энциклопедия славянской филологии. Вып. 3–4. Л., 1929.

«ДМИТРИЙ ФРАНЗБЕКОВ ЧЕЛОМ БЬЁТ...»



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

К 385-ЛЕТИЮ КРИПТОГРАФИЧЕСКОЙ СЛУЖБЫ РОССИИ

В августе нынешнего года исполняется 385 лет со времени создания двух известных документов, важных для истории отечественной криптографии. Один из них впервые регламентировал криптографическую деятельность в России, а второй стал первым учебным пособием по криптографии.

ПЕРВЫЕ ВЛАСТНЫЕ УКАЗАНИЯ

Напомним содержание регламентирующего указания в современном прочтении:

«Восьмого августа (по старому стилю, по новому стилю 18 августа — авт.) 1633 года Великий Государь Святтейший Патриарх московской и всея Руси Филарет Никитич дал написанные его рукой шифровальную азбуку и пример её использования думному дьяку Ивану Грязеву (главе Посольского приказа — авт.). Государь Святитель написал шифровальную азбуку для государственных и посольских тайных дел. Если понадобится государственным послам, посланникам или агентам писать о важных государственных делах, то им писать к Государям (царю и патриарху — авт.) непременно шифрованным письмом, чтобы содержание не стало известно в тех государствах».

Особенно следует подчеркнуть, что это распоряжение безусловно выполнялось. Оно сразу же было подкреплено административными мероприятиями, в частности, составлением пособия по тайнописи и обучением шифровальщиков, организацией особого тайнописного делопроизводства. Сохранившиеся

документы, регламентирующие работу с шифрами, свидетельствует не только о своей детальной проработке, но также и о наличии кадров, занятых такой деятельностью, и об их квалификации.

Есть ещё немало доводов в пользу признания 8 августа 1633 года датой рождения криптографической службы России. Политическая воля, силы и средства неуклонно применялись для использования возможностей криптографии в делах государственной важности. К середине века были созданы условия для того широкого распространения шифрованной связи, о котором свидетельствуют документы второй половины XVII столетия.

СКРОМНЫЙ УЧАСТНИК ИСТОРИЧЕСКИХ СОБЫТИЙ

Среди именитых авторов упомянутого выше первого учебного пособия по криптографии — патриарха Филарета и И. К. Грязева, скромно присутствует и Дмитрий Франзбеков. От его имени и его рукой написана часть текстов в пособии, он же стал первым из тех, кому довелось проверить эффективность этого пособия на практике.

Как мы знаем, Франзбеков стал вскоре первым постоянным представителем Русского государства в Швеции. Наш дальнейший рассказ будет связан с личностью и жизненным путём этого человека. Как представляется, идя по его следу, можно открыть для себя нечто новое в понимании истории нашего отечества середины XVII века.

Дмитрий Андреевич Франзбеков по своему происхождению был ливонским немцем, первоначально его зва-

ли Альфред Фаренсбах. Он поступил на русскую службу в 1613 году, вероятно, сперва послужив в польских войсках. В 1627 году Франзбеков принял православное крещение у патриарха Филарета и, будучи офицером, был записан в дворяне по московскому списку. В Подмоскovie ему выделили вотчинные земли. С апреля 1630 года Дмитрий Франзбеков служил воеводой в Яранске, городке-крепости на полпути от Казани до Вятки. Во время воеводства Франзбекова в Яранске размещался солидный гарнизон: две сотни стрельцов плюс два небольших отряда дворянской конницы и служилых людей из представителей народностей Поволжья. Кроме того, здесь же находились семь пушкарей с артиллерией. Общее число войск составляло около 250 человек, они и были основным населением Яранска. Размеренная гарнизонная жизнь у Дмитрия Андреевича продолжалась до 1633 года. Той весной, согласно документам, начался новый этап его службы — дипломатический.

ИЗ ТЫЛОВОГО ГАРНИЗОНА — НА ПЕРЕДНИЙ КРАЙ ПОЛИТИКИ

Как отмечают историки, в начале 30-х годов XVII века состоялось окончательное вхождение Русского государства в европейскую политику. К 1626–1628 годам руководство внешнеполитической деятельностью Московии перешло к патриарху Филарету. Понимая неизбежность войны с Польшей и учитывая слабость своих военных сил, он стремился к созданию коалиции против Польши. Международная обстановка давала та-



Иллюстрация 1. Карта Русского государства 1614 года

кой шанс. Это было время Тридцатилетней войны, разделившей Европу на два лагеря. В ту пору Польша примыкала к австро-испанской Габсбургской коалиции. Противники этого лагеря — Дания, Голландские штаты, Англия, Франция, Турция, Венгрия и особенно Швеция — активно пытались привлечь Русское государство на свою сторону.

Они нуждались в Московии и как в поставщике зерна. К 1626 году западноевропейские цены на хлеб выросли в 10 раз, а к 1628 году — в 20 раз. В результате многосторонних дипломатических переговоров к лету 1632 года был выработан союзный договор со Швецией о войне против Польши, близилось его подписание.

Как мы знаем, в августе началась русско-польская война, выросла потреб-

ность в оперативной информации и связи. Но ещё в августе 1632 года в Москве умер шведский резидент Мёллер и русская власть вполне ощутила его отсутствие. Информацию о шведских и европейских делах теперь сообщал губернатор Лифляндии Шютте, он принял предложение руководителя русской разведки И. Б. Черкасского и стал его агентом. По этому поводу И. Б. Черкасский высказался так: «...покамест прямой агент будет, кому в делах можно верить». Представляется, что под прямым агентом он имел в виду русского резидента, чьё постоянное жительство в Стокгольме по образцу пребывания шведского резидента в Москве, было уже согласовано дипломатами. Этим резидентом и предстояло стать Д. Франзбекову. Действительно, приказ об отправке Франз-

бекова резидентом в Стокгольм был издан 22 марта 1633 года.

Но события, как известно, развивались по другому сценарию. В ноябре 1632 года погиб король Густав-Адольф. Без короля шведское правительство воздержалось от начала войны с Польшей. Изменение обстановки задержало командировку Франзбекова в Швецию на полтора года, но она всё же состоялась. Причиной тому стало восстановление взаимного интереса после некоторого охлаждения отношений. Москве был необходим постоянный и надёжный источник информации о войне и европейских делах, прежде всего польских, а Стокгольм остро нуждался в возобновлении беспоплатных поставок русского зерна, прекращённых в 1634 году.

СВИДЕТЕЛЬСТВА УСЕРДНОЙ УЧЕБЫ

Франзбеков много тренировался в шифровании и даже участвовал в составлении учебного пособия по тайнописи. На илл. 2 представлен фрагмент листа из этого пособия Посольского приказа. Здесь рукой Франзбекова выписана зашифрованная им фраза: «господину ивану кнриловичю дмитреи франзбеков челомъ бьет». При этом использовался шифр, разработанный патриархом Филаретом [1].

Наконец, все дипломатические бумаги были согласованы и подписаны. В наказе Франзбекову поручалось не только вести официальные сношения со шведским правительством, но также «тайно проводывать от нарочитых людей, добрых и досужих, кому бы доверять можно, и у агентов разных земель, как с цесаревыми людьми войну ведут, чаять ли миру...». Самая значительная часть обширного наказа касалась польских и крымских дел.

Кроме этого наказа дан был еще тайный, который агенту приказали выучить наизусть в Москве. При составлении донесений царю, посол должен был использовать тайнопись. «А про те тайные дела и про затейное письмо (шифр) подъячей Иван Исаков и иной ни кто отнюдь не ведал, и чёрные отписки о тех тайных делах тем же затейным писмом держати у себя бережно, чтоб о тех о тайных делах и про затейное письмо опричь его Дмитрея подъячий Иван Исаков и иной никто однолично не проведаль». Наказ заканчивался следующим образом: «Да что он, Дмитрий, будучи в Свее (Швеции), по сему тайному наказу о тех или иных о наших тайных делах и наших тайных вестей проведает и ему о всем писати ко государю царю и великому князе Михаилу Федоровичу всея Руси к Москве по сему государеву тайному наказу закрытым письмом».

Упомянутый здесь подъячий был послан специально для письма, но, как видим, зашифрованная переписка осуществлялась особо. Посылать зашифрованное письмо можно было лишь с особыми гонцами [1].

НЕГОСТЕПРИИМНЫЙ СТОКГОЛЬМ

21 ноября 1634 г. Д. Франзбеков и И. Исаков были «у руки» царя Михаила Фёдоровича, а 27 декабря выехали из Москвы.

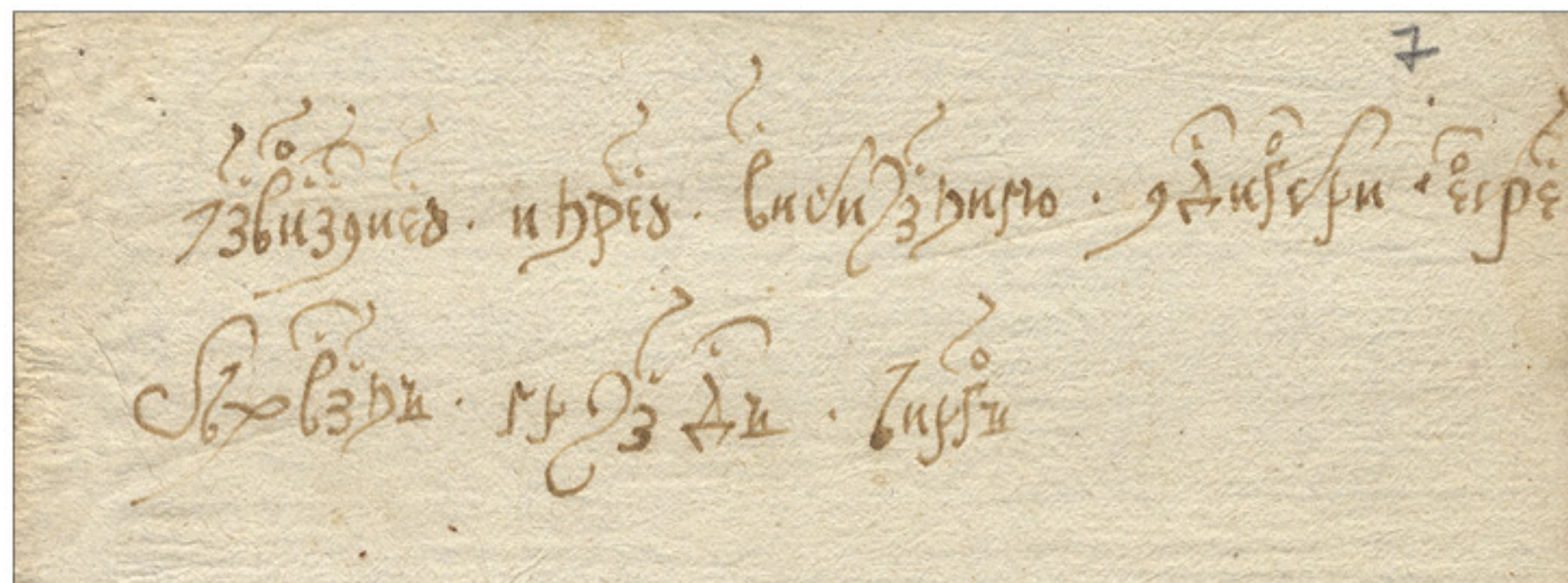


Иллюстрация 2. Автограф Д.А. Франзбекова

При отправлении в Швецию Франзбеков получил государева жалованья 500 р. деньгами, да соболями на 200 р., кроме того, повёз разные запасы (рыба, икра, мёд, пастила и т.п.), «чем ему иноземцев потчивать». С Франзбековым поехала большая свита в 34 человека.

Прибыв в Стокгольм, московские посланники немедленно столкнулись с другой дипломатической традицией. Вернее, с её отсутствием. Ведь дипломатическая служба Швеции тогда только формировалась.

По дороге в шведскую столицу Д. Франзбеков и И. Исаков подвергались «бесчестию», их людей избивали, а часть имущества украли. В Стокгольме Д. Франзбекова поселили за городом, на «кабацком дворе». Обо всем случившемся русский агент написал в Москву. Кроме того, из его грамот и из рассказа привезшего их гонца Осипа Кузьмищева выяснилось, что в Стокгольме произошел инцидент с участием людей Д. Франзбекова. К хозяину двора, где они остановились, днём и ночью приходили военные и гражданские «немецкие» люди для покупки спиртного. Однажды пьяные солдаты устроили драку и ранили двух слуг русского резидента. Жалобы Д. Франзбекова шведские должностные лица проигнорировали. Затем произошел еще один аналогичный конфликт. На этот раз резидент и его люди, доведенные до крайности выходками посетителей «кабацкого двора», связали не без побоев пьяного солдата и отдали его хозяину двора. Усмирённый швед на следующий день умер. О случившемся Москву известили грамотой от имени королевы, в ней сообщалось, что действия русского агента оставляются на рассмотрение царя. Царь Миха-

ил Фёдорович отвечал королеве Христине: «Пишешь, что люди нашего агента били вашего служилого человека, от чего он и умер; но задор произошёл от вашего человека, который нашего человека по лицу шпагою ранил».

А Франзбекову государь писал, чтоб в обидных делах бил челом королеве, а сам не своевольничал: «Ты оказался в чужом государстве таким дурным делом, что и слышать стыдно: самому управляться и до смерти побивать человека непригоже» [2].

Не устраивало резидента и выдаваемое шведами содержание, такое же, какое получал в Москве агент П. Крузбьорн, то есть по 35 рублей в месяц. Когда Д. Франзбеков начал жаловаться, что на эти деньги ему не прожить, так как в Стокгольме хлеб и прочие продукты стоят гораздо дороже, чем в Москве, шведское правительство решило действовать по-иному. В королевской грамоте царю предлагалось, чтобы и тот, и другой представители содержались своими правительствами. В ответной царской грамоте королеве напомнили о предыдущем шведском агенте — И. Меллере, который жил в Москве четыре года, и каждый месяц ему выдавали «корм». В то время шведы ничего не писали об изменении этих условий. Д. Франзбеков же прожил в Стокгольме чуть более полугода, и тут шведы вдруг начали поднимать вопрос о переводе его на содержание русского двора. Однако в России согласились принять предложение шведской стороны: оба полностью перешли на содержание своих правительств.

ВНИМАНИЕ К ПИСЬМАМ ФРАНЗБЕКОВА В МОСКВЕ

Обращает на себя внимание скорость реагирования приказных чиновников



Иллюстрация 3. Панорама Стокгольма в середине XVII века (художник Вольфганг Хартманн)

в Москве на письма русских представителей из зарубежья. Так, сразу после приезда первого гонца от Д. Франзбекова с письмами, где сообщалось о непочтительном отношении к дипломатическому представителю России в дороге, о не построенном дворе для русских купцов и многом другом, были проведены переговоры с П. Крузьборном. Тогда гонца О. Кузьмищева расспрашивали в Москве 31 июля 1635 г., а переговоры между комиссией во главе с думным дьяком И. Т. Грамотиным и шведским агентом произошли уже 1 августа 1635 г. П. Крузьборну объявили обо всех нарушениях со стороны шведского правительства по отношению к русским купцам и Д. Франзбекову, а также об оскорблениях, которым московский представитель подвергся в пути и в Стокгольме. От шведа потребовали объяснений, почему он писал «приказным людям» своей страны, будто бы по пути в Москву его «бесчестили» и дали «пустой» двор за городом. На самом деле, никаким оскорблени-

ям он не подвергался, и двор выделили «добрый и с палатою». П. Крузьборн, вероятно, испуганный такими расспросами, всё отрицал: он ни о каких оскорблениях не писал, так как их не было, но и русского агента никто не «бесчестил» и двор ему выделили такой, на каких живут посланники других государств.

В одном из писем Д. Франзбеков сообщил о переговорах с канцлером Оксеншерной. Благодаря им агент узнал о событиях на фронтах европейской войны. Д. Франзбеков и И. Исаков сообщили царю, что 2 сентября 1635 г. шведы подписали мир с Польшей сроком на двадцать шесть лет. Копию мирного договора, полученную от шведских «думных людей», русские представители отправили в Москву [3].

КОНСУЛЬСКИЕ ХЛОПОТЫ В СТОКГОЛЬМЕ

Всё же по характеру своей деятельности Франзбеков более походил на консула, занимающегося торговыми отно-

шениями и защитой прав российских подданных. Основные его усилия оказались направлены на решение вопросов торговли между двумя государствами. Проблем в этой сфере накопилось много. Столбовский мир 1617 г., а также захват шведами в 1621 г. Риги, привели к тому, что все контакты Русского государства с Западной Европой по Балтийскому морю теперь должны были осуществляться через владения Швеции. Условия договора вынуждали Россию вести торговлю через посредничество купцов Ревеля, Нарвы и Риги. В то же время, договор способствовал и развитию русско-шведской торговли, поскольку именно в Швецию русские торговые люди имели право ездить через Балтийское море. В этих торговых передвижениях использовались исключительно русские корабли. В Московское государство они везли в основном медь, железо и изделия из них, до 2500 тонн в год. Швеция, несмотря на кустарное производство, стала крупнейшим продавцом металлов в XVII веке. Почти вся

медь, потребляемая в Московском государстве, имела шведское происхождение [4]. Всё же основная русская торговля с Западной Европой шла тогда через Архангельск: так было выгоднее.

Дела русской дипломатической миссии осложнялись ещё и тем, что первоначально Д. Франзбеков и И. Исаков не имели указаний принимать жалобы русских подданных. Те жаловались на местные власти в Нарве, Колывани и других городах, бравших пошлины, не предусмотренные договорами. Кроме того, шведские купцы не отдавали долгов русским. В письмах в Москву Д. Франзбеков сообщал: «О таких делах думным людям без твоего государева указа говорить не смеем. В твоём государевом наказе, каков дан нам... о таких делах не написано». В Москве отреагировали быстро, в очередной грамоте указав вести переговоры с представителями шведского правительства о жалобах русских купцов «примеряясь к сему нашему указу» [3].

Главная же проблема заключалась в том, что правительство Швеции не построило гостиный двор для русских купцов в Стокгольме, хотя это предусматривалось Столбовским договором. В июле 1635 г. Д. Франзбеков сообщил об отсутствии двора, из-за чего торговым людям из России приходилось принимать по высокой цене амбары для товаров, и о жалобах русских купцов. На основании его донесения королеве Кристине была отправлена царская грамота от 26 августа 1635 г. В ней говорилось о нарушениях прав русских людей из Новгорода и Пскова в шведских городах, в частности, о неуплате шведскими подданными долгов. Далее указывалось на игнорирование шведскими «думными людьми» данных проблем, которые Д. Франзбеков не раз пытался с ними обсуждать.

От имени царя в грамоте выражалось недовольство тем, что для русских купцов торговый двор все еще не постро-

ен, хотя в России для подданных Швеции устроено даже два таких двора: в Москве и в Великом Новгороде. Ещё ранее, 13 августа 1635 г. русские купцы, торговавшие в Стокгольме, подали коллективную челобитную на имя королевы Кристины с жалобой на притеснения и с просьбой устроить в Стокгольме русский торговый двор. Вполне возможно, что они составили это обращение при участии Д. Франзбекова.

Оба документа, царская грамота и челобитная, сдвинули дело с мертвой точки. «Думные люди» обещали построить торговые дворы в столице и других городах и соблюдать права русских купцов. Действительно, временные строения особого двора приняли торговых людей из России летом 1637 г. А к началу 1641 г. завершилось строительство нового, уже постоянного торгового двора. Таким образом, первый постоянный дипломатический представитель России вполне успешно справлялся и с миссией по защите прав её подданных. Главным результатом его деятельности стало строительство русского гостиного двора в Стокгольме [3].

ОКОНЧАНИЕ МИССИИ И НОВЫЕ ПОРУЧЕНИЯ

В то же время в Москве высказывали недовольство тем, что резидент присылает мало информации о международной ситуации. Это обстоятельство, связанное и с заметным ослаблением роли Швеции в европейских делах, послужило впоследствии причиной его отъезда на родину. Д. Франзбеков прибыл в Москву 26 октября 1636 г. За свою «свейскую службу» он получил в награду придачу к поместному окладу, да и к денежному содержанию ему добавили 30 рублей.

В 1642 и 1643 гг. Франзбеков занимал довольно важное место Вятского воеводы в Хлынове (ныне г. Киров). Как известно, там до сих пор проходят дороги на Урал и в Сибирь.

В 1644 г. Франзбекова вновь вызвали в Москву для исполнения ответственного поручения. В ту пору в Москве находился датский королевич Вольдемар, он прибыл в качестве жениха царевны Ирины Михайловны. Франзбекову поручено было склонять королевича к принятию православия, это было необходимым условием для женитьбы. Но, несмотря на все усердие Франзбекова, его духовный и дипломатический опыт, ведь он сам перешёл в православие, добиться согласия королевича не удалось.

ТРУДЫ ПО УКРЕПЛЕНИЮ ВОСТОЧНЫХ ПРЕДЕЛОВ

Пожалуй, более известен Д. Франзбеков, как Якутский воевода 1648–1651 годов. Особенно, в связи со снаряжением в походы на Амур известного землепроходца Ерофея Хабарова. Весьма ответственное назначение Франзбекова Якутским воеводой состоялось в конце 1648 года. Тогда Якутский острог был самым восточным военным поселением Русского государства. Его гарнизон насчитывал 300 казаков. В 1634 году острог пережил осаду со стороны якутов, а в 1638 году стал центром новообразованного Якутского воеводства.

Направлявшимся в Сибирь воеводам разрешалось провозить с собой беспошлинно на казенных подводах изрядное количество собственного продовольствия, одежды, обуви, утвари и по 300–500 руб. наличных денег. Считалось, что этого воеводскому семейству и двум-четырем десяткам его дворовых должно было хватить на первый год службы в Сибири.

Прибыв на место назначения, Франзбеков принялся энергично исполнять данный ему наказ, рассылал людей для приискания «новых ясачных земель».

Особенную важность, как центр сбора ясака, представлял острог, расположенный в верховьях реки Лены. В 1648 году буряты, понимая значение Верхотурского острога, старались его уничтожить, во что бы то ни стало. Этот острог представлял собой квадрат 20×20 сажень, т.е. со стороной 42,5 метра, стены были устроены из вертикально поставленных брёвен. В углах стояли избы, между ними проезжая башня.

ПЕРВЫЙ ПОСТОЯННЫЙ ДИПРЕДСТАВИТЕЛЬ РОССИИ ВПОЛНЕ УСПЕШНО СПРАВЛЯЛСЯ И С МИССИЕЙ ПО ЗАЩИТЕ ПРАВ ЕЁ ПОДДАННЫХ



Иллюстрация 4. Сбор ясака (картина неизвестного художника XIX века)

Верхоленский острог был доведен осадой до последней крайности. Для защиты Верхоленска Франзбеков сформировал в 1648 году в Илимске отряд из 200 промысловых людей под начальством московского дворянина Федора Нефедьева. Они не только выручили верхоленцев, но и разорили ангарских бурят. Такова суровая правда местной жизни. С этого времени враждебные действия значительно ослабели.

Будучи в Якутске, Франзбеков фактически финансировал знаменитый поход Ерофея Хабарова на Амур, иначе он вряд ли бы состоялся. Тогда, в 1649 году, Франзбеков разрешил Хабарову набрать 150 охотников и снабдить их «в ссуду», без всякого пособия из государственной казны, оружием, припасами и всем необходимым для похода. Его участники, очевидно, надеялись не только подчинить Даурию великому государю, но и пограбить даурских «князцов», чтобы вознаградить себя за труды и издержки.

Тяжелейшая экспедиция, участники которой обогнули Байкал с севера и

прошли на юг, как известно, увенчалась блестящим успехом. Хабаров, достигнув Амура, взял несколько даурских городков и с большой добычей в мае 1650 года вернулся в Якутск. Немедля, Франзбеков написал в Москву о приведенной под государственную руку новой богатой земле.

Отпустив Хабарова опять в Даурию, Франзбеков послал с ним служилых людей для сбора ясака и для поиска серебряной руды, и в мае 1651 года уже послал в Москву собранный Хабаровым ясак. Но еще не успели в Москве получить донесения Франзбекова, как в Якутск доставили государев указ об отозвании его с воеводства.

БОРЬБА С САМОУПРАВСТВОМ И КОРРУПЦИЕЙ

Франзбекову поставили в вину то, что, несмотря на государственное требование держать к ясачным людям ласку, он посылал ратных людей на бурят, из которых многие были убиты. Ясачных якутов ограбил под предлогом, что они

затевают бунт, и реквизированным скотом себя обогатил. Да и служилым людям не выдавал жалованья, брал посулы и поминки, не посылал в Москву отчетов о расходе государственной казны, многих промышленных и торговых людей «животы пограбил» и т.п. А чтобы об этих действиях не узнали в Москве, Франзбеков устроил около Якутска заставы, где всех людей, ехавших на Русь, «обыскивали накрепко, раздевая до нага и разрезывая шубы», чтобы нельзя было провезти в Москву челобитных. Но, несмотря на предпринятые Франзбековым меры предосторожности, в 1651 году вышел указ царя Алексея Михайловича: стольнику Акинфому ехать в Якутск, принять у Франзбекова воеводство и «сыскать о всех его злоупотреблениях, а все его грабежные и посульные животы отписать на государя».

Прибывший в Якутск Иван Акинфов, описал все имущество Франзбекова, как нечестно приобретенное. Ценность имущества была определена в сумму 12742 р. Впоследствии Франзбекову была возвращена мягкая рухлядь (меха) на 2000 рублей, но все остальное было изъято в казну. Такой благоприятный поворот в деле Франзбекова произошел в 1652 году после его рассмотрения в Москве. В феврале состоялся приговор: «Дать государеву грамоту в Сибирь на Лену в Якуцкой острог к стольнику к Ивану Акинфому, а велеть ему Дмитрея Франзбекова из Якуцкого острогу отпустить ко государю к Москве, а что будет у него, у Дмитрея, взято животных и все те его животы ему, Дмитрею, отдать» [5].

* * *

Так завершилась почти сорокалетняя служба Д. А. Франзбекова.

ЛИТЕРАТУРА

1. Столпаков Б. В., Никонов В. Г. Чтоб было в тех землях не знатно. М., 2016.
2. Соловьёв С. М. История России с древнейших времён в пятнадцати книгах. М., 1962. Т. 9.
3. Коллегов С. С. Развитие русско-шведских отношений в контексте дипломатической деятельности Д. А. Францбекова (1634–1636 г.г.). Институт истории СО РАН. Новосибирск, 2012.
4. Шаскольский И. П. Русская морская торговля на Балтике в XVII в. (торговля со Швецией). СПб., 1994.
5. Русский биографический словарь А. А. Половцова. СПб., 1912. Францбеков Д. А.



Валерия МЕЩЕРЯКОВА
студентка факультета журналистики
МГУ им. М. В. Ломоносова



СТУДЕНТЫ В ОБЛАСТИ ИБ: КТО ОНИ?

ОТ РЕДАКЦИИ

Отражая процессы в кадровой сфере отрасли ИБ, *BIS Journal* стоит на позиции государственного прагматизма. Иначе нельзя: потребность в специалистах с каждым годом стремительно увеличивается, соответственно растет и их дефицит, угрожая отрасли кадровым коллапсом. Отечественные вузы в массовом порядке открывают факультеты и отделения по специальностям ИБ, но сама отрасль — вот парадокс! — не торопится принять этот ресурс, объясняя собственный «рефлекс отторжения» недостатком квалификации и опыта у студентов и выпускников. С одной стороны, работодатели правы, с другой, такой жесткий, потребительский подход к юным кадрам говорит о молодости и агрессивности самой сферы ИБ. Возможно, пришло время повзрослеть, стать мудрее и гуманизировать подходы? Например, начать создавать и культивировать преемственность, индивидуальное обучение, передачу опыта от мастера к учени-

ку — те самые институты, которые веками (не зря же!) работают в массовых профессиях, в том числе и достаточно технологизированных.

Представленный ниже материал — это зарисовка, штрихи к коллективному портрету студента в области ИБ. Того самого, который завтра постучится в двери вашего отдела кадров. Да, он по-детски наивен, и непонятно, какой степенью умений, опыта и таланта обладает, но он уже связал свою жизнь с информационной безопасностью, верит в нее и ждет от нее многого. Взамен он готов посвятить отрасли ИБ всю свою сознательную жизнь. И это не высокопарные слова — разве с вами не так? Так неужели он не заслуживает того, чтобы на первых порах отрасль уделила ему внимание?

Тем более, что (возвращаясь к позиции прагматизма) другого молодого специалиста не будет. Этот — единственный.

Знакомьтесь.

Сегодня в сфере информационной безопасности со всех сторон кричат, что в образовательном процессе не хватает практики, реальных знаний. Вопрос: а когда хватало? Бывает ли такое, что из университета выходит готовый специалист?

По моему мнению, место обучения и преподаватели — не столь значимо. К тому же стоит честно признать: хороших учителей крайне мало, если они вообще еще остались. Дело в том, что

преподаватели, способные научить думать, — а для работы в области ИБ необходимо уметь максимально точно анализировать информацию и сопоставлять факты — скованны рамками ФГОСов и других стандартов, норм и правил.

Очевидно, что все зависит от желания самого школьника или студента развиваться в выбранной сфере, от работоспособности и мотивации двигать мир к лучшему. В то же время существует тренд на технические профес-

сии, поэтому студенты охотно выбирают информационную безопасность. Это перспективно, востребовано, хорошо оплачивается.

Я поговорила с молодыми дарованиями в области ИБ и выяснила, есть ли у российской информационной безопасности надежды на светлое будущее.

АЛЕКСАНДР МАРЧЕНКО, АБИТУРИЕНТ, ПОСТУПАЕТ НА ФАКУЛЬТЕТ БЕЗОПАСНОСТИ ТУСУР, ТОМСК

Я надеюсь работать в органах федеральной безопасности. Моя цель — бороться с терроризмом. Ведь кто-то должен защищать людей, спасать жизни. Не страшно ли мне? Нет, а почему должно быть? Если задуматься, в любой профессии присутствует доля опасности, да и в принципе никто от нее не застрахован. Мы сейчас разговариваем, а может что-нибудь случиться на ровном месте. Обычно я так говорю маме, когда она просит прийти домой пораньше («а вдруг что-то случится?»): а если на землю метеорит упадет?

К тому же, думаю, это основополагающее качество для настоящего мужчины — уметь защищать.

Выбирая специальность, отталкивался от своих умений и ощущений. Мне нравится общаться с людьми, решать значимые для общества проблемы. Выбирал между юридическим факультетом и факультетом безопасности. Все же понял, что мне ближе программирование.

Первый курс планирую полностью посвятить учебе в университете, буду многое изучать дополнительно сам, участвовать в учебных проектах. А со второго курса начну искать стажировку или подработку: нужно набирать как можно больше опыта.



ПОЛИНА ВАСИЛЬЕВА, II КУРС, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ, КОЛЛЕДЖ АКСиБГУ, КРАСНОЯРСК

Пошла на эту специальность после окончания школы — так посоветовали родители. Для меня здесь все новое, потому интересно — как изучать новый язык. Пока учусь, сложилось впечатление, что в России профессии в сфере информационной безопасности не востребованы. А молодому человеку после колледжа найти работу по специальности уж точно — задача не из легких.

У нас есть преподаватель по основам ИБ с двумя высшими образованиями. Он работает в колледже, потому что получается, что спрос в России на безопасников не велик и платят мало. Поэтому решила: окончу АКСиБГУ и буду поступать на программиста, — это всегда будет актуальным.

Сейчас, на первых двух курсах, у нас больше базовых предметов: математика, экономика, история. Из тех, что учат профессии, в этом семестре только программирование, в прошлом — основы безопасности, в следующем — криптография. По факту, практические занятия — только по предмету ЭВМ: работали в Excel и Access. Однако преподавателей по специальности у нас немного, и дают они мало, практически ничего — все изучаем сами. После школы это, конечно, непривычно.

**КИРИЛЛ КАЧАЛОВ, II КУРС, ФАКУЛЬТЕТ БЕЗОПАСНОСТИ ТУСУР**

Я считаю, что моя специальность, несмотря на рост безработицы, будет востребована во всем мире, поэтому и учусь на информационной безопасности.

Все направления IT-отрасли связаны, и потому необходимы специалисты, которые умеют делать все. А еще важно уметь изучать большой объем информации за короткие сроки. Именно поэтому я учусь в университете, хотя сегодня можно освоить специальность (причем любую) и без лекций в четырех стенах. Где еще я так быстро научусь общаться с людьми, понимать общественные процессы и впитывать огромный объем информации за день до экзамена? Наше время — это пора тотальной глобализации. Будучи безопасником, я могу работать в любой точке мира, что важно. Кроме того, любой успешный проект в мире всегда создается с помощью межнациональной команды. Нужен лишь ноутбук и доступ в интернет.

IT-сфера постоянно меняется, обновляется, улучшаются принципы и методы работы. Каждые полгода придумывают новую сферу! То есть в вузе я буду узнавать информацию, которая уже устарела. Соответственно многое нужно изучать самому. Это я и собираюсь делать ближайшие пять лет.

**МАЛИК БУРХАНОВ, II КУРС, ФАКУЛЬТЕТ ИНФОРМАТИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ МГТУ ИМ. Н.Э. БАУМАНА, МОСКВА**

IT-сфера — самая перспективная на сегодняшний день. Поэтому учусь в одном из лучших вузов страны. В обучении, с одной стороны, многое зависит от университета, с другой — программирование можно изучить и самостоятельно.

Думаю о работе во всемирно известной корпорации, но больше привлекает собственный бизнес. Это позволит стать (насколько это возможно) независимым, взять жизнь в свои руки и, надеюсь, преуспеть. Немаловажно учитывать и финансовую сторону вопроса: в технической сфере реальнее

всего заработать достойные деньги. Конечно, просто так ничего в руки не приплывет: необходимо много работать, посвящать своему делу все время. Я, в принципе, считаю, что работать нужно как можно раньше: со школы или с I курса, — это закаляет характер.



АСЯ ИЛЬИНЫХ, IV КУРС, ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ АЛТГТУ, БАРНАУЛ

ИБ очень интересная сфера, но сложная. Обычному человеку тут трудно ориентироваться, почти невозможно. Я имею в виду разного рода конкурсы, соревнования по безопасности: побеждает самый талантливый.

Чтобы быть успешным в ИБ, нужно думать по-особому — как безопасник, а это дано единицам. К примеру, у нас в группе 25 человек, и я вижу, что мало кому дается специальность. То есть работать по профессии пойдут далеко не все: талантов мало, может, 1–2 человека.

Я пробовала реализовываться — некоторое время работала в сервисном центре. Потом поняла, что такая работа с учебой малосовместима, особенно для девушки. Так что первостепенная задача для меня — получить диплом.



МАТВЕЙ СТАРОДУБОВ, ВЫПУСКНИК БАКАЛАВРИАТА, ФАКУЛЬТЕТ АВТО- МАТИКИ И ВЫЧИС- ЛИТЕЛЬНОЙ ТЕХНИКИ НГТУ, НОВОСИБИРСК

Поступал в 11 классе в Институт криптографии, связи и информатики ФСБ, но не прошел медкомиссию. Хотел попасть туда до второго курса, а потом желание пропало.

С какого курса следует устраиваться на работу — не знаю. В вузе дают базу, достаточную для начальных этапов профессионального становления, так что начать можно в любое время. Однокурсники работают: кто по специальности, например, внедряет системы информационной безопасности, кто-то разрабатывает приложения, например, в компаниях Entesys, Werbary. Я же решил не торопиться: учеба занимает все время, к тому же я профессионально занимаюсь баскетболом, играю за университет.

Сейчас защитил диплом, поступаю в магистратуру, нахожусь в поиске работы. Возможно, это будет какая-то коммерческая корпорация.



АЛЕКСАНДР ЧУЕШЕВ, МАГИСТРАНТ ФАКУЛЬТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, АЛТГТУ

Недавно защитил диплом, сейчас стажируюсь во Франции, в лаборатории Lirb UPMC. Год назад меня отобрали на стажировку в Университет Пьера и Марии Кюри, прошел конкурс в аспирантуру со следующего года. Переехал из России, это новый опыт — мне нравится постоянно меняться, общаться с разными людьми из моей сферы (и не только).

Есть однокурсники, которые остаются в Барнауле, и предложения при этом получают хорошие. Но я решил: если есть возможность, почему не попробовать? В любом случае, если не сложится, вернусь обратно в любой момент.

Я еще на втором курсе начал брать небольшие проекты, потом работал на фрилансе. Все зависит от способностей человека: нужно успевать многое, но в то же время качественно. Важно не хватать звезд: если ты лучший на курсе или даже в университете, этому не стоит придавать большое значение — «лучшесть» меряется другими способами. Одновременно с этим, если студента отобрали на какое-то предприятие от университета, он думает, что все знает и умеет, и учеба ему, умному, теперь не нужна. Тут самая большая ошибка: сейчас понимаю, что мне помогает вся информация, полученная в вузе.

Чтобы идти работать на первых курсах, нужно точно определиться с направлением информационных технологий, в котором хочется развиваться, тогда все сложится. Если студент не уверен или проработал какое-то время, а потом резко решил пойти в другом направлении — время потрачено зря. Конечно, какие-то деньги заработаны, но я не считаю это важным.

Исходя из своего студенческого и жизненного опыта могу рассуждать: сфера IT очень быстро меняется, поэтому выход для молодых студентов — помимо освоения университетской базовой программы обязательно участвовать в конференциях, посещать предприятия — вообще быть профессионально активным. Нужно использовать все возможности для понимания современных тенденций в IT и ИБ.



БЕЗОПАСНОСТЬ — ЭТО ЧТО?

Безопасность: Состояние защищенности интересов (целей) организации БС РФ в условиях угроз (СТО БР ИББС)

Защищенность достигается обеспечением совокупности свойств ИБ — доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) организации БС РФ (там же)

«ЗЕМНУЮ ЖИЗНЬ ПРОИДЯ ДО ПОЛОВИНЫ,
Я ОЧУТИЛСЯ В СУМРАЧНОМ ЛЕСУ...»

Чем больше пытаюсь это осознать, тем больше сомнений меня одолевает. Пытался найти синоним к слову «состояние». Нашел 42. Ближе всех к моему пониманию — это «ощущение». Да оно и действительно ближе. Безопасность — это ощущение. Но вот беда, ощущение никак не может быть получено «достижением обеспечения совокупности свойств информационной безопасности». Это совершенно из другого смыслового ряда. Ощущение — понятие, связанное с каким-то чувством, оно по сути своей субъективно, присуще только конкретному индивидууму только в конкретной обстановке в конкретный момент времени. Момент изменился — изменилось и ощущение. Ведь я не могу приказать: «Остановись, мгновенье!».

Но если следовать этой логике, то безопасность — сущность субъективная, живущая только у нас в голове и

только в наших ощущениях? Если нет нас или наших ощущений, то и безопасности нет?

Второй вывод тоже какой-то странный: если безопасность существует в моей голове какая-то своя, то в другой голове она другая? Ведь это же ощущение другого человека — человека с другим жизненным опытом, другими взглядами, другими оценками окружающего мира. Его ощущения отличаются от моих, пусть на маленькую малость, но отличаются. А значит, мы думаем про разную безопасность.

Тогда, может быть, все эти нормативные документы нужны, чтобы мы стали думать об одном и том же одинаково? Но ведь мы все разные и читаем все по-разному. Больше того, я многие книги читаю по несколько (а некоторые, так и помногу) раз, и всякий раз нахожу в них что-то новое, или то, что раньше было интересно, вдруг становится скучным. То есть чтение документа тоже не делает нас ощу-

щающими одинаково эту самую «безопасность».

А если начать спрашивать окружающих об их ощущениях безопасности? Попробовал. Получилось еще запутанней. Все боятся по-разному и разных вещей. Одни до дрожи боятся троянов и вирусов, другие боятся своих системных администраторов, а третьи вообще боятся только мошенников «за периметром». Чтобы все были спокойны, надо делать совершенно разные вещи, иной раз противоречащие друг другу. Так, может, их не делать?

Или плюнуть на «их» мнение, и делать «по-своему», тоже нехорошо, ведь зачастую финансируют мое «по-своему» именно они.

Так какая же она, эта безопасность? Да и существует ли она вообще? Объективно, я имею в виду. А если это так, то чем мы тогда занимаемся столько лет?



РКИ-Форум Россия

г. Санкт-Петербург
25–27 сентября 2018 года

www.pki-forum.ru



Встречаемся в Питере!

АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Книжное
издательство

ib-bank.ru