



10> Игорь ЛЯПУНОВ
ПАО «Ростелеком»
**Вызовы на уровне
государственной
кибербезопасности**

26> Анатолий АКСАКОВ
Государственная Дума РФ
**Все грани цифровизации
в 2019 году**

58> Алексей СИДОРОВ,
Сергей РУБЛЕВ
ООО «Пангео Радар»
**Постройте свой SOC
на Платформе Радар**



81> Наталья КАСПЕРСКАЯ
ГК InfoWatch
**Шаг за шагом,
постепенно...**

114> Валентин ЗЯЗИН
РТУ МИРЭА
**Новое слово
в ИБ-образовании**

НАВИГАЦИЯ В МИРЕ ИБ: SOC-ФОРУМУ — 5 ЛЕТ!



АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Образование
и карьера

ib-bank.ru



Игорь НЕКРАСОВ
главный редактор
BIS Journal

«**Н**е стоит прогибаться под изменчивый мир», — магический призыв, гимн целого поколения, звучит сегодня, кажется, как-то не так. Мир вокруг стремительно меняется и просто необходимо успевать за этими изменениями, меняться самим. Тем более, когда речь идет о целой отрасли.

На пятом Финополисе в Сочи, который сам по себе стал грандиозным образом и символом изменений в области финансовых технологий (вспомните, что говорили на нем пять лет назад о блокчейне, online-банках, криптоактивах, искусственном интеллекте, облаках и т.д., и что говорят сегодня!), эта мысль звучала определяющим ритмом. Эльвира Набиуллина сформулировала ее предельно просто, практически стихотворно: «Финансовые технологии меняют мир. Они несут с собой и преимущества и риски. Мы все должны измениться, чтобы ответить на эти вызовы».

Перемены в сфере ИБ будут обсуждаться на SOC-Форуме — мероприятии не менее грандиозном для своей отрасли. Этот номер BIS Journal — по сути, конспект, разминка перед большим разговором. Вот только некоторые из вопросов, которые нас интересуют:

- ◆ насколько российские компании готовы противостоять серьезным атакам на КИИ? И готовы ли вообще, ведь со стороны злоумышленников в данном случае выступают не привычные нам ворышки и мошенники, а масштабные, серьезно подготовленные организации, использующие ПО, с которым наши безопасники раньше не сталкивались?
- ◆ обладают ли наши безопасники достаточными ресурсами: отечественными технологиями, кадрами и опытом?
- ◆ не пора ли изменить регуляторные подходы? Например, предъявлять требования не к наличию средств защиты, а к процессу их функционирования?
- ◆ не пора ли сместить акценты в нормативной базе: с ответственности за невыполнение требований на ответственность за инциденты?

По сути, получается, речь на SOC-Форуме пойдет не о том, чтобы прогибаться или не прогибаться под изменчивый мир. А о том, чтобы провести ревизию на судне, определиться с курсом и правильно перенастроить паруса.

Чтобы ветра перемен стали попутными.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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

Сычев А.М. — Первый заместитель директора Департамента информационной безопасности Банка России, доктор технических наук

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

Вихорев С.В. — заместитель руководителя направления информационной безопасности НТЦ «Вулкан»

Дзержинский Ф.Я. — главный эксперт — координатор системной экспертизы блока «информационные технологии» ООО «ТехноСофт», CSDP

Зубков А.Н. — генеральный директор ООО «Медиа Группа „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)

Курило А.П. — президент компании «Реальная Безопасность», кандидат технических наук

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

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

Музипов Ф.Х. — председатель правления НП «ПСИБ»

Некрасов И.В. — главный редактор журнала

Окулесский В.А. — заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук

Пазизин С.В. — заместитель начальника Управления по обеспечению информационной безопасности ОАО Банк ВТБ, кандидат физико-математических наук

Шумский Л.С. — CISO в Ассоциации «Финтех»

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

ЭКСПЕРТНАЯ ГРУППА

Одувалов М.В. — эксперт BIS Journal

Филипчук А.А. — технический директор ГК ЦРТ

Калашникова Е.В. — Банк ВТБ (ПАО)

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**

Шеф-редактор: **Былевский П.Г.**

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

Арт-директор: **Мельников Н.С.**

Руководитель интернет-проектов: **Воробьева А.А.**

Руководитель спецпроектов: **Седов О.В.**

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

Куликов В.А., Бродская М.А., к.т.н.

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

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

wikipedia.org, waralbum.ru, ramyat-naroda.ru

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: journal.ib-bank.ru

E-mail: bis@ib-bank.ru

Отдел рекламы: reklama@ib-bank.ru

Отдел распространения: tirazh@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство ПИ № ФС77-61378 от 10 апреля 2015 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 25.10.2019. Тираж 7000 экз.

Заказ №42519. Цена договорная.

Отпечатан в типографии

«Московский Печатный Двор»,

123298, г. Москва, 3-я Хорошевская 18,

корп.1, офис 201А

© BIS Journal, 2019



НОВОСТИ

- 5 **В России, в мире, происшествия, технологии**

ТЕМА НОМЕРА

- 10 **SOC**
Игорь Ляпунов (ПАО «Ростелеком»)
Вызовы на уровне государственной кибербезопасности
- 15 **SOC**
Муслим Меджлумов (BI.ZONE)
Амулеты не защищают от киберпреступников
- 18 **SOC**
Александр Бодрик (Cyberlands B.V.)
Первый после SOC'a
- 20 **SOC**
Дмитрий Ким (Positive Technologies)
SOC: типовые трудности и советы по запуску
- 22 **SOC**
Иван Мелехин (Информзащита)
SOC: внешний или внутренний? Выбор неизбежен

РЕГУЛЯТОРЫ

- 26 **Законотворчество**
Анатолий Аксаков (Государственная Дума РФ)
Все грани цифровизации
- 28 **Контроль и надзор**
Андрей Выборнов (Банк России)
Готовность номер один

БАНКИ

- 30 **Круглый стол**
Анна Воробьева (BIS Journal)
ИБ-риски: сегодня и завтра
- 36 **Дорожная карта**
Валерий Естехин (эксперт ИБ)
Банк, ты готов?
- 40 **Социальная инженерия**
Евгений Карпов (АО КБ «Хлынов»)
Лёгкая кавалерия
- 43 **СТО БР ИББС**
Валерий Естехин (эксперт ИБ)
Роль СТО БР ИББС
- 44 **Кейсы**
Дмитрий Орлов (эксперт по ИТ и ИБ)
Сами с усами
- 46 **Технологии**
Диана Князева (ПАО «Сбербанк»)
Безбумажный банк

УГРОЗЫ И РЕШЕНИЯ

- 51 **Облака**
Антон Тихонов (ГК MONT)
Защищая «неиспользуемое» облако
- 54 **Интеграторы**
Андрей Перкунов (СТИ)
СТИ создает защиту, адаптивную к любым угрозам и динамичным изменениям среды





УГРОЗЫ И РЕШЕНИЯ

- 56 **MSSP**
Иван Лопатин (ДиалогНаука)
На новом уровне
- 58 **Новые продукты**
Алексей Сидоров, Сергей Рублев
(ООО «Пангео Радар»)
Платформа Радар
- 60 **SOC**
Максим Павлуниин
(Angara Professional Assistance)
Как стать аналитиком SOC
- 62 **Интеграторы**
Дмитрий Михеев (АйТи БАСТИОН)
«АйТи БАСТИОН» + DLP = Согласие
- 63 **Антифрод**
Дмитрий Слободенюк (ARinteg)
Антифрод в российских реалиях
- 66 **За рубежом**
Куаныш Талгаров (АО «ИО «Казахстанская
Ипотечная Компания»)
**«За время первого этапа проекта мы
подключили к IIDM шесть систем»**

ИНФРАСТРУКТУРА

- 68 **Деловые мероприятия**
PKI-Форум 2019
- 72 **Деловые мероприятия**
Марк Новодачный (BIS Journal)
Осенняя сессия Уральского форума 2019
- 74 **Деловые мероприятия**
Николай Кольский (BIS Journal)
Oracle Systems Advantage Forum
- 75 **Деловые мероприятия**
Корней Реут (BIS Journal)
Mobile Forensics Day
- 76 **Импортозамещение**
Александр Баранов (НИУ ВШЭ)
«Будем с ужасом смотреть...»
- 81 **Импортозамещение**
Наталья Касперская (ГК InfoWatch)
Шаг за шагом, постепенно...
- 86 **Обзор АИС**
Валерий Хурматуллин, Андрей Колесников,
Дмитрий Колесников, Евгения Колесникова
На основе патентов



HI-NUME

- 90 Социальная инженерия**
Игорь Долотин (UBS)
Важная тема
- 92 Социальная инженерия**
Марина Бродская (BIS Journal)
«Лучше поздно, чем никогда»
- 96 Социальная инженерия**
Сергей Волдохин, Ольга Лимонова,
Андрей Жаркевич (ООО «Антифишинг»)
Психология цифровых атак
- 102 Биохакинг**
Павел Былевский (BIS Journal)
Биохакинг государство пока в упор не видит
- 104 Биохакинг**
Елена Милова (Life Extension Advocacy Foundation)
Наше будущее, которое не за горами
- 105 Новое здравоохранение**
Валентина Буркова (Биолит)
Больше здоровья — меньше болезней

ОБРАЗОВАНИЕ И КАРЬЕРА

- 110 Репортаж**
Искать таланты интересно!
- 113 Новое слово**
Артем Зубков (ФСРБИТ)
Такому в школе не научат
- 114 Новое слово**
Валентин Зязин (РТУ МИРЭА)
Киберполигон в МИРЭА
- 118 Обзор**
Марина Бродская (BIS Journal)
Наступление троечников?
- 121 Мысли вслух**
Валерий Куликов (BIS Journal)
Бритва Оккама и ИБ



СУБЪЕКТЫ

- 124 История**
Борис Столппаков (историк криптографии)
Генеральная репетиция штурма Берлина
- 128 История**
Дмитрий Ларин (историк криптографии)
Подвиг радиоразведчика
- 129 История**
Борис Столппаков (историк криптографии)
7 из 11
- 134 Заметки безопасника**
Александр Бодрик (Cyberlands B.V.)
Двенадцать богатырей
- 136 Репортаж**
BIS-огонёк



СОВЕТ ФЕДЕРАЦИИ ВЗЯЛСЯ ЗА КИБЕРБЕЗОПАСНОСТЬ

Любая цифровая инфраструктура потенциально подвержена угрозам. Необходимо минимизировать риски и комплексно обеспечивать информационную безопасность, заявил глава Комитета Совета Федерации по экономической политике Андрей Кутепов.

По его словам, степень устойчивости определяется средствами защиты. Поэтому необходимо минимизировать риски, связанные с утечками информации, несанкционированным воздействием на данные или другие информационные ресурсы городов.

А. Кутепов сообщил, что в Совете Федерации создана Временная комиссия по законодательному регулированию вопросов кибербезопасности, развития и использования цифровых технологий. Задача комиссии — до конца текущего года с помощью привлечённых экспертов разработать проект базового документа, отража-

ющего текущую ситуацию и предлагающего «дорожную карту» (в том числе в виде законодательных инициатив, которые направлены на формирование правового поля в области кибербезопасности).

Такая же рабочая группа есть и при Комитете СФ по конституционному законодательству и государственному строительству, а также работает секция Совета по развитию цифровой экономики при СФ. Она ведёт разработку рекомендаций по обеспечению ИБ для детей.



ЗНАЙ СВОЕГО КЛИЕНТА!

Банк России планирует запустить единую банковскую платформу по проверке клиентов, в которой юридические лица и индивидуальные предприниматели будут поделены на группы риска «по принципу светофора» — Know your customer (KYC, «Знай своего клиента»).



В «красной» зоне (высокий риск) будут компании, требующие контроля в режиме онлайн. В «жёлтой» — так называемые «сомнительные» клиенты, чьи операции требуют офлайн-анализа. Подавляющая часть клиентов останется в «зелёной» зоне и не потребует повышенного внимания банков. Клиенты будут оцениваться примерно по 100 параметрам.

Для внедрения платформы потребуются поправки к «антиотмывочному» закону и закону о банковской деятельности. Созданием платформы займётся Банк России вместе с банками и вендорами банковского ПО. Решение уже прошло тест в «Сбербанке».

В Банке России пояснили, что система будет только помогать оценивать уровень риска клиентов — основная работа останется на банках. Участники рынка в целом одобряют инициативу, однако отмечают: важно, чтобы оценка не превратилась в инструмент давления на бизнес.

ПО НОМЕРУ ТЕЛЕФОНА

Клиентов банков будут идентифицировать по номеру телефона. Соответствующий законопроект находится в разработке, сообщил глава комитета Госдумы по финансовому рынку Анатолий Аксаков.

Идентификация будет проводиться посредством Единой информационной системы проверки сведений об абоненте. За её создание заплатят банки. Система позиционируется как связующее звено между банками и операторами связи. Инициатива призвана избавить россиян от звонков коллекторов и предотвращать кражи денег с помощью социальной инженерии.

Банки относятся к идее неоднозначно. Например, сведения из абонентской базы операторов часто не соответствуют действительности (если SIM-карта оформлена на одного, а пользуется ей другой). Сотовые операторы также сомневаются: предложенные механизмы не помогут решить проблему с мошенничеством.

БИОМЕТРИЯ ПОВСЮДУ

Банк России должен обладать правом выставлять требования к безопасности биометрических систем, чтобы утечек клиентских данных больше не происходило, заявила первый заместитель председателя Банка России Ольга Скоробогатова.

Сейчас Банк России обсуждает с банками возможность обязать своих клиентов совершать финансовые действия — открывать кредиты и депозиты через ЕБС. Председатель ЦБ Эльвира Набиуллина рассказала, что многие банки всё ещё не практикуют предоставление услуг клиентам по биометрическим данным. Однако это нужно сделать.

Более того, ведётся активная работа по расширению сферы применения ЕБС за пределами финансовой отрасли. Это может быть приобретение авиа- и железнодорожных билетов, возможность пройти в поезд или самолет, получить программу лояльности.

АМЕРИКАНСКИЙ ХАКЕР В КИЕВЕ

Киберполиция Украины задержала в одном из самых дорогих отелей Киева разыскиваемого в США киберпреступника. 32-летний мужчина подозревается в хищении 6 млн долларов со счетов американских финучреждений.

Расследование его преступной деятельности начато ещё в 2010 году силами ФБР и Службы расследования финансовых преступлений (FNTT) США. В этом году к властям Украины поступил запрос о предоставлении международно-правовой помощи по розыску и задержанию подозреваемого.

Мужчине выдвинуты обвинения в незаконном вмешательстве в работу компьютерных систем, хищении и отмывании денег в особо крупных размерах и мошенничестве. В настоящее время решается вопрос о выдаче задержанного властям США.

РАБОТАЕТ ЕВРОПОЛ!

Европол провёл масштабную операцию eComm 2019 по задержанию киберпреступников в 19 странах. При поддержке правоохранительных органов и частных компаний было задержано 60 человек.

Задача операции — пресечение деятельности сети online-мошенников, работающих по профилю электронной коммерции с использованием online-платформ, приложений и сервисов.

Было проведено более 40 обысков (изъяты гаджеты, данные карт и наличные деньги), выявлено 6500 мошеннических транзакций, оценён ущерб от мошенничества (5 млн евро) и предотвращён дальнейший ущерб (93 тыс. евро).

Плюс было установлено, что часть подозреваемых была связана с преступными группировками и замешана в фишинге, кибератаках с использованием вредоносных программ, создании поддельных сайтов, отмывании денег и прочем.

АТАКОВАНЫ ГУМАНИТАРНЫЕ ОРГАНИЗАЦИИ ООН

Эксперты Lookout выявили вредоносную кампанию против гуманитарных организаций ООН. Под атаками оказались детский фонд UNICEF, Всемирная продовольственная программа, Программа развития ООН и другие. Специалисты уведомили всех об угрозе и предупредили о новых атаках.

Хакеры создали фишинговые сайты, скопировав дизайн с оригинальных сайтов ООН, с целью заманивать

сотрудников организаций на поддельные страницы авторизации и похищать их учётные данные. Их интересовали не отдельные сотрудники, а вся организация в целом. Завладев учётными данными одних сотрудников, преступники изучают их электронные ящики в поисках других сотрудников и пытаются скомпрометировать уже другие учётные записи.

Эксперты Lookout выявили несколько небезынтересных методов, используемых в данной кампании. Например, способность обнаруживать мобильные устройства и напрямую регистрировать нажатия клавиш, когда жертва вводит данные в поле пароля.

Исследователи также обнаружили кейлоггер, встроенный в поле пароля на фишинговых страницах авторизации. То есть, даже если жертва ввела учётные данные, но не нажала на кнопку ввода, они все равно будут перехвачены кейлоггером.



В КИТАЕ ПРИНЯТ ЗАКОН О ШИФРОВАНИИ

26 октября правительство Китая приняло закон о шифровании данных, первый в истории страны. Закон предполагает разделение криптографических стандартов на типы и предоставление компетентным органам власти контроля над ними. Закон вступит в силу 1 января следующего года.

Информагентство «Синьхуа» сообщило: цель нового закона — предотвращение утечек данных, которые могут навредить госструктурам, компаниям и частным лицам. В документе также прописаны наказания за нарушения принципов безопасности.

По этому закону стандарты шифрования делятся на категории: «ключевые и общепринятые» и «коммерческие». Ключевые и общепринятые будут использоваться органами власти и госучреждениями, а коммерческие — будут разрабатываться соответственно в коммерческих целях.

Закон предусматривает, что ко всем коммерческим субъектам, включая предприятия, финансируемые из-за рубежа, следует относиться одинаково в вопросах «изучения, разработки, производства, обслуживания и продажи» стандартов из второй категории.

Также документ возлагает на китайское правительство обязанность стимулировать подготовку квалифицированных специалистов в области криптографии и их работу в национальных интересах.



СТРАННАЯ ИСТОРИЯ С УТЕЧКАМИ

Этим летом в СМИ разразилась шумиха по поводу утечек персональных данных клиентов трех крупных банков — Альфа-банка, Тинькофф-банка и банка «Открытие». BIS Journal провёл свое расследование и выяснил следующее.

Во-первых, источники внутри всех трёх банков факты утечек отрицают, и у журнала нет оснований им не верить. Во-вторых, в каждый из этих банков в июне обращался менеджер компании DeviceLock, сообщал, что в банке произошла утечка данных, и предлагал купить продукты компании именно для борьбы с утечками. После отказа в сотрудничестве информация об утечке появлялась в СМИ. В-третьих, DeviceLock предлагала свои решения банкам по ценам заметно выше рыночных. В-четвёртых, в начале августа DeviceLock распространила отчёт, в котором говорится, что клиентские базы данных половины крупнейших банков России можно купить через DarkNet.



Напрашивается вывод, что таким образом DeviceLock пытается поднять «хайп» вокруг утечек и заставить банки покупать свою продукцию. Но ряд независимых экспертов считает, что шантаж и нечестная игра со стороны столь крупной и успешной компании маловероятны. Возможно, это конкретный сотрудник совершил опрометчивый «ход конём», рассчитывая таким образом повысить личные продажи.

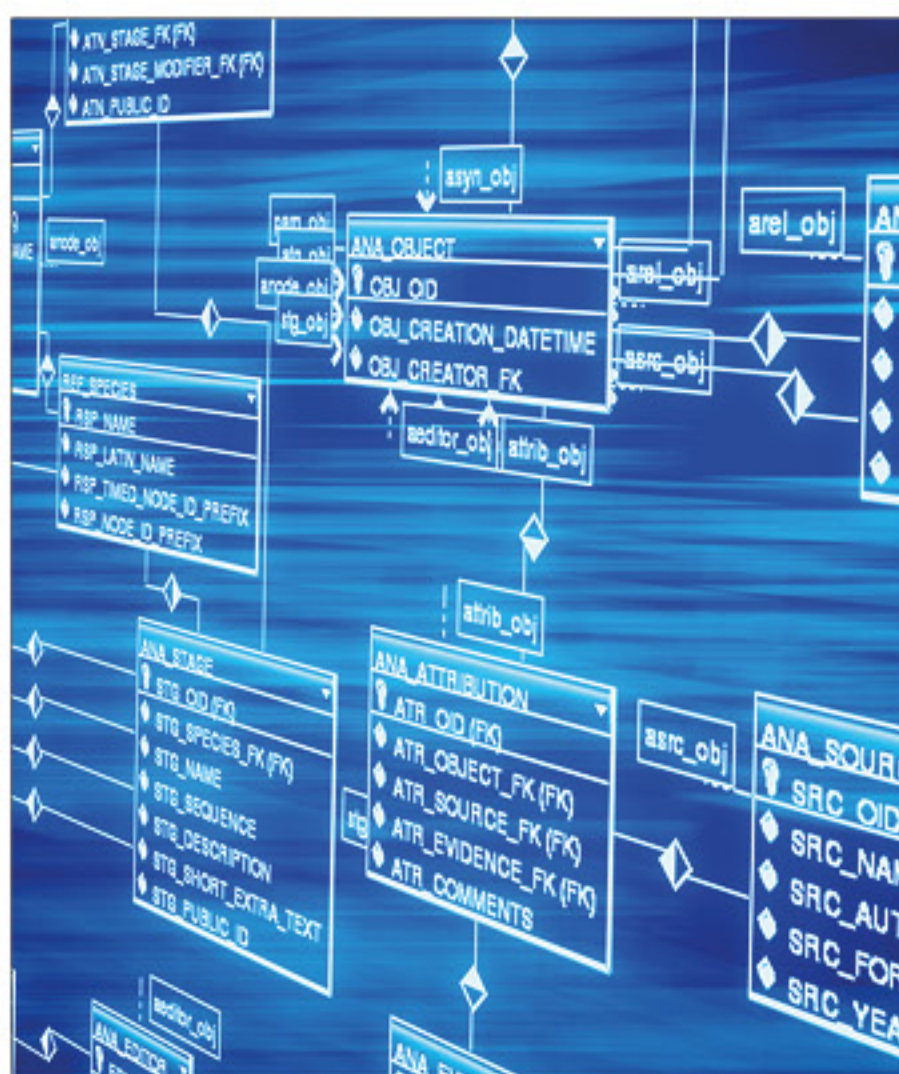
СЛУЧАЙНАЯ НАХОДКА

Обнаружено около 20 млн записей с данными российских налогоплательщиков. Они находились в открытом доступе с мая прошлого года.

Две базы с налоговыми и персональными данными 20 млн россиян за 2009–2016 годы разместили неизвестные в облаке Amazon Web Services Elasticsearch. Из них можно было узнать полное имя человека, адрес, статус резидента, номер паспорта и телефона, ИНН, сумму уплаченных налогов, а также имя и телефон работодателя. В основном информация относилась к жителям Москвы и Подмосковья.

Базы данных в середине сентября обнаружил независимый исследователь. Прежде всего он попробовал связаться с владельцем облака, но тот не вышел на связь. Тем не менее, 20 сентября доступ к информации был закрыт. Владелец баз данных находится на территории Украины.

Откуда произошла утечка, пока неизвестно. Технический директор Qrator Labs Артём Гавриченко отметил, что в таких случаях источник утечки налоговых данных определить сложно, но обычно подобные инциденты случаются по вине подрядчиков или субподрядчиков.



УЖЕСТОЧИТЬ НАКАЗАНИЯ ЗА КИБЕР-ПРЕСТУПЛЕНИЯ

Глава ЦБ Эльвира Набиуллина заявила о важности координации между бизнесом и властями в вопросах борьбы с хакерами и призвала повышать ответственность за киберпреступления.

В ходе дискуссии на форуме инновационных финансовых технологий Fi-popolis руководитель Сбербанка Герман Греф отметил, что за часть киберпреступлений ответственность в РФ просто не предусмотрена, а за другую часть она значительно ниже, чем в других странах.

Эльвира Набиуллина поддержала его. По её словам, регулятор видит риски в том, что вопросы ИБ не включены во многие бизнес-процессы банков.



СБЕРБАНК ПОЙМАЛ ВИНОВНИКА УТЕЧКИ

Сведения о 60 млн кредитных карт клиентов Сбербанка появились 3 октября на одном из заблокированных Роскомнадзором форумов. Сбербанк провёл внутреннее расследование и выявил виновника. Им оказался 28-летний руководитель сектора в одном из бизнес-подразделений. Мужчина имел доступ к конфиденциальной информации.

Герман Греф охарактеризовал ситуацию как «внутреннее предательство». Он отметил, что персональные данные клиентов не оказались в открытом доступе, а все скомпрометированные карты уже перевыпущены. Глава Сбербанка заявил, что банк планирует «кардинально усилить» контроль доступа сотрудников к системам банка, чтобы «минимизировать влияние человеческого фактора».

SWIFT РАЗВИВАЕТ ОТКРЫТЫЙ БАНКИНГ

Международная межбанковская система SWIFT опубликовала новый стандарт API для предварительной авторизации средств. Стандарт создаст условия для дальнейшего внедрения инноваций в финансовых услугах с помощью открытого банкинга.

Новый стандарт позволяет банку плательщика заранее выделить средства на покупку, гарантируя, что платеж будет выполнен. Это второй из стандартов SWIFT API Open Banking Extensions и последнее дополнение к глобальной библиотеке API, которую SWIFT создает в сотрудничестве с банками, торговыми предприятиями и финтех-компаниями. Ранее в этом году SWIFT представила стандарт API Pay Later.

Новый стандарт уже доступен для применения разработчикам API.

ЯВЛЕНИЕ «СЕРАФИМА»

Система быстрых платежей появилась в мессенджере «Серафим». Разработчики наглядно продемонстрировали работу встроенной СБП на VII ежегодном всероссийском форуме «Взгляд в цифровое будущее».

О планах Банка России внедрить СБП в «Серафим» стало известно в августе — в качестве модели развития разработчики взяли китайский WeChat. Для использования функции быстрых платежей нужно иметь аккаунт на «Госуслугах» и идентифицировать лицо. Мессенджер позиционируется как решение для обеспечения безопасности коммуникаций в госкорпорациях и крупном бизнесе. Его пользователи могут обмениваться текстовыми сообщениями и проводить аудиоконференции.

Новости подготовила
Анна Воробьева

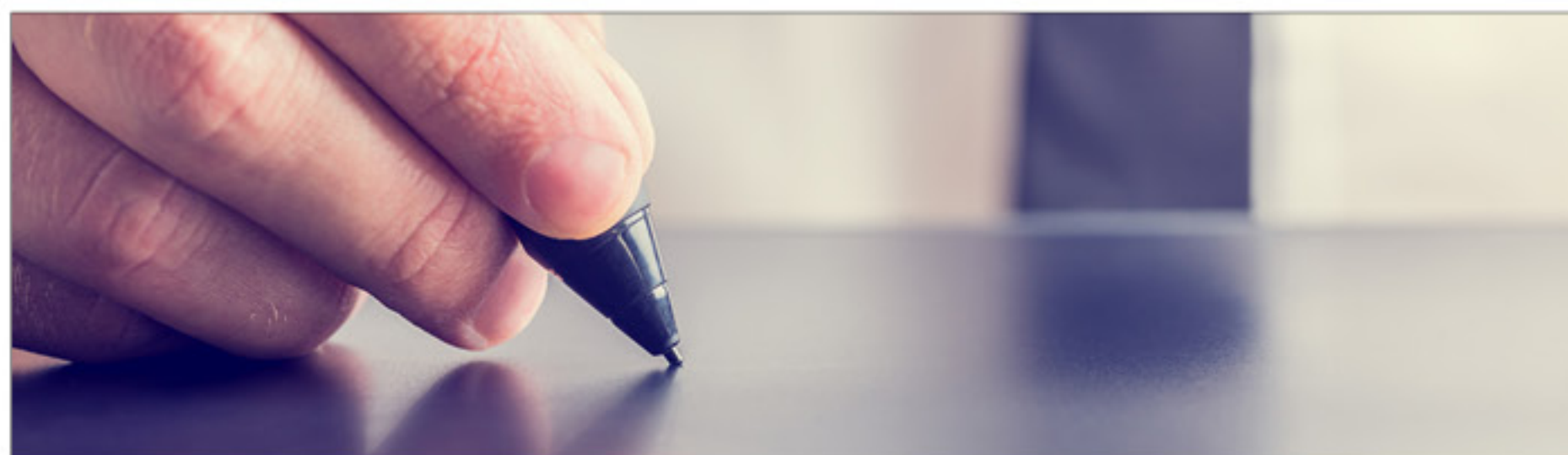
ЦИФРОВАЯ ПОДПИСЬ ДЛЯ ВСЕХ

Правительство планирует запустить двухлетний эксперимент по выдаче и использованию облачной цифровой подписи. Сегодня в РФ можно использовать три вида цифровой подписи: простую, усиленную неквалифицированную и усиленную квалифицированную. Самые широкие полномочия у последней, поскольку это аналог собственноручной подписи. Во время эксперимента будет использоваться именно она.

Облачную цифровую подпись можно будет получить дистанционно (например, в ЕБС). Госструктуры, компании и граждане смогут дистанционно

оформлять бумаги для регистрации недвижимости, договоры об оказании услуг связи, документы для получения банковских гарантий и так далее.

За работу системы будут отвечать «Ростелеком» и НИИ «Восход» (подведомственен Минкомсвязи). По итогам эксперимента «Ростелеком» может стать оператором единой системы. Преимущество облачной цифровой подписи — в отсутствии необходимости установки специального ПО и флешки. По словам экспертов, среди возможных проблем — пробелы в законодательстве, проблемы с информационной безопасностью и психологический фактор.



СУПЕРКОМПЬЮТЕР СТАНЕТ МОЩНЕЕ

Производительность мощнейшего российского суперкомпьютера «Ломоносов-2» вырастет почти в полтора раза. Об этом сообщил Виктор Садовничий, ректор МГУ им. Ломоносова, на форуме «Цифровизация-2019».

Мощность суперкомпьютера увеличится с 5 до 7,2 петафлопсов (количество операций над числами с плавающей запятой, которые может выполнить вычислительная машина за секунду: 1 петафлопс — 1000 трлн операций). Сегодня «Ломоносов-2» используется более 3 тыс. пользователей из научных центров и университетов.

Суперкомпьютер заработал на базе МГУ в 2014 году. Со слов Виктора Садовничего, увеличение производительности ожидается не ранее, чем через восемь месяцев. «Скорее всего, это будут многоядерные процессоры вместе с ускорителями, некоторыми — скорее всего, графическими», — сказал ректор.

Точная информация об оборудовании, за счёт которой компьютеру добавят мощности, должна появиться после утверждения технического проекта и финансирования.





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

© АО «Лаборатория Касперского», 2019. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей

ВЫЗОВЫ НА УРОВНЕ ГОСУДАРСТВЕННОЙ КИБЕРБЕЗОПАСНОСТИ

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ ВИЦЕ-ПРЕЗИДЕНТ
ПАО «РОСТЕЛЕКОМ» ПО ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ИГОРЬ ЛЯПУНОВ



Игорь ЛЯПУНОВ
вице-президент
ПАО «Ростелеком»
по информационной
безопасности

О РОЛИ SOC

— Тема пленарной дискуссии SOC-Форума — «Роль центров мониторинга в современной системе информационной безопасности РФ». А какую роль они играют в ИБ с вашей точки зрения?

— На сегодняшний день динамика и сложность угроз в глобальном цифровом пространстве такова, что центры мониторинга, различные CERT и ГосСОПКА играют ключевую роль в вопросах защиты. Посмотрите, как изменился в последнее время даркнет: аналитики нашего центра мониторинга и реагирования на кибератаки Solar JSOC фиксируют 2–3 принципиально новых типа угроз ежемесячно и 5–6 новых хакерских инструментов еженедельно. Преступное сообщество работает очень быстро и слаженно, и для эффективного противодействия требуются структуры, способные обеспечить адекватную скорость реакции и располагающие максимально полной картиной инструментария и методов атак, которые есть у противника в каждый момент времени.

— Можно подробнее?

— Какой была динамика атак, например, лет 5 назад? По нынешним меркам, события развивались как в замедленной видеосъемке. Условно, обнаруживалась уязвимость в ОС Windows, через месяц Microsoft выпускал патчи, и ещё примерно через три месяца появлялись эксплоиты. То есть с момента выявления уязвимости до момента атаки у компаний был временной запас в 3–4 месяца, чтобы подготовиться и защититься.

Сейчас эксплоиты иногда появляются уже через сутки после публикации информации о серьёзных уязвимостях. При этом средний срок закрытия, например, критичных уязвимостей в операционной системе даже в очень передовом с точки зрения информационной

безопасности сегменте, банках, в среднем составляет 42 дня, в ТЭК — 66 дней, в госорганах — 134 дня. Это даёт широкий простор для массовых атак, поэтому они происходят всё чаще.

Злоумышленники атакуют целевые инфраструктуры, используя самое слабое звено — человека. Фишинг и социальная инженерия сейчас являются дешёвым и одним из самых эффективных инструментов, позволяющих быстро доставить в атакуемую компанию вредоносное ПО, эксплуатирующее новые, ещё не закрытые уязвимости.

Модель управления безопасностью должна соответствовать таким скоростям, поэтому ключевым элементом системы ИБ становится организационно-техническая конструкция, позволяющая моментально видеть изменения, реагировать на них, управлять ими. В этом особенно и заключается роль центров мониторинга в национальной кибербезопасности.

ПРОФИЛЬ ЗЛОУМЫШЛЕННИКА

— Как меняется профиль злоумышленника?

— Даркнет как таковой делает многие нелегальные продукты и сервисы более доступными, появился спрос и на инструменты для организации кибератак. Их доступность — как физическая, так и экономическая — сейчас приводит к притоку капитала в этот сегмент. По нашим оценкам, бюджет даркнета составляет несколько миллиардов рублей только в России. Это способствует формированию более взрослого, серьезного рынка. Скажем, появляется определенная стандартизация — сложившиеся практики заключения сделок и контроля исполнения условий договора с обеих сторон. Формируется понимание, какие бизнес-модели наиболее выгодны,

этот рынок начинает всё больше напоминать любой другой сегмент, лежащий в правовом поле, — вплоть до инструментов маркетингового продвижения.

— И насколько компании готовы противостоять таким угрозам?

— Большинство, конечно, совсем не готовы. Это и есть вызов для страны сегодня.

ПРО МОДЕЛЬ УПРАВЛЕНИЯ

— Вы сказали, что модель управления безопасностью должна измениться?

— Сегодня акцент в ИБ смещается с отражения атаки на её ранее обнаружение. Угрозу важно выявить быстро, чтобы дать защищаемым резерв времени для полноценного противодействия и минимизации ущерба.

— То есть ситуация изменилась принципиально?

— Если говорить образно, раньше мы строили вокруг компании высокую стену и следили, чтобы через неё никто не перелез. Теперь у компаний нет чёткого периметра, и его безопасность серьёзной роли в обеспечении защиты уже не играет. Сегодня наша задача — не столько охранять стену, сколько, прежде всего, увеличить дистанцию от входа в инфраструктуру до защищаемого актива. База данных или расчётный узел в банке не должен быть виден «с порога». Защита должна быть эшелонированной, разбитой на этапы, на каждом из которых мы можем обнаружить и остановить атакующего.

Но основная сложность не в отражении атаки, это как раз более механическая задача. Главное сегодня — иметь хороший инструментарий и отлаженные процессы ИБ для выявления угрозы на максимально раннем этапе.

ПРО СИТУАЦИЮ В ОТРАСЛИ

— Чего вы ждёте от дискуссии на SOC-Форуме?

— Программа SOC-Форума в этом году очень обширна. Помимо технологических и процессных задач в части противодействия угрозам из даркнета, мы обсудим и задачи информационной безопасности, которые ставит перед нами цифровая трансформация.

Во-первых, это внутренние, структурные вызовы. В саму модель современного бизнеса априори заложены постоянные изменения. Это и модернизация процессов, и agile-модель, и необходимость в максимально коротком time-to-market — быстром выпуске новых коммерческих продуктов или новых релизов. Всё это формирует новые задачи информацион-

ной безопасности. От неё сейчас требуются не просто другие скорости, а другие подходы к защите. Поэтому, прежде всего, мы, как отрасль, должны себе признаться, что модель управления безопасностью должна быть перестроена. Нет больше мира заблокированных атак, есть постоянный процесс по совершенствованию методов их раннего выявления и оперативного реагирования.

Мы также должны осознать и признать, что переход к этой новой модели будет весьма сложным. Он требует и серьёзного технологического развития, и изменения процессов в управлении ИБ, и подготовки кадров. То, что нам предстоит обсудить, это уже не теоретизирование и футурология, а совершенно практические вещи — как отрасли соответствовать новым вызовам.

Ещё одна важная проблема, которая возникает в контексте цифровой трансформации, — переход к интернет-связанности самых чувствительных сегментов, таких как АСУ ТП, в том числе на промышленных и топливно-энергетических предприятиях. Эти сегменты, ранее изолированные от глобальной сети, часто больше таковыми не являются, а значит, подвергаются гораздо большему числу киберугроз. При этом ввиду специфики и нишевости технологий АСУ ТП отработанных механизмов защиты пока нет, очень мало и квалифицированных специалистов.

— Вы имеете в виду атаки на КИИ?

— Да, в том числе. Сейчас защита КИИ становится сложной задачей, потому что объекты критической инфраструктуры вызывают повышенный интерес, в том числе у высококвалифицированных злоумышленников. Там мы сталкиваемся и с бесфайловым ПО, и с вредоносным ПО, способным обходить «песочницы», и с тщательным уничтожением киберпреступниками любых следов своей деятельности в инфраструктуре.

Защита объектов КИИ — сложная задача: нет нужных отечественных технологий, или их недостаточно, или их зрелость пока невысока. Безопасники часто не имеют необходи-

Злоумышленники атакуют целевые инфраструктуры, используя самое слабое звено — человека. Фишинг и социальная инженерия сейчас являются дешёвым и одним из самых эффективных инструментов

мого опыта, нет кадров, которыми необходимо насыщать службы ИБ. Это, повторюсь, вызов, и вызов на уровне не отдельных организаций или даже отрасли, а на уровне национальной безопасности. В рамках SOC-Форума эти вопросы будут обсуждаться и на сессии с регуляторами, и на практической секции по защите АСУ ТП.

ПРО РЕГУЛЯТОРОВ

— Напрашивается вопрос: а что по этому поводу думают, говорят регуляторы?

— Они тоже видят, как меняется ситуация, и соответствующим образом совершенствуют требования к информационной безопасности организаций.

Первое важное изменение состоит в том, что это уже не требования к средствам защиты, а требования к процессам обеспечения информационной безопасности. Для этого организации должны иметь квалифицированные кадры, средства, ресурсы.

Второе — смещение акцента с ответственности за невыполнение требований на ответственность за инциденты. Раньше все боялись проверок регуляторов и строили пресловутую бумажную безопасность. Новые подходы будут толкать субъекты КИИ к тому, чтобы обеспечивать фактическую защищённость. Но как это делать правильно? На SOC-Форуме об этом тоже будем говорить.

ПРО ДЕФИЦИТ КАДРОВ И КИБЕР-ГРАМОТНОСТЬ НАСЕЛЕНИЯ

— Вы упоминали о проблеме дефицита кадров в отрасли. Как её решает «Ростелеком-Солар»?

— Кадровый голод в информационной безопасности действительно очень силен. Многие игроки рынка идут по пути переманивания специалистов, но это скорее разрушает нашу отрасль. Я считаю, что кадры нужно выращивать, и это — наша стратегия. Мы активно работаем с вузами по всей России — Университетом Лобачевского, Дальневосточным федеральным университетом,

Самарским национальным исследовательским университетом, Тихоокеанским государственным университетом и другими. Берём на стажировку студентов четвертых-пятых курсов, лучшим предлагаем работу в штате. За два-три года они превращаются в сильных ИБ-специалистов.

С прошлого года мы запустили совместный проект с образовательным центром «Сириус»¹. «Ростелеком» является организатором всероссийской олимпиады «Кибервызов», после чего наши эксперты отбирают победителей — тех, кто поедет в «Сириус» на образовательную программу по кибербезопасности. В прошлом году это были школьники старших классов, в этом мы впервые создали такую программу для студентов. Она включала теоретические и практические занятия по защите АСУ ТП, веб-приложений, реверс-инжинирингу и форензике с ключевыми экспертами отрасли. Завершающим этапом стали масштабные киберучения.

Сейчас стартует всероссийская олимпиада Кружкового движения Национальной технологической инициативы (КД НТИ) по профилю «Информационная безопасность», задания для которой разрабатывались в сотрудничестве с «Ростелеком-Солар». Она ориентирована на школьников старших классов, и её финалисты также отправятся в «Сириус». В этом году школьная программа по кибербезопасности, помимо базовых аспектов, будет сфокусирована на защите интернета вещей. Каждый раз мы стремимся дать талантливым ребятам знания и навыки в актуальных, развивающихся сферах, защита которых уже завтра станет задачей отрасли информационной безопасности.

Конечно, это очень долгосрочные вложения, но без создания такой базы, кадрового потенциала для отрасли ИБ, скоро будет невозможно оставаться конкурентоспособными в цифровом пространстве.

— Сколько студентов у вас работают сейчас?

— Когда в прошлом году Solar Security вошла в состав «Ростелекома», нас было двести человек. Сейчас нас больше шестисот. Понятно, что набрать за год четыреста человек с рынка было бы просто невозможно. Больше половины вакансий нам удалось закрыть из вузов. Это те кадры, которые мы сами подготовили, первые плоды нашего труда.

¹ Репортаж «Искать таланты интересно!» читайте на стр. 110

Раньше все боялись проверок регуляторов и строили пресловутую бумажную безопасность. Новые подходы будут толкать субъекты КИИ к тому, чтобы обеспечивать фактическую защищённость



Но, конечно, мы учим и воспитываем ребят не только для себя. Из одного вуза мы берём на стажировку примерно шестьдесят человек. Впоследствии у нас остаются работать 10–15 из них. Остальных — обученных и адаптированных к профессии — выпускаем на рынок. И дальше они работают в других компаниях — у наших заказчиков, конкурентов... В этом мы видим свою системообразующую, созидательную роль.

— В этом году вы также запустили проект по повышению кибербезопасности населения. Расскажите о его целях и задачах.

— Как я уже говорил, люди остаются основным вектором атак, поэтому повышение грамотности населения в области информационной безопасности — необходимая составляющая процесса по обеспечению защищённости страны в целом, наряду с развитием технологий, деятельностью регуляторов и созданием общенациональных процессов по выявлению и предотвращению кибератак.

Мы обладаем достаточными ресурсами и компетенциями для реализации такого проекта, и потому видим это своей социальной миссией.

Уже сейчас мы проводим открытые уроки по кибербезопасности в школах и вузах, готовим книгу по безопасному поведению в интернете для детей. В ближайших планах ещё много масштабных проектов в этой сфере.

ПРО АУТСОРСИНГ

— Что сегодня происходит на российском рынке сервисов ИБ?

— Ключевая проблема заказчиков та же — отсутствие кадров. Многие, как и мы, работают над этим — сотрудничают с вузами, поддерживают кафедры ИБ, но защищаться нужно здесь и сейчас. И единственный вариант получить хороший уровень защиты, особенно в регионах, — аутсорсинг, сервисная модель. Она даёт компаниям не просто технологию или набор инструментов — средств защиты, а работающую функцию.

В 2012-м году, когда мы только начинали, нам говорили: «Вы безумные — никогда ИБ не будут отдавать на аутсорсинг». Solar Security тогда был пионером, стартапом, и на этот рынок стремились не многие. Сегодня всё изме-

Три кита, на которые опирается кибербезопасность сегодня, — это экспертиза, кадры и технологии. Мы обладаем, пожалуй, самыми широкими возможностями в этих сферах

нилось. У государственных организаций и бизнеса выкристаллизовался перечень функций ИБ, которые выгоднее и эффективнее передавать на аутсорсинг. Созрел спрос, и на этот рынок пришли крупные игроки: «Ростелеком», Сбербанк. Ряд компаний заявляет об инвестициях в эту область. Ожидаемо для нас, сервисы кибербезопасности превращаются в серьёзную индустрию.

— Можете рассказать о заказчиках?

— У нас много компаний-заказчиков в регионах, а в ближайшее время перезаключаем крупный контракт с банком «Тинькофф». Он стал одним из первых наших заказчиков, и сейчас мы серьёзно расширяем сотрудничество. Но самое интересное и показательное — к нам стали обращаться госорганы. Уровень зарплат в этом сегменте ниже, чем в коммерческом, им трудно нанимать много специалистов в штат, а требования к безопасности очень высоки. И конечно, им выгодно отдавать безопасность на аутсорсинг.

— А какова динамика вашего нового направления Solar MSS — управляемых сервисов кибербезопасности?

— В прошлом году первыми в России запустили огромную платформу по предоставлению сервисов кибербезопасности вместе с инфраструктурой и каналами «Ростелекома». Она построена на технологии программно-определяемых сетей SD-WAN (software-defined wide area network), по сути, это прорыв для России. Это программно-определяемые глобальные сети, территориально распределённые. С помощью этой технологии мы доставляем клиентам сервисы ИБ, и, конечно, мы их увязываем в единую экосистему с нашим центром мониторинга. Это мировой тренд, и тут мы идём в фарватере.

Управляемые сервисы кибербезопасности Solar MSS быстро набирают популярность, и мы уже серьёзно расширили список сервисов и технологий, поставляемых в рамках платформы.

— Есть ли у вас конкуренты? Как вы к ним относитесь?

— Мы — лидеры рынка, по сути, естественная монополия. Но на самом деле мы очень

ждем, когда на рынок выйдут зрелые компании, готовые инвестировать в развитие. Здоровая конкуренция только способствует развитию отрасли и усилению национальной кибербезопасности.

ДРАЙВЕРЫ РЫНКА

— И всё же, кто, на ваш взгляд, является драйвером рынка — государство, корпорации, цифровая трансформация как тренд?

— Это общие усилия и общая заслуга. На развитие отрасли сильно повлияли и кибератаки, в том числе политически мотивированные, они способствовали росту спроса на защиту от киберугроз.

Драйвером выступают и корпорации, инвестирующие в отрасль. Они дают вендорам возможность развивать инновационные технологии, без которых кибербезопасность просто невозможна.

Например, Solar Security с самого начала развивает свои уникальные технологии, в которые решил инвестировать «Ростелеком». Наш продукт для анализа исходных кодов на уязвимости считается сегодня одной из лучших в мире. Количество языков программирования, которые мы поддерживаем, превышает зарубежные аналоги, не говоря об уникальной технологии анализа бинарных файлов. Мы также развиваем технологии в области контроля коммуникаций, защиты от утечек, интегрируя в него самые передовые технологии анализа поведения пользователей на базе машинного обучения.

ПРО ЦЕЛЬ

— Какие цели стоят перед «Ростелеком-Солар» на ближайшие годы?

— Мы являемся частью «Ростелекома» — национального провайдера цифровых услуг и сервисов. Это ключевой поставщик традиционной телекоммуникационной инфраструктуры и связи, услуг ЦОД и сервисов кибербезопасности. Это даёт нам всё необходимое для обеспечения фактической защищённости цифровых активов всей России.

Три кита, на которые опирается кибербезопасность сегодня, — это экспертиза, кадры и технологии. Мы обладаем, пожалуй, самыми широкими возможностями в этих сферах, и это накладывает на нас, как на лидера рынка, ответственность за реализацию самых масштабных задач.

— Спасибо.

Беседовал Игорь Некрасов

АМУЛЕТЫ НЕ ЗАЩИЩАЮТ ОТ КИБЕРПРЕСТУПНИКОВ

ПОЧЕМУ КЛАССИЧЕСКИЙ ПОДХОД УСТУПАЕТ ДОРОГУ АУТСОРСИНГУ ИБ?

О тенденциях в информационной безопасности и том, каким требованиям должен соответствовать современный SOC, рассказывает директор блока управляемых сервисов компании BI.ZONE Муслим Меджлумов.

— Муслим, какие ключевые тенденции вы фиксируете сейчас в сфере информационной безопасности?

— В последние годы мы наблюдаем, что, в банковском секторе, да и в других сферах, «работают» несколько преступных группировок, которые используют достаточно продвинутые техники. Чтобы оперативно выявлять такую активность и реагировать на сложные инциденты, финансовым организациям приходится все больше внимания уделять проактивной защите, выявлению таргетированных атак, поэтому популярность набирает направление threat hunting. Речь не о попытке предотвратить инцидент, а об обнаружении угрозы на как можно более ранней стадии с целью предотвращения последствий. Иными словами, вы исходите из принципа, что вас могут взломать и, скорее всего, гарантировать обратное не сможете, но ваша первоочередная задача — обнаружить злоумышленника до того, как он успеет получить доступ к защищаемому активу.

Второй момент: преступные группировки всё чаще действуют одновременно по множеству организаций, зачастую находящихся в разных регионах мира. В этих условиях огромное значение приобретает быстрый обмен информацией об инцидентах. В рамках нашего SOC этот процесс протекает бесшовно: сотрудники, обнаружив атаку в одной организации, используют индикаторы компрометации для проверки их наличия у других заказчиков и транслируют полученную информацию в Платформу обмена данными о киберугрозах — совместный проект BI.ZONE и Ассоциации банков России.

Самым слабым звеном в обеспечении информационной безопасности был и остаётся человек. В связи с популярностью атак, используя

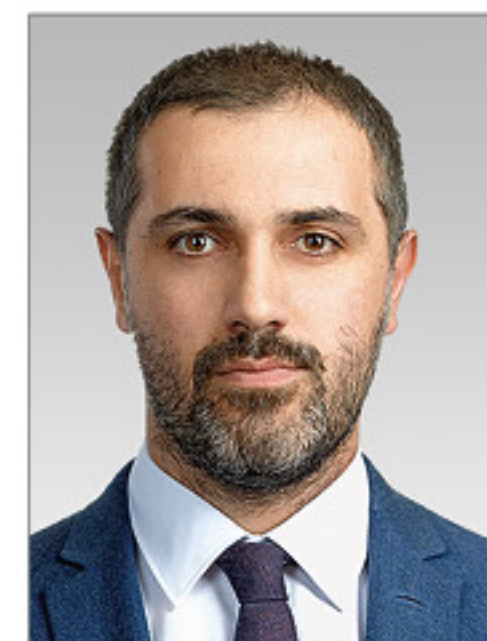
щих методы социальной инженерии, заказчики стали всерьёз заботиться о повышении киберграмотности сотрудников. Практика показывает, что любые усилия безопасников может свести на «нет» всего один работник, открывший, например, фишинговое письмо и создавший таким образом брешь, через которую можно атаковать организацию. Мы проводили исследования, и минимум трое из десяти сотрудников ведутся на уловки злоумышленников при фишинговой атаке.

Четвёртая тенденция — более активное государственное регулирование. Из интересного, помимо такого тектонического сдвига, как ФЗ-187, ввели стандарт в сфере аутсорсинга кибербезопасности — СТО БР ИББС-1.4–2018. Банк России понимает, что не у всех участников финансового сектора хватает ресурсов для самостоятельного обеспечения процессов кибербезопасности, и многие организации будут прибегать к услугам аутсорсеров для повышения эффективности защиты при одновременном сокращении затрат.

— Какие изменения произошли в сегменте аутсорсинга ИБ помимо усиления госрегулирования?

— Я бы сказал, что происходит переоценка ценностей. Заказчики стали понимать, что модель «купи и будет хорошо» больше не работает. Все эти SIEM без качественных сценариев выявления атак, Anti-APT без сбора телеметрии с конечных узлов и написания сложных правил детектирования тактик поведения злоумышленника, межсетевые экраны с пачкой устаревших правил — бесполезны без сильной команды специалистов, которых на рынке уже просто не осталось. Всех, кого можно было, «пропылесосили» с пяток сильных игроков. Для разумного CISO, которому «ехать, а не шашечки», это ещё один фактор, который подталкивает его в сторону аутсорсинга.

В сытые годы заказчики «палили» бюджеты, не сильно беспокоясь о реальном уровне защищённости. На этом активно паразитировали



Муслим МЕДЖЛУМОВ
директор блока
управляемых
сервисов компании
BI.ZONE

многие вендоры и интеграторы, так как можно было делать продукты-«пустышки» и проекты-«бумажки». В результате за долгие годы такого творчества у них не сформировалась экспертиза, позволяющая создать систему или решение, которые действительно помогают защитить от реальных атак, а не выступают в качестве амулета. Конечно, за это время появились сильные конкуренты, которые способны отвечать за эффективность работы своих продуктов или услуг, что, кстати, позволяет им достойно выступать не только на локальном рынке. На мой взгляд, первый тип как класс должен исчезнуть, уступив место молодым.

И еще одна интересная тенденция — развитие подходов по управлению угрозами на стороне поставщиков. Простыми словами, злоумышленник понимает, что бессмысленно тратить силы на пробитие бетонной стены заказчика, когда рядом есть калиточка, через которую можно пройти, отодвинув шпингалет. Переводя на профессиональный язык, это означает, что, даже при качественной защите собственной сети, всегда остаётся шанс развития атаки через сеть подрядчика, с которым взаимодействует организация, например, через компанию, которая выполняет заказную разработку ПО. К сожалению, эффективно бороться с этой проблемой научились еще не многие, и это направление будет активно развиваться.

— Тенденции определяют спрос со стороны заказчиков на различные решения и услуги. Какие из них наиболее востребованы сейчас, с учётом всего сказанного?

— В контексте аутсорсинговых сервисов можно выделить четыре типа заказчиков. Первые обладают достаточными финансовыми ресурсами, чтобы поддерживать высокий уровень информационной безопасности. Они охотно инвестируют и в решения, и в обучение персонала, и в организацию собственных SOC. Такие заказчики реже идут в аутсорсинг, предпочитая in-house решения и команду.

Для них передача функций ИБ на аутсорсинг это скорее возможность сосредоточиться на достижении «операционного совершенства» и не плодить внутри экзотическую экспертизу, например, тестирование на проникновение, Digital Forensics & Incident Response, Malware Response (DFIRMA), защиту бренда, выстраивание процедур безопасной разработки, киберразведку и прочие.

Вторая категория относится к тем, кто только начинает делать первые шаги в ИБ, и им нужно сократить отставание за счёт внешнего поставщика. Есть третья группа, самая многочисленная: организации, которые осознают проблему кибербезопасности и обладают финансовым ресурсом, но не готовы инвестировать в команду и решения, которые не связаны с профильным бизнесом. Им помощь аутсорсеров интереснее всего, причём таким заказчикам зачастую требуется не только SOC, но и дополнительные сервисы.

Наконец, последняя группа — это заказчики, которые слабо осознают последствия от кибератак на их бизнес, у них отсутствует возможность вкладывать значительные бюджеты в защиту, поэтому они покупают сервисы, исходя из принципа «сколько не жалко». Перевод капитальных затрат в операционные для них является важным преимуществом. При выборе услуг предпочитают фокусироваться на тех, что действительно важны здесь и сейчас, например, безопасность электронной почты, защита веб-сайта от взлома или отражение DDoS-атак. Увы, выбор сервис-провайдеров для данной категории заказчиков сильно ограничен, так как в основном цены на подобные услуги держатся на уровне бутиковых.

— На что нужно обращать внимание заказчикам при выборе поставщика услуг SOC?

— Конечно, крайне важна автоматизация работы аналитиков и повышение скорости реакции на инциденты. Это принципиальное требование, если учесть, что сейчас примерно 70% времени у специалистов уходит на сбор информации об инциденте и работу с ложными срабатываниями. То есть, фактически большую часть времени аналитик тратит на «белый шум». Современный SOC должен максимально автоматизировать этот процесс, сокращая как время на анализ «белого шума», так и время реагирования на сам инцидент.

Общаясь с заказчиками, мы также видим, что у них есть потребность в услуге SOC индивидуального пошива. Клиенты хотят, чтобы

Злоумышленник понимает, что бессмысленно тратить силы на пробитие бетонной стены заказчика, когда рядом есть калиточка, через которую можно пройти, отодвинув шпингалет

мы лучше понимали их инфраструктуру, бизнес-процессы. Им недостаточно просто получать информацию об инциденте с набором рекомендаций, они хотят, чтобы эта информация была обработана и проверена с учётом особенностей инфраструктуры и сразу доходила до нужных сотрудников внутри компании, таким образом сокращалось время реагирования на инциденты, и заказчик меньше тратил своих ресурсов, работая только с реальными инцидентами.

Третий момент, на который я хотел бы обратить внимание, это максимальная прозрачность со стороны аутсорсера при предоставлении услуг. Заказчик, отдавая свою инфраструктуру посторонней компании, принимает ряд рисков от такого взаимодействия. И он хочет и должен понимать две принципиальных вещи. Как выстроены процессы обеспечения кибербезопасности у сервис-провайдера? Из чего состоит приобретаемый сервис — какие правила настраиваются, какие технологии используются, какая логика выстроена внутри сервиса и, что немаловажно, как часто провайдер обновляет и предоставляет контент?

— Как вы решаете эту задачу?

— Мы запустили уникальное для российского рынка решение — SOC-портал BI.ZONE. Это веб-ресурс, где полностью отражается информация о подключаемых сервисах, обращениях клиента и статусах инцидентов. Подробная отчётность, реализованная наглядно и в удобном интерфейсе, позволяет в режиме онлайн отслеживать процессы кибербезопасности, переданные на аутсорсинг. Портал даёт абсолютно прозрачное понимание состава сервиса и получаемых результатов, а также позволяет усилить контроль за командой SOC.

Пожалуй, ещё одна востребованная особенность SOC-портала — нативная интеграция с Главным центром ГосСОПКА. Теперь сведения об инцидентах субъектов КИИ автоматически отправляются в НКЦКИ, без дополнительного взаимодействия, подключений и интеграционных работ на стороне заказчика.

— Вы рассказали, какие решения и услуги аутсорсеров сейчас наиболее востребованы. Но наверняка даже больше этого востребована экспертиза, то есть знания и умения специалистов компаний-аутсорсеров.

— Существует общее правило: любое решение, даже самое современное и совершенное, без специалистов, умеющих правильно им управлять, напоминает болид «Формулы-1» без

Любое решение, даже самое современное и совершенное, без специалистов, умеющих правильно им управлять, напоминает болид «Формулы-1» без пилота: красиво, дорого, но не эффективно

пилота: красиво, дорого, но не эффективно. Как я уже говорил, на рынке серьёзный дефицит опытных «пилотов», а для их удержания необходимо платить высокую зарплату и давать им возможность расти профессионально. Ещё одна аналогия с пилотом: ему, чтобы развиваться и удерживать позиции, необходимо постоянно участвовать в гонках, так же как и безопаснику нужно постоянно заниматься инцидентами. А в одной организации их количество или сложность могут быть недостаточными. Передача процессов кибербезопасности на аутсорсинг позволяет уйти от необходимости решать эту проблему. Сервис-провайдер в этом плане имеет преимущество: сотрудники работают одновременно со множеством заказчиков, а значит, с разной спецификой, набором СЗИ, внутренними процессами обеспечения ИБ.

— Наверняка вы поддерживаете с заказчиками постоянную обратную связь, и они делятся информацией о том, насколько им помогают сервисы вашей компании. Какие позитивные моменты сотрудничества они отмечают в первую очередь?

— Главная позитивная оценка для меня и для компании в целом в том, что, обратившись к нам за одним сервисом, заказчики довольно быстро начинают либо распространять его на все свои зависимые и/или дочерние общества, либо подключать другие сервисы BI.ZONE. Пожалуй, основную ценность наших сервисов можно прочувствовать, подключив как минимум 2–3 из них, так как они начинают работать в единой экосистеме, которая зонтиком объединена на уровне SOC.

Ещё одно преимущество, которое отмечают заказчики, возможность опробовать наши сервисы. Какое-то время они пользуются услугой бесплатно, убеждаются в её эффективности, а затем могут либо подключиться к ней уже в полном объёме, либо отключиться. На время пилотного проекта заказчикам доступны все функции и управление каждой услугой в едином личном кабинете.



Александр БОДРИК
управляющий партнер
бизнес-инкубатора
по кибербезопасности
Cyberlands B.V.,
вице-президент
по ИБ ISACA Moscow
Chapter

ПЕРВЫЙ ПОСЛЕ SOC'A

УПРАВЛЕНИЕ КИБЕРНАВЫКАМИ ПОЛЬЗОВАТЕЛЕЙ СТАНОВИТСЯ ВАЖНЕЙШИМ СЕРВИСОМ ДЛЯ КЛИЕНТОВ MSSP

За последние четыре года на рынке появилось около двух десятков коммерческих провайдеров управляемых услуг информационной безопасности (Managed Security Services Providers—MSSP). Исторически их портфель услуг включает мониторинг кибербезопасности (в просторечии SOC) и «все остальное», но в последнее время выделяется второй сервис, такой же востребованный и важный для клиентов MSSP: управление кибернавыками пользователей. К примеру, крупнейший мировой MSSP—IBM Security Services—запустил сервис Managed Security Awareness на базе американской платформы Wombat, а крупнейший российский—Ростелеком—на базе российской платформы Антифишинг.

Мониторинг хорош универсальностью: все организации владеют сетевой инфраструктурой, серверным парком, все подвергаются тем или иным угрозам—шифровальщикам, целевым атакам, атакам на ДБО... Аналогично и управление кибернавыками: бизнес клиентов MSSP делают люди, и развитие их навыков всегда важная часть повестки топ-команды клиентских организаций. А сегодня, с ростом киберугроз, тем более... И продукты, позволяющие решать такие задачи, по мнению соответствующего магического Gartner (2018 г.), будут расти по выручке со скоростью 56% как минимум до 2022 г.

СТРУКТУРИРОВАННЫЙ ПРОЦЕСС

Очевидно, что такой сервис для крупного MSSP в России, задачей которого является помощь клиентам из разных индустрий с решением проблемы «человеческого фактора» в информационной безопасности, не может состоять из одного технологического решения или набора курсов. Зрелый мощный MSSP выполняет не только коммерческую, но и социальную функцию—помогает клиентам постепенно растить программы повышения осведомлен-

ности и управления кибернавыками сотрудников (далее—Программы). Например, используя модель «Введи-Обучи-Проверь-Исправь-Введи (ВОПИ)».

Рассмотрим эту модель.

Этап «Введи» фокусируется на определении, установке и внедрении обязательных к исполнению в организации норм по кибербезопасности. Согласитесь, без утвержденных политики ИБ и политики допустимого использования информационных ресурсов организации говорить не о чем. Нет норм, которые являются стандартом поведения пользователей, а значит, нет фундамента-опоры-каркаса выстраиваемой системы.

Этап «Обучи» пересекается с предыдущим в части внедрения политик, однако является непрерывным: обучение должно происходить регулярно. В корпоративной практике это проводится один раз каждые 1–2 года, а также включает обучение при введении новых технологий или по специфичным триггерам.

Этап «Проверь» позволяет понять, что пользователь усвоил в части знаний (помнит ли он термины, усвоил ли понятия ИБ), а также навыков—будет ли он бездумно кликать по ссылке или превратится в союзника службы кибербезопасности и отправит подозрительное письмо на её «горячий» ящик.

Этап «Исправь» создаёт обратную связь для пользователей, помогая им закрывать пробелы в своих знаниях и навыках путём повторного обучения или общения с ответственными службами. На этом этапе важно установить доверительные отношения с пользователями, для чего крупнейшие корпорации обычно делегируют эту работу локальным офицерам кибербезопасности в регионах, или отделам/управлениям режима кибербезопасности в центральном аппарате.

По мере прохождения этапов иногда становится понятно, что нужно ввести новые нормы кибербезопасности—вслед за новыми техно-

логиями, но иногда разумно отменить и старые, создавая тем самым цикл контроля качества Программы.

МОДЕЛЬ ЗРЕЛОСТИ ПРОГРАММЫ

Приведённые этапы описаны в статике, что не применимо к реальной жизни. На деле, это колесо крутится много раз, что затрудняет его использование «в лоб» в корпорации. Соответственно предлагается применять управляемую модель зрелости Программы (Таблица 1).

На каждом из уровней зрелости MSSP может предложить свой набор услуг: от поддержки в разработке политик ИБ до цифровой платформы

повышения осведомлённости, тем самым поддерживая клиента по мере роста его потребностей.

Повышение осведомленности и развитие кибернавыков пользователей видится той точкой пересечения служб ИБ и сервис-провайдеров, где без существенных проектных рисков и миллиардных инвестиций в технологические решения и десятки операторов SOC возможно быстро приносить и демонстрировать пользу бизнесу и конкретным бизнес-руководителям.

УРОВЕНЬ ЗРЕЛОСТИ						
	0 «Зеро»	1 «Начальный»	2 «Базовый»	3 «Стандарт»	4 «Развитый»	5 «Ведущий»
Организация	Не существует ответственного за реализацию программы	Реализация программы вменена CISO (неформально)	Программа выделена в виде проектов, есть проектный менеджер	+ менеджер по обучению	+ интеграция с обязанностями менеджеров по ИБ подразделений и регионов компании	+ KPI по реализации программы назначены CISO и/или CIO
Технологии	Отсутствуют	Для донесения информации исп. корпоративный портал	+ система обучения пользователей	+ система проверки практических навыков	+ система контроля показателей и интеграции с другими процессами	+ технологический стэк охватывает все подразделения и регионы компании
Процессы	Не утверждена политика ИБ и правила допустимого использования	Утверждена политика ИБ и правила допустимого использования	+ процесс обучения пользователей	+ процесс проверки практических навыков пользователей	+ процессы интегрированы с другими процессами ИБ: управление доступом, управление инцидентами и др.	+ процессы работают в «цифровом» режиме с минимизацией участия человека — от проверки навыка до реагирования на инцидент и др.
Культура	Персонал организации не понимает важности ИБ, не знает кто отвечает за ИБ и с кем советоваться	+ персонал знает кто отвечает за ИБ	+ персонал понимает основные понятия ИБ	+ персонал коммуницирует со службой ИБ, сообщает о потенциальных инцидентах	+ персонал проактивно консультируется со службой ИБ	+ персонал вовлекает службу ИБ в стратегические проекты
Стратегия	Программа не отражена в Стратегии ИБ, не имеет спонсора из состава топ-команды	+ включена в Стратегию ИБ	+ имеет спонсора из состава топ-команды	+ расширена на клиентов организации (например, в банковском секторе)	+ трансформирована из отдельной программы в одно из измерений успешности Стратегии ИБ	+ публично поддерживается руководителем организации

Таблица 1. Модель зрелости Программы повышения осведомлённости

SOC: ТИПОВЫЕ ТРУДНОСТИ И СОВЕТЫ ПО ЗАПУСКУ



Дмитрий КИМ
эксперт Positive
Technologies

В зависимости от своих задач и уровня зрелости инфраструктуры, компании выбирают путь построения собственного центра оперативного реагирования (т.н. in-house SOC), либо — использования услуг сторонних центров (outsourced SOC). Сегодня мы расскажем о типовых проблемах возникающих в каждом из этих случаев и дадим несколько советов по построению собственного Security Operation Center (SOC).

SOC И РЕАГИРОВАНИЕ НА СОВРЕМЕННЫЕ УГРОЗЫ

На взлом 90% компаний в среднем нужно от одного до пяти дней, и только в одном случае из десяти факт взлома атакуемая организация выявляет самостоятельно. Все чаще организации становятся жертвами целевых атак (APT)¹. И особенно явно этот тренд виден в финансовой сфере: по данным ФинЦЕРТ, за 2018 год было зафиксировано 687 атак на организации кредитно-финансовой отрасли, из них 177 были целевыми. По данным Positive Technologies, в 58% банков злоумышленник может получить доступ к тем или иным критически важным системам — к управлению банкоматами, системам межбанковских переводов, карточному процессингу или платежным шлюзам. Security operation center во многом являются ответом на современные угрозы (включая APT-атаки). В первую очередь они помогают постоянно и тщательно наблюдать за активами в инфраструктуре, а во вторую — становятся центром управления уязвимостями, выявления и расследования инцидентов ИБ, и реагирования на них, поиска новых угроз.

Команда центра оперативного реагирования — один из ключевых элементов экосистемы, благодаря которому удастся выстроить устойчивые внутренние процессы и обеспечить эффективную работу средств защиты. Команда, глубоко понимающая современный ландшафт киберугроз, способна адаптировать систему ИБ к новым угрозам и гарантировать непрерывность процессов обеспечения кибербезопасности.

ГЛАВНЫЕ ОШИБКИ

Построение SOC — сложный процесс, во время которого многие делают типовые ошибки, не

позволяющие добиться высокой эффективности, например:

- ♦ **Чрезмерная надежда на аутсорсинг**, возглавляющая этот рейтинг, чревата иногда тем, что экспертиза внутренних команд перестает расти, а обеспечение кибербезопасности превращается в слепое следование рекомендациям сервис-провайдера. История начинается красиво, но хэппи-энда не будет: утрачивается контроль над развитием ИБ, команда теряет способность оперативно влиять на ситуацию (из-за снижения уровня компетенций), а компания становится заложником тарифов и уровня SLA сервис-провайдера;

- ♦ **Неправильное планирование**, или попытка купить и внедрить все необходимые средства защиты разом — решение героическое, но, как показывает практика, — тоже часто обреченное на неудачу. Построение SOC — процесс небystрый, требующий тщательного планирования и удачных случаев построения центра оперативного реагирования с нуля и за один шаг история пока не знает;

- ♦ **Слепое следование стандартам** и бездумное применение международных практик. В этом случае все начинается с правильной мысли о том, что не нужно изобретать велосипед, а заканчивается тем, что в процессы ИБ внедряются международные стандарты, принципы agile, копируются все подряд практики и пр. Без адаптации к специфике конкретной организации, это оказывается скорее вредным, чем полезным.

ПОШАГОВЫЙ ЧЕК-ЛИСТ

Это были основные «грабли», по которым часто ходят строители SOC. Есть и другой подход, более неспешный, но, вместе с тем, системный и поэтапный. Этапность в данном случае зависит от уровня зрелости ИБ в организации и квалификации экспертов. Зрелость ИБ и от квалификации персонала в этом случае будут наращиваться от этапа к этапу с одновременным «причесыванием» инфраструктуры, построением процессов, написанием регламентов, набором новых сотрудников и их обучением, внедрением средств защиты. В итоге, на каждом этапе применяется то, что действительно необходимо в конкретный момент и не делаются внедрения «на вырост». Такой подход поможет

¹ Атака типа advanced persistent threat (APT-атака) — это хорошо организованная, тщательно спланированная кибератака, которая направлена на конкретную компанию или целую отрасль. За APT-атакой, как правило, стоят преступные группировки, имеющие значительные финансовые ресурсы и технические возможности.

оптимизировать инвестиции и трудозатраты на создание SOC, выработать стратегию развития ИБ на несколько лет, с понятными задачами, результатами и показателями эффективности.

Шаг первый: аудит периметра. Периметр компании — первый барьер защиты на пути атакующего. От защищенности периметра напрямую зависит количество векторов атак на инфраструктуру и скорость их реализации. Потому в первую очередь важно понять, как выглядит периметр с точки зрения киберпреступника и какие белые пятна необходимо устранить. Необходимы инвентаризация и анализ типовых уязвимостей внешних информационных систем. Эти задачи можно выполнить самостоятельно, а можно воспользоваться внешней услугой по усиленному контролю сетевого периметра (advanced border control).

Шаг второй: защита периметра. Первичный аудит позволяет оценить текущий уровень защищенности периметра, имея эту оценку, можно принимать обоснованное решение о том, каким образом защищать периметр, какие меры предпринимать. И здесь необходимо уделить внимание самым простым, но наиболее эффективным методам проникновения в инфраструктуру, к которым относится, например, фишинг (к ним по статистике уязвимы до 75 % банков). Базу для закрытия основных векторов проникновения в инфраструктуру организации могут сформировать, к примеру, межсетевые экраны уровня приложений, позволяющие обнаружить атаки на публичные сервисы компании (PT Application Firewall), решения класса network traffic analysis, решающие задачи по выявлению атак на периметре (PT Network Attack Discovery), решения для выявления вредоносного ПО (PT MultiScanner). Таким образом основные векторы проникновения в организацию извне — веб, электронная почта и пользовательский трафик — будут закрыты.

Шаг третий: защита внутренней инфраструктуры. Когда периметр защищен, можно переходить к защите внутренней инфраструктуры. Этот переход связан с решением ряда задач:

- ◆ с инвентаризацией и выявлением уязвимостей внутренних информационных систем;
- ◆ выявлением вредоносного ПО внутри инфраструктуры;
- ◆ выявлением следов компрометации в трафике;
- ◆ анализом событий безопасности и выявлением инцидентов.

Основным инструментом здесь может выступать сканер уязвимостей (например, MaxPatrol 8),

на базе которого строится цикл управления уязвимостями. Также логичным на этом этапе является внедрение системы выявления инцидентов ИБ (MaxPatrol SIEM) и средств мониторинга трафика: это ключевые элементы комплексной системы выявления угроз.

Шаг четвертый: продвинутые методы защиты. Всесторонняя защита периметра и внутренней инфраструктуры готова. Что же дальше? Для борьбы с продвинутыми угрозами требуются новые способы оценки защищенности. Таким образом достигается непрерывное и устойчивое развитие системы информационной безопасности. Эти способы могут показаться знакомыми: регулярная оценка защищенности (тесты на проникновение, аудит исходного кода, ретроспективный анализ трафика и пр.), расследование инцидентов, Threat Intelligence и Threat Hunting. Продвинутой программой может быть бесконечно широкой, но она должна давать ответ на вопросы:

- ◆ Снизятся ли в итоге риски взлома?
- ◆ Позволит ли это выстроить процессный подход к выявлению и расследованию атак?
- ◆ Соответствует ли инфраструктура внутренним политикам ИБ?
- ◆ Если все три ответа положительные, то путь выбран верно.

Шаг пятый: обучение специалистов SOC. Без людей нет процессов и нет необходимости в средствах защиты. Экспертов на рынке катастрофически мало, а их обучение длится зачастую довольно долго, рост числа инцидентов диктует свои правила: экспертов важно растить внутри компаний, ведь их ценность удваивается, если прикладные знания подкреплены пониманием инфраструктуры компании. Повышать уровень экспертизы важно для специалистов всех линий SOC: первую линию стоит «прокачивать» в области непрерывного мониторинга, первую и вторую — в расследовании и реагировании на инциденты. Третью линию также желательно иметь в штате, но при необходимости для расследования сложных киберинцидентов можно привлекать внешнюю экспертизу. Это весьма успешная практика, которая позволит снизить стоимость владения SOC.

* * *

Построение SOC — процесс кропотливый, требующий серьезного планирования и ресурсов. Уровень зрелости ИБ в организации будет расти от этапа к этапу, а итоговый результат будет, безусловно, стоить всех затраченных усилий, финансов и времени.

SOC: ВНЕШНИЙ ИЛИ ВНУТРЕННИЙ? ВЫБОР НЕИЗБЕЖЕН

ОШИБКА ОБХОДИТСЯ ДОРОГО: «ЗАРЫТЫЕ В ЗЕМЛЮ» ДЕНЬГИ И НЕОБХОДИМОСТЬ ПОДДЕРЖИВАТЬ РАБОТУ СТРУКТУРЫ, НЕ ПРИНОСЯЩЕЙ ОТДАЧИ



Иван МЕЛЕХИН
директор по развитию
компаний
«Информзащита»,
руководитель IZ:SOC

Иван Мелехин рассказывает BIS Journal о плюсах и минусах внешних и внутренних центров управления безопасности (SOC), о том, что следует учитывать при заключении SLA между компаниями-заказчиками и компаниями-аутсорсерами, и о том, каким должен быть приближённый к идеалу SOC.

— Иван, поделитесь своим экспертным мнением: какие сервисы должны предоставляться современными SOC, чтобы полностью отвечать ожиданиям заказчиков?

— Не бывает двух одинаковых заказчиков, у каждого есть свои проблемы, запросы и предпочтения. Также на стороне заказчиков сильно отличаются уровни зрелости функций ИБ: запросы по конфигурации сервисов у стартапа и крупного банка зачастую несопоставимы. Поэтому, если мы говорим о внешнем центре управления безопасности (SOC), то он должен быть достаточно гибким, для того чтобы наиболее полно соответствовать потребностям клиентов. Если же мы говорим о базовом наборе сервисов, из которого можно выбрать конфигурацию под потребности практически любого заказчика, то можно назвать следующие:

- ◆ Сбор и хранение логов и событий информационной безопасности.
- ◆ Автоматизированный анализ потока событий с использованием адаптируемых сценариев мониторинга и обогащением данных от различных внешних источников.
- ◆ Ручная обработка инцидентов командой аналитиков с учётом особенностей вашей инфраструктуры, информационных сервисов и нормативно-организационной документации.
- ◆ Оповещение об инцидентах по выбранным каналам связи (телефон, электронная почта, мессенджеры) и представление рекомендаций по реагированию.
- ◆ Автоматизированный регулярный анализ защищённости и рекомендации по устранению уязвимостей.
- ◆ Регулярная аналитическая отчётность.

- ◆ Управление инцидентами и заявками.

В качестве дополнительных сервисов, которые пользуются популярностью, можно назвать следующие:

- ◆ Анализ защищённости (пентесты, red team).
- ◆ Расследование инцидентов.
- ◆ Управление СЗИ и реагирование на инциденты.
- ◆ Киберразведка и киберучения.
- ◆ Взаимодействие с регуляторами.

— Внутренний и внешний SOC? Иногда банки, приступающие к решению этой задачи, долго размышляют, какому бы из этих вариантов отдать предпочтение. В чём, по вашему мнению, плюсы и минусы каждой из этих опций?

— К основным плюсам внешнего SOC можно отнести скорость подключения к сервису, существенную экономию бюджета (2–3 раза на промежутке в три года) и высокую квалификацию персонала, ежедневно сталкивающегося с большим количеством разнообразных инцидентов у клиентов. Также внешний SOC обычно имеет большой набор глубоко проработанных сценариев мониторинга и реагирования. К минусам внешнего SOC можно отнести сложности перехода между поставщиками услуг, отсутствие принадлежащего организации контента (сценариев мониторинга и реагирования) и слабое формирование профильных компетенций внутри организации. Фактически, если поставщик внешнего SOC покинет организацию, то она вернется к тому же состоянию, что и до подключения SOC, капитализации вложений не произойдёт. Также зачастую персонал внешнего SOC при большом количестве подключённых организаций может формально относиться к потребностям заказчика.

К основным плюсам внутреннего SOC можно отнести то, что на вложенные деньги организация не только получает сиюминутный сервис, но и фактически инвестирует их в развитие своей инфраструктуры и компетенций. Правда, к сожалению, посчитать возврат от этих инвестиций зачастую очень сложно. Также органи-

зация в случае выбора этого варианта получает сильно адаптированный под нужды организации сервис, тесно интегрированный со смежными бизнес- и вспомогательными функциями. К основным минусам внутреннего SOC можно отнести крайне высокие затраты на внедрение инфраструктуры и поддержание функционирования: например, затраты на содержание всего лишь двух аналитиков могут превысить 6 млн рублей в год, с учётом всех налогов и косвенных затрат, а в случае круглосуточного режима работы нужно не менее семи квалифицированных аналитиков. Также необходимо отметить отсутствие на рынке достаточно количества квалифицированного персонала и взвинченные высокой конкуренцией зарплатные ожидания, не всегда соответствующие уровню компетенций соискателей. Назову и ещё один минус: организация, строящая свой SOC, сталкивается с большими сложностями и трудозатратами по разработке контента (сценариев реагирования и мониторинга). К сожалению, внешний купленный контент (или поставляемый поставщиками SIEM из «коробки») зачастую практически бесполезен.

— **Итак, и в том, и в другом варианте есть серьёзные плюсы и минусы. По вашему опыту, к какому выбору чаще склоняются компании-заказчики, и в силу каких причин?**

— Как специалист, общающийся с заказчиками со стороны внешнего коммерческого SOC, я вижу несколько однобокую картину этого рынка. К нам приходят люди, которые осознанно не хотят или не могут построить свой SOC, или те, кто попробовал его построить, но безуспешно и с большими издержками. К сожалению, часто приходится видеть ситуацию, когда заказчику продали продвинутую техническую инфраструктуру SOC — начиная от SIEM и заканчивая IRP, но про процессы или забыли, или не смогли их внедрить. В результате заказчик имеет «зарытые в землю» капитальные вложения и плюс к этому он сталкивается с необходимостью поддерживать работу SOC, который не приносит организации какой-либо значимой пользы и ощутимой отдачи.

— **Ваши советы в связи с этим?**

— Прежде всего, мы рекомендуем подходить к этому вопросу итеративно — начать с полностью внешнего SOC для того, чтобы понять, какие сервисы и какой контент нужен заказчику и в какой конфигурации. Подключение внешнего SOC проходит быстро (в течение одного-двух месяцев) и является вполне приемлемым с бюджетной точки зрения. По мере осознания своих потребностей, можно переносить к себе или в

зону своей ответственности части инфраструктуры и процессов SOC, например, внедрив у себя IRP или SOAR-систему, тесно интегрированную со своей инфраструктурой. Или наоборот, можно передавать внешним подрядчикам такие сервисы как реагирование на инциденты и управление СЗИ.

— **Как следует правильно прописать разделение зон ответственности между компанией-заказчиком и компанией-аутсорсером в том случае, если мониторинг ИБ передаётся на аутсорсинг? Что компании-заказчику необходимо предусмотреть в данном случае?**

— Во-первых, хотелось бы, чтобы компании, выступающие в роли заказчиков, не воспринимали внешний аутсорсинг мониторинга ИБ как некоего рода серебряную пулю, которая позволит им защититься от любой нечисти. Иногда приходится видеть, как в SLA, например, пытаются включить требования по обнаружению в течение пяти минут любых атак с уязвимостями нулевого дня. Это принципиально невозможно. Если во внешний SOC не передаются события от источников, например, фиксирующих определённую активность на рабочих станциях, то выявить некоторые инциденты можно только достаточно поздно и по косвенным признакам. Поэтому определение зоны ответственности — это итеративный договорной процесс, результат общения между поставщиком услуги и заказчиком.

Для ряда типовых сценариев мониторинга, безусловно, есть понимание матрицы ответственности. Но если разрабатываются сильно кастомизированные сценарии, то процесс определения ответственности может быть довольно долгим и сложным. Также необходимо помнить, что заказчик никогда не передаёт на аутсорсинг одному поставщику все функции, необходимые для реагирования и выявления инцидентов: нужно учитывать и интегрировать в матрицу ответственности между поставщиком и заказчиком ответственность ИТ-подразделений заказчика в части выполнения рекомендаций и требований, ответственность руководства и финансов в части поддержки и финансирования корректирующих мер.

Также крайне сложно определить финансовую ответственность поставщика услуг SOC за те или иные инциденты: с одной стороны, из-за сложности определения реального ущерба, а с другой стороны, из-за того, что рекомендации аутсорсера никогда не соблюдаются в полном объёме, как из-за финансовых ограничений, так и из-за баланса требований бизнеса и безопасности. Таким образом, устанавливать от-

ветственность поставщика сервиса SOC необходимо в тех границах, в которых у этого поставщика есть ресурсы для принятия на себя этой ответственности. Это выражается в том, что в SLA практически всегда включаются исключительно временные метрики по реализации тех или иных процессов на стороне SOC, такие как время принятия в работу или время первичного реагирования. Также могут включаться метрики по доступности сервисов.

— **Насколько эффективным инструментом для разрешения дальнейших споров (например, о том, с какой скоростью следует реагировать на инциденты) является соглашение SLA? Особенно этот вопрос интересен в российских условиях.**

— SLA является приложением к контракту, соответственно является достаточным инструментом для решения любых споров законными методами, включая судебные разбирательства. Другое дело, что зачастую реальных механизмов контроля SLA у заказчика нет, и он ориентируется на данные, представляемые исполнителем. Объективности ради добавлю, что построение системы контроля аутсорсера за целым рядом внутренних процессов на стороне заказчика представляется крайне затруднительной задачей. Её решение возможно только в случае, если вся техническая инфраструктура SOC находится под управлением заказчика.

— **Как, по вашему мнению, следует решать вопрос о допуске аутсорсера к критически важным для компании-заказчика данным и системам?**

— Аутсорсер мониторинга информационной безопасности в штатном режиме работы обычно не имеет доступа ни к критичным данным, ни к критичным системам. Он имеет доступ к логам и событиями информационной безопасности, которые, безусловно, могут содержать некую критичную информацию. Доступ к данным и системам может потребоваться либо в случае выполнения расследований, либо в случае, если реагирование и управление СЗИ также передаётся внешней стороне. Но при любом раскладе правильно спроектированная система защиты должна в модели нарушителей учитывать и своих и внешних администраторов, и аутсорсеров, и поставщиков услуг и сервисов. И в любом случае между поставщиком сервисов и заказчиком заключается соглашение о конфиденциальности.

— **Как избежать зависимости внутренней службы ИБ от аутсорсера?**

— Если мы говорим о внешнем SOCе, то первым шагом, который можно сделать для

облегчения процесса переключения между различными поставщиками и снижения зависимости от аутсорсера может являться реализация внутреннего хранилища логов. В этом случае, зеркалируя события, поступающие в такое хранилище можно достаточно безболезненно менять поставщиков услуг мониторинга. Необходимо отметить, что в этом случае организация должна иметь достаточно глубоко проработанную политику мониторинга, реализованную на ИТ инфраструктуре. Также очень важно иметь возможность выгрузки из систем провайдера всей информации касательно имевших место инцидентов, либо впоследствии реализовать IRP платформу внутри организации.

— **Какие решения и услуги в сфере SOC предоставляет ваша компания? В чём их конкурентное преимущество?**

— Мы предоставляем весь набор сервисов, перечисленных в первом вопросе. Также, так как наш SOC работает в рамках крупнейшего интегратора на рынке ИБ, мы можем предоставить большое количество смежных сервисов, начиная от аудитов заканчивая сервисным сопровождением систем защиты. В рамках наших сервисов SOC мы основной упор делаем на качество контента — сценариев реагирования и мониторинга, предоставляемых Заказчику. Мы имеем большой набор типовых сценариев, которые мы можем достаточно быстро адаптировать под нужды Заказчика, а также можем разработать кастомизированные сценарии, причём для самых различных случаев применения — от мониторинга облачной инфраструктуры до выявления мошеннических действий. Также мы делаем упор на удобство взаимодействия Заказчика с нами, начиная от использования различных каналов для общения, включая мессенджеры, заканчивая разработкой удобного клиентского портала.

— **Как вы видите процесс дальнейшего развития SOC?**

— Если не рассматривать коммерческие вопросы, то одними из основных направлений развития SOCа я вижу разработку качественного контента, адаптированного под специфические нужды заказчиков из разных отраслей, и разную инфраструктуру (например, активно используемые технологии контейнеризации), реализацию мультивендорной технологической платформы SIEM, активную разработку своих кастомных решений для автоматизации деятельности SOC. Также, хотелось бы видеть больше активности в части взаимодействия различных SOC друг с другом.



НИЧЕГО ЛИШНЕГО ТОЛЬКО SOC

Security Operation Center

izsoc.ru



Анатолий АКСАКОВ
председатель
Комитета Госдумы
по финансовому рынку

ВСЕ ГРАНИ ЦИФРОВИЗАЦИИ

РАЗВИТИЕ ЗАКОНОДАТЕЛЬНОЙ БАЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВОЙ СФЕРЫ В 2019 ГОДУ

Среди законодательных инициатив Банка России, поддержанных в 2019 году Государственной Думой РФ, есть имеющие прямое отношение к цифровизации и информационной безопасности финансовой сферы. В июне во втором чтении принят законопроект № 261689-7 «О внесении изменения в статью 46-1 Федерального закона „О Центральном банке Российской Федерации (Банке России)“».

S.W.I.F.T. ПО-РОССИЙСКИ

Банку России предоставляются полномочия передавать финансовые сообщения Федеральному казначейству и его территориальным органам. Расширен перечень участников СПФС — российской системы передачи финансовых сообщений, аналога международной системы S.W.I.F.T. Урегулирован ряд вопросов, связанных с платёжными сервисами.

Установлены требования к различным участникам платёжных рынков. Подключиться к СПФС теперь могут практически любые юридические лица, и российские, и иностранные, только по разным правилам. Таким образом, наш внутренний рынок, права бизнеса и граждан теперь защищены.

Международным платёжным системам VISA и MasterCard предстоит привести свою деятельность в соответствие с этими новыми требованиями, никто с российского рынка уходить не собирается. Напротив, сотрудничество будет расширяться, одна из предстоящих программ — программа повышения финансовой грамотности населения.

РЕГУЛИРОВАНИЕ КРИПТОВАЛЮТ

Среди ближайших перспектив работы в финансовой сфере — законодательное регулирование цифровых финансовых активов, криптовалют, доработка законопроекта № 419059-7 «О цифровых финансовых активах и о внесении изменений в отдельные законодательные акты Российской Федерации (о цифровых финансовых активах)».

Вопрос о законодательном регулировании криптовалют был поднят работавшими в России членами комиссии ФАТФ (Financial Action Task Force on Money Laundering — международной группы разработки финансовых мер борьбы с отмыванием денег). Согласно поручению Председателя Пра-

вительства РФ Д.А. Медведева, эта работа должна быть завершена до 1 ноября.

Есть разные, часто противоположные точки зрения на легализацию криптовалюты и операции с ней на территории Российской Федерации. Одни считают, что делать этого вообще нельзя. Другие, — что можно, но гибко регулируя, а регулятором должен выступать Банк России. Сторонники легализации ссылаются на то, что российские организации и граждане уже используют криптовалюты.

Базовый законопроект уже готов, доработка должна занять максимум две недели. Активная дискуссия, в какую сторону его дорабатывать, пока продолжается. ФАТФ будет устроена любым вариантом законодательного урегулирования.

ПЕРСПЕКТИВЫ MARKET PLACE

К сожалению, пока задерживается работа над законопроектом № 617867-7 «О совершении сделок с использованием электронной платформы» — правовой основой для Market Place — супермаркета финансовых продуктов, позволяющем гражданам инвестировать посредством электронных платформ.

В первом чтении он был принят в июле, в настоящее время идёт обсуждение поправок, расширяющих перечень операций и сделок на новой платформе. В частности, представители электронных бирж не видят необходимости вести деятельность с помощью Market Place.

Есть и другая точка зрения: что преимущества того или иного механизма работы должны быть выявлены в ходе конкуренции. В частности, в вопросе о регистраторе финансовых транзакций нужно законодательно определить требования к нему, а уж сколько таких будет, пусть решает рынок. Второе чтение этого законопроекта должно состояться в ноябре.

ЦИФРОВОЙ ПРОФИЛЬ ГРАЖДАН

Два законопроекта, подготовленные и внесённые членами Совета Федерации РФ, касаются цифрового профиля граждан и работы удостоверяющих центров.

На первый, № 760029-7 «О внесении изменений в статью 10-1 Федерального закона «Об информации, информационных технологиях и о защите информации» (в части

установления обязанностей организатора сервиса электронной почты)», правовое управление Государственной Думы РФ сделало заключение, что возможны значительные затраты из государственного бюджета. Этот законопроект пока не рассматривается.

На второй, № 747528–7 «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с совершенствованием регулирования в сфере электронной подписи», уже получен положительный отзыв Правительства России. Предполагается, что частные удостоверяющие центры будут работать только с гражданами, для бизнеса эти функции будет выполнять Федеральная налоговая служба России, а для банков — Банк России.

В отношении этого законопроекта есть серьёзная критика со стороны участников рынка. Через другую группу членов Совета Федерации РФ предлагается альтернативный законопроект, согласно которому удостоверяющие центры должны работать в конкурентной среде. Предлагается всем им предоставить право выдавать электронные подписи бизнесу, руководителям юридических лиц. Чтобы завершить дискуссии и определить, какую версию законопроекта выбрать, рассмотрение было перенесено с июля на осень.

ЕДИНЫЙ ЭЛЕКТРОННЫЙ АРХИВ

Далее предстоит работа над законопроектом, касающимся электронного документооборота, № 657361–7 «О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» и иные законодательные акты Российской Федерации (в части использования и хранения электронных документов)». В ходе согласования в разных ведомствах было получено много критических замечаний.

Со стороны силовых ведомств высказывались опасения, что массовый переход на электронный документооборот чреват рисками потери информации, критически важной и для них, и для судов, и для самих граждан.

После обсуждения всех полученных замечаний было принято решение сузить сферу законопроекта до финансового рынка. Завершается подготовка второй версии этого законопроекта, предлагающая на первом этапе его «отраслевизацию». Финансовый рынок несёт значительные затраты на бумажный документооборот и готов работать по новым правилам.

Подготовлена и обсуждается концепция расширения действия этого законопроекта в дальнейшем и на другие отрасли. Предусматриваются технологии подготовки и сертификации, определения ответственности специалистов по работе с электронной документацией, переходу с бумажных носителей на цифровые.

Другой аспект — формирование специального института, определяемого государством, для хранения единого электронного архива и заверения выдаваемых документов. Это может быть Росархив — Федеральное архивное агентство, предлагают и нотариат. Подготовительная работа уже ведётся.

К декабрю законопроект № 657361–7 будет доработан с учётом высказанных замечаний и далее, в 2020 году, будет приниматься как федеральный закон.

ДОСУДЕБНАЯ БЛОКИРОВКА ФРОДА

В октябре ожидается окончательное принятие законопроекта о досудебной блокировке интернет-ресурсов по решению Банка России — № 605945–7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и защите информации» и Гражданский процессуальный кодекс Российской Федерации» (в части уточнения перечня информации, распространение которой в Российской Федерации запрещено)».

Председателю Банка России предоставляется исключительное право принимать решения о блокировке в отношении сайтов «финансовых пирамид» и мошеннических «двойников» реальных банков. По действующим процедурам за 2018 год уже было заблокировано около 2 000 подобных ресурсов. Но на обращение Банка России в прокуратуру, а затем на судебные процедуры, уходило время, когда злоумышленники продолжали действовать.

«ОДНО ОКНО» ДЛЯ КРЕДИТОРОВ

В высокой степени готовности находится законопроект № 747030–7 «О внесении изменений в статью 7 Федерального закона „О кредитных историях“». В нём предусматривается введение института квалифицированных бюро кредитных историй (БКИ), формулируются требования к ним и их полномочия. Такие организации будут наделены правом получать информацию от всех бюро, ведущих кредитные истории. Таким образом, станет возможно собирать полную, сводную информацию о заёмщике и его задолженностях.

Банкам обойдётся дешевле запрашивать такие данные не в 13 ныне действующих бюро кредитных историй, а в одном, квалифицированном. Механизм будет выглядеть так. Банк обращается в квалифицированное бюро, которое, с согласия заёмщика, собирает и предоставляет агрегированный актуальный показатель его долговой нагрузки. На основании методики Банка России кредитная организация определяет ежемесячный платёж, который заёмщик способен осуществлять. Эта сумма соотносится с подтверждённым доходом заёмщика, чтобы вычислить предельную долговую нагрузку.

* * *

Прорабатывается механизм проверки кредиторами, с согласия заёмщика, справки о его доходах, обращением в Пенсионный фонд России и ФНС России. Если банки не хотят сами рассчитывать показатель предельной долговой нагрузки заёмщика, они могут, опять-таки с его согласия, за отдельную плату перепоручить бюро кредитных историй эту процедуру. Такая цепочка теоретически возможна и может быть реализована в будущем.

**Андрей ВЫБОРНОВ**

заместитель директора — начальник
Управления методологии и стандартизации
информационной безопасности
и киберустойчивости Департамента
информационной безопасности Банка России

ГОТОВНОСТЬ НОМЕР ОДИН

ГОТОВА СТАРТОВАТЬ КОНТРОЛЬНО-НАДЗОРНАЯ
ДЕЯТЕЛЬНОСТЬ ЗА ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОСТИ
БИОМЕТРИЧЕСКИХ ДАННЫХ КЛИЕНТОВ БАНКОВ

Полномочия Банка России как государственного регулятора информационной безопасности финансовой сферы в 2019 году были значительно расширены. Отраслевой регулятор, помимо прочих новых полномочий, готовится осуществлять надзор и контроль в финансовой сфере за сбором, обработкой, верификацией и дальнейшим использованием данных для Единой биометрической системы.

ОТТАЛКИВАЯСЬ ОТ БИЗНЕС-ПРОЦЕССОВ

Подведомственными для Банка России как мегарегулятора всей финансовой сферы оказались и около 20 тыс. некредитных финансовых организаций. Расширение сферы регулирования и расширение полномочий требует ещё более систематизированного подхода, в том числе в выстраивании процедур регулирования и надзора.

Надзорно-контрольная деятельность должна быть адаптирована к профилю, специализации «поднадзорных» юридических лиц и информационным технологиям, которые они используют. Очевидно, что нормативные акты, которые издаются для кредитных организаций, в меньшей степени применимы к технологии обработки информации у финансовых компаний, работающих на рынке ценных бумаг. И ещё менее применимы к организациям, действующим на рынке коллективных инвестиций.

Банку России важно разобраться в технологиях обработки информации, сейчас эта работа активно ведётся в отношении некредитных финансовых организаций разного вида. Регулятор разбирается, из каких конкретных операций состоит процесс обработки защищённой информа-

ции подведомственными организациями в соответствии с профилями их деятельности. Происходит определение рисков реализации компьютерных атак на каждом из технологических участков. В этой работе Банк России активно использует опыт международных площадок, где решают схожие задачи.

ТРИ УРОВНЯ РЕГУЛИРОВАНИЯ

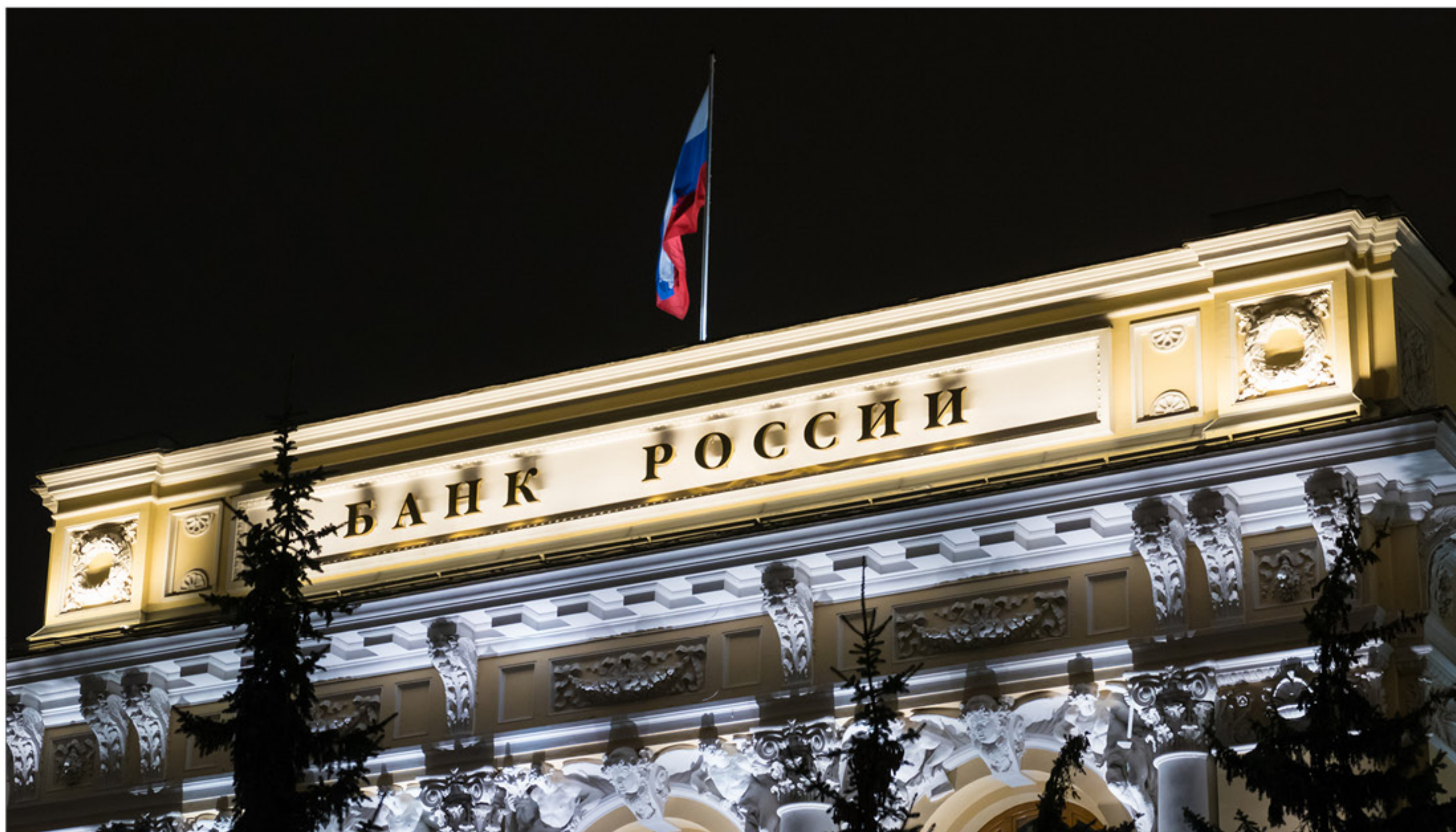
Государственное регулирование должно исходить из понимания бизнес-процессов, особенностей обработки информации и концентрироваться на трёх уровнях.

Первый уровень — выбор технологических мер защиты информации при проведении операций. То есть всё, что связано с обеспечением целостности и достоверности информации.

Второй уровень — требования к безопасности программного обеспечения, такие нормативные документы разрабатываются и применяются.

Третий уровень — требования к инфраструктуре. Существует широко известный ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия». В настоящее время разрабатывается новый государственный стандарт, инфраструктурные требования к защите информации.

Банк России обладает правовыми основаниями и полномочиями устанавливать требования к защите информации в финансовой сфере. Начиная с уровня федерального законодательства, где Банк России готовит и вносит законодательные инициативы. В том числе взаимодействуя с други-



ми ведомствами, такими как, например, Минфин России и Минкомсвязи РФ, поскольку их субъекты регулирования поднадзорны Банку России.

Кроме того, Банк России разрабатывает и публикует отраслевые нормативно-правовые документы рекомендательного и обязательного характера. Предварительно прорабатываются технологии, используемые для проведения операций в банковской сфере и на финансовых рынках. Результатом выступают положения и концепты, которые переходят в отдел нормативного регулирования.

Требования нормативных актов формируются на основе действующих технологий, которые сегодня уже применяются как в банковских организациях, так и в организациях не-кредитной финансовой сферы. Для частных случаев предусмотрены нормативные документы более низкого уровня: информационные письма, методические рекомендации, которые более подробно разъясняют требования для тех или иных технологий и правовые аспекты.

ЗАЩИЩЁННАЯ БИОМЕТРИЯ

Так, законодательной базой обеспечения информационной безопасности Единой биометрической системы служит Федеральный закон от 31 декабря 2017 года № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» — о создании механизма удалённой биометрической идентификации физлиц. Модель угроз и требования к информационной безопасности в единой биометрической системе в процессе сбора биометрических данных и дистанционной идентификации пользователей были сформулированы Банком России в Методических рекомендациях № 4-МР.

О ходе выполнения методических рекомендаций регулятора на начало сентября 2019 года можно было судить по данным 38 банков, обслуживающих физических лиц. Встречи с ними в ходе этой работы проводятся регулярно. Семь банков разрабатывают и внедряют самостоятельные решения, 31 банк пользуется продуктами, купленными у поставщиков. На рынке будут представлены четыре типовых решения — облачные, «коробочные» и адаптированные под заказчика. Большинство банков стремятся использовать типовые решения, что поддерживается, и разработка их должна быть ускорена.

Ожидается, что почти все, 37 банков, завершат внедрение в текущем 2019 году и один — в следующем. Единственным фактором неопределённости, способным повлиять на эти сроки, является время, которое потребуется на согласование ФСБ России системных проектов поставщиков решений. С уполномоченным органом должны быть согласованы вначале системный проект, а потом и решение на его основе.

Банки получили информационное письмо Банка России о неприменении надзорных мероприятий в отношении обеспечения информационной безопасности биометрических данных до конца года. Старт их проведения запланирован на начало следующего, 2020 года. Интенсивность и глубина этой деятельности будут определяться тем, насколько результативно банки внедрят наличествующие решения.

ИБ-РИСКИ: СЕГОДНЯ И ЗАВТРА

РАЗГОВОР О КИБЕРБЕЗОПАСНОСТИ НА МЕЖДУНАРОДНОМ
ФОРУМЕ «БАНКИ РОССИИ — XXI ВЕК»



Анна ВОРОБЬЕВА
обозреватель
BIS Journal

Тема кибербезопасности не обошла стороной Международный банковский форум «Банки России — XXI век». Мероприятие, организуемое Ассоциацией банков России, уже который год служит площадкой для обсуждения перспектив развития российской банковской системы и экономики страны в целом.

На круглом столе «Киберугрозы и обеспечение информационной безопасности: проблемы и решения» обсуждались различные аспекты ИБ: техника, нормативные акты, кадры и пр.

Своё мнения высказали Артём Сычёв, первый заместитель директора Департамента информационной безопасности Банка России, Матвей Геринг, директор по Центральной и Восточной Европе SWIFT, Артем Гутник, заместитель начальника управления безопасности АО «НСПК», Василий Карташов, руководитель направления TI BI.ZONE, Сергей Пазизин, заместитель начальника Управления по обеспечению информационной безопасности Департамента по обеспечению безопасности Банка ВТБ (ПАО), Андрей Лищицын, директор Центра РСПП по финансовой политике и финансовым рынкам, Алексей Волков, управляющий директор-начальник управления методологии кибербезопасности, ПАО Сбербанк.

Модерировал дискуссию Алексей Лукацкий, бизнес-консультант по безопасности Cisco Systems.

СТРАТЕГИЯ ИБ ОТ БАНКА РОССИИ. ФОРМИРОВАНИЕ РИСК-ПРОФИЛЯ

В качестве затравки Артём Сычёв сообщил, что Совет Директоров Центрального Банка одобрил довольно серьёзный концептуальный документ «Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов», определяющий ближайшие перспективы. По этому документу под регулаторику ЦБ подпадают не только кредитные и некредитные организации, но и площадки маркетплейсов, операторы и иные участники национальной платёжной системы.

Документ определяет не только курс развития и тренды, но и целевые показатели. Прежде всего, речь идёт о двух показателях:

- ♦ **уровень доверия населения к ИБ финансовых услуг и устойчивости функционирования сервисов.** Определяется на основании социологических опросов, взаимодействия с банками, анализа удовлетворённости сервисами, которые есть у финансовых организаций;

- ♦ **доля объёма несанкционированных операций от общего объёма операций.** Исчисляются на основании отчётности и реальных цифр, поступающих в форме отчётов и в ходе обмена информацией по противодействию мошенничеству (Рис. 1).

Главный акцент при реализации «Основных направлений» регулятор планирует сделать на формировании риск-профиля. Риск-профиль — это обобщённый показатель, вычисляемая вероятность, формирующаяся на основании нескольких групп показателей:

- 1. Уровень несанкционированных операций и показатели операционной надёжности.** Формируется на основании отчётности и информации, получаемой ЦБ в ходе информационного обмена с ФинЦЕРТ (Рис. 2).

К примеру, если взять банки топ-10 и небольшой региональный банк, то одна и та же сумма хищений будет иметь у них совершенно разные показатели. Поэтому куда важнее, как руководство кредитной организации реагирует на изменение тренда. Если видны поло-

Главный акцент при реализации «Основных направлений» регулятор планирует сделать на формировании риск-профиля. Риск-профиль — это обобщённый показатель, вычисляемая вероятность, формирующаяся на основании нескольких групп показателей



Цель Банка России в области обеспечения информационной безопасности организаций кредитно-финансовой сферы

Наименование целевого показателя	Целевое значение на 2017 год	Фактическое значение за 2017 год	Целевое значение на 2018 год	Фактическое значение за 2018 год	Целевое значение на 2020 год
Уровень доверия*	30%	40%	60%	70%	80%
Доля объема несанкционированных операций в общем объеме операций, совершенных с использованием платежных карт	0,005%	0,0016%	0,005%	0,0018%	0,005%



Показатель доли объема несанкционированных операций в общем объеме операций, совершенных с использованием платежных карт, не должен превышать 0,005%

* уровень доверия клиентов и контрагентов финансовых организаций к безопасности реализуемых электронных платежных сервисов

Рисунок 1. Цель БР в области информационной безопасности организаций кредитно-финансовой сферы



Рисунок 2.

жительные изменения — растёт объём операций, сокращается количество хищений, — это свидетельствует, что руководство банка заинтересовано в правильной оценке управления рисками.

2. Показатель оценки соответствия нормативным требованиям Банка России. Имеются в виду три группы требований: безопасность технологий, безопасность ПО, безопасность информационной инфраструктуры. Причём последние связаны с показателем операционной надёжности. Тут главной задачей ЦБ будет не просто заполнить акт проверки финансовой организации, а научиться распознавать вероятность возникновения проблемы у банка, исходя из факта нарушения.

3. Качество управления риском. Именно степень вовлечённости руководства в процесс управления информационной безопасностью — один из тех показателей, который в целом будет влиять на формирование риск-профиля.

Дополнительный показатель, который не входит в вероятностную оценку, но будет учитываться регулятором, это показатель уровня информационного фона, формирующегося вокруг организации.

Естественно, если коммерческий конкурент сделал вброс, он не будет включаться в риск-профиль, но станет поводом задуматься, что происходит (Рис. 3).

Расчёт и его оценка по риск-профилю в конечном счёте должны привести к двум вещам:

ПНО, ПОН	КО	НФО	СНПС
Подключение поднадзорных организаций к автоматизированной системе обработки инцидентов (АСОИ) для организации информационного обмена с Банком России	✓	✓	✓
Классификация инцидентов защиты информации	✓	✓	✓
Сбор информации об инцидентах защиты информации (ПНО, ПОН)	✓	4 квартал 2019 г.	✓
ПОС	КО	НФО	СНПС
Нормативное закрепление требований по обеспечению информационной безопасности	✓	✓	✓
ГОСТ по защите информации	✓	✓	✓
ГОСТ по обеспечению операционной надежности	2020 г.	2020 г.	2020 г.
Разработка методики оценки соответствия установленным требованиям	✓	✓	✓
Сбор информации по показателю (ПОС)	4 квартал 2019 г. в виде самооценки	4 квартал 2019 г. в виде самооценки	4 квартал 2019 г. в виде самооценки
КУР	КО	НФО	СНПС
Установление базовых требований по управлению риском информационной безопасности	✓	✓	✓
ГОСТ по управлению риском информационной безопасности	2020 г.	2020 г.	2020 г.

Рисунок 3. Перспективный подход для расчёта риск-профиля поднадзорных организаций

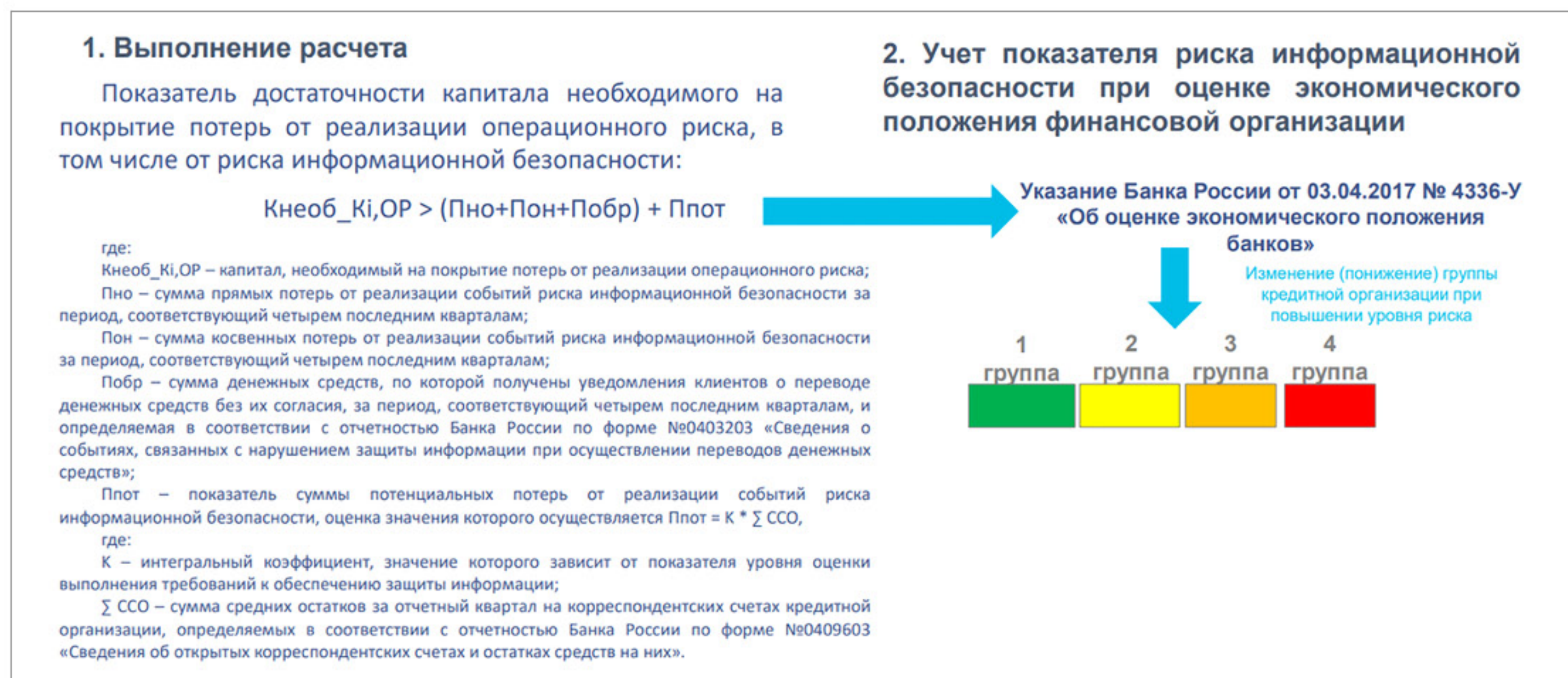


Рисунок 4. Перспективный подход для расчёта профиля риска кредитных организаций

1. Обоснованное и адекватное формирование мер воздействия, включая штрафы и иные меры, предусмотренные законом.

2. Изменение экономического положения банка. Практика разбора ситуаций с хищениями показывает, что отсутствие правильного корпоративного управления, адекватной оценки рисков, невнимание к вопросам информационной безопасности приводит к потере и собственного капитала, и изменению ситуаций с возможностью кредитования на межбанковском рынке (Рис. 4).

При этом, было отмечено, что потенциальный риск на кредитную организацию оценивается, как средний дневной остаток по корсчёту

плюс средний дневной приход на корсчёт. Как показывает практика по хищениям, начиная с 2015 года, статистика точно попадает в этот показатель.

РИСКИ И ФИНТЕХ

Большинство современных технологий разрабатывались IT-компаниями для IT-компаний. Однако у них совершенно другая цена при реализации рисков. К чему может привести бездумное использование технологий в финансовой отрасли рассказал представитель НСПК Артём Гутник.

Облака. Практически все компании сегодня используют облачные решения. Но, к сожалению,

нию, это становится причиной потери контроля над периметром.

Недавно появилась новость о том, что задержана бывшая сотрудница Amazon, которая сканировала облако и находила компании с небезопасно настроенным сервисом. В публичный отчёт попала только компания Capital One, пострадавшая от её действий, но по факту в деле фигурируют 29 компаний.

API. Открыто сервис обсуждается на многих площадках, всё понимают, что API — это скорость интеграции между компаниями, за этим будущее. Но, с другой стороны, существует другое понятие — Security through obscurity («безопасность через неясность»). Когда что-то внедряется, о безопасности не думают, поскольку это настолько сложно, что в этом никто не разбирается. А когда появляется открытое API, всё, что пытались спрятать, где надеялись, что не взломают, оказывается снаружи, и двери для злоумышленников открываются сами.

Большие данные. У большинства компаний информация превращается в хаос, поэтому контролировать данные практически невозможно, не говоря уже о том, что полностью удалить информацию о клиенте становится практически невозможно.

DevOps даёт скорость внедрений и возможность воплощать идеи в реальность буквально за считанные дни. Безопасность здесь зачастую тормозит процессы, она становится в параллель, где риск обнаруживается позже, чем попадает на пользователей и клиентов.

Безусловно, технологии — это хорошо, но безопасность и бизнес должны научиться жить в сегодняшних реалиях, потому как, кроме эффективности, есть ещё и свойства безопасности, и они между собой очень тесно связаны.

Весьма показательна здесь история с базой данных MongoDB, которая произошла год назад. Изначально база разрабатывалась, как говорилось выше, IT-компаниями для IT-компаний. А ведь дефолтные конфигурации небезопасны. В итоге пострадало свыше 10 тыс. компаний просто от того, что все базы были открыты. Соответственно, кроме того, что защищать, необходимо понимать, от чего защищаться. Уязвимости есть везде, но, чтобы их найти, нужно потратить много времени и средств.

О МЕЖДУНАРОДНОМ ОПЫТЕ ОБМЕНА ДАННЫМИ. ЧТО МЕШАЕТ?

По словам Василия Карташова, мы значительно проигрываем злоумышленникам в скорости реагирования на новые угрозы и для этого есть вполне объяснимые факторы.

В первую очередь, существуют технические ограничения: какую площадку обмена использовать, какие стандарты, протоколы и т.д.

Конечно, злоумышленники тоже сталкиваются с этой проблемой, но у них нет задачи защищать распределённую инфраструктуру, применять автоматизировано информацию на средства защиты. Преступникам достаточно узнать на форуме о новой угрозе, подобрать соответствующий эксплойт, выбрать жертву и провести атаку.

Юридические ограничения и бизнес-нюансы. Речь идёт о запретах юридических департаментов на обмен информацией о внутренних инцидентах. Кроме того, есть нежелание бизнеса обмениваться информацией с конкурентами.

Законодательные ограничения касаются обмена информацией в рамках антифрода, где трудно соблюсти тонкую грань, что является персональными данными, а что нет.

Геополитические ограничения. Нередко обмен противоречит политике страны-участницы обмена или её руководства. С этим достаточно трудно что-либо сделать, но такие нюансы есть.

Положительные примеры обмена информацией компании BI.ZONE в 2019 году:

1. К платформе обмена Ассоциации банков России, которой не так давно исполнился год, сейчас подключено 70 организаций. Безусловно, платформа, на данный момент, в большей степени функционирует в рамках Российской Федерации, но создана она с прицелом на международный обмен.

2. Киберучения Cyber Polygon. В рамках учений 5 команд из различных международных компаний на практике продемонстрировали, что наличие единого инструмента автоматизированного обмена с применением этой информации на средства защиты, позволяет в несколько раз увеличить общую скорость реагирования на угрозы.

3. Активное взаимодействие с зарубежными вендорами (ESET, Fortinet, Avira).

Автоматизированный инструмент обмена позволяет значительно повысить скорость реагирования на новые угрозы; значительно повышает эффективность расследований инцидентов безопасности, позволяет сэкономить экспертные ресурсы, особенно тем компаниям, у которых нет финансовых возможностей на поддержание большого штата сотрудников по кибербезопасности.

Артём Сычёв обратил внимание, что информационный обмен может осуществляться на разных уровнях. Есть проблемы, которые решаются только между регуляторами стран. К примеру, из юрисдикции Бразилии были атакованы



Фото: Олег Зубко/Ассоциация банков России

российские банки. Банки пытались самостоятельно решить вопрос с представителем Бразилии, но безрезультатно. Атаки прекратились только после взаимодействия Банка России с бразильским регулятором.

ЭКОСИСТЕМЫ. ОПЫТ СБЕРБАНКА

Развитие экосистемы в банках — наиболее обсуждаемая и даже «хайповая» тема последних лет. Но действительно ли эта бизнес-стратегия является панацеей для кредитных организаций? Своим видением поделился представитель Сбербанка Алексей Волков.

Любая компания, входящая в экосистему, должна инвестировать в свою защиту. Это некий комплаенс.

В экосистеме есть большая проблема: её участники имеют разный уровень кибербезопасности и устойчивости. Компания с наименее защищённой инфраструктурой становится главным вектором атаки на всех участников экосистемы.

Сегодня в Сбербанке около 340 дочерних обществ при этом около 70 — фокусные, они тесно интегрированы в инфраструктуру и бизнес-процессы. При построении общей кибербезопасности, по словам Волкова, далеко не на первом месте находятся финансовые затраты. Куда важнее ряд других компонентов:

1. Обмен информацией.

2. Общие правила и стандарты. Сбербанк разработал для всех компаний, участвующих в информационном обмене, свою методологию.

В рамках разработки методологии индивидуально определялся риск-профиль компании через 16 риск-факторов, далее рассчитывался risk

score и на его основании строился индивидуальный ИБ-профиль соответствия. Также формировался текущий профиль и уровень компании, определялись гэпы и составлялся план действий для улучшения защищённости.

3. Технологии. Естественно, не каждая компания может позволить себе специальную технологическую платформу. Дочерние компании Сбербанка, которые подключены к платформе BI.ZONE, получают всю информацию о киберугрозах, проходят экспресс-аудиты, отгружают туда информацию об инцидентах, проходят самооценку защищённости.

Сбербанку это даёт возможность в режиме реального времени видеть состояние всех компаний с точки зрения кибербезопасности, определять эффективность защиты. Также платформа позволяет оперативно взаимодействовать компаниям при возникновении инцидента.

4. Риски и ответственность. Когда компании находятся в общей экосистеме, они должны разделять риски и ответственность за то, что делают. В Сбербанке эта проблема решается следующим образом.

Существует 4 вида соглашения о кибербезопасности в зависимости от степени интеграции в инфраструктуру. В каждом из них указаны меры соответствия минимальному уровню защищённости, прописана ответственность за возможные инциденты/ущерб, который может быть причинён всей экосистеме. Выполнение этого соглашения юридически обязательно для всех.

5. Опыт и знания. Одним из условий является наличие в компании подразделения, отвечающего за кибербезопасность, либо такого

сотрудника. Задача каждого аккаунт-менеджера заключается не в том, чтобы строить кибербезопасность, а в том, чтобы осуществлять коллаборацию между участниками всей экосистемы. Сейчас примерно 15 компаний закреплены за каждым аккаунт-менеджером. При этом не все из 340 дочерних компаний находятся под наблюдением, фокусных — чуть больше семидесяти, поэтому шесть человек прекрасно справляются с этой задачей.

Резюмируя выступление представителя Сбербанка, Артем Сычёв анонсировал, что в следующем году в планах Банка России заняться формированием риск-профиля на экосистему, дабы иметь возможность проследивать развитие атаки на бизнес-уровне, начиная от одного участника системы и заканчивая другим. Как показывает опыт Сбербанка, это единственно правильный вариант для сокращения количества хищений не в одной единице, а в экосистеме в целом.

КАДРЫ

Рост рынка ИТ усугубляет проблему кадров в сфере ИБ. Разобраться в ней попытался Сергей Пазизин.

Представитель ВТБ отметил, что сегодня происходит качественный переход, связанный с изменением места и роли ИБ в бизнесе. Задачи ИБ уже не ограничиваются выполнением контрольных функций. А простое следование стандартам безопасности уже не позволяет обеспечить необходимый уровень защиты. Практически любое изменение бизнес-процессов в банке влияет на работу автоматизированных систем, следовательно, требует анализа со стороны ИБ.

В число задач ИБ-подразделений банка входит не меньше шести направлений: внедрение средств защиты, их настройка и поддержка; выполнение функций операторов ПАК; контроль соблюдения требований ИБ: комплаенс; поиск уязвимостей, тестирование на проникновение, анализ кода разрабатываемых приложений на безопасность; взаимодействие с бизнес-подразделениями, сопровождение разработки.

Чаще всего пытаются поставить на поток универсального безопасника, но это бессмысленно. Каждое направление требует наличия специальных знаний и опыта, а также разных личных качеств.

Для решения этой проблемы нужна, во-первых, гибкая система переподготовки кадров, во-вторых, комплекс профессиональных стандартов, покрывающий все направления. Имеющиеся стандарты покрывают только часть

потребностей. Например, профстандарт «Специалист по информационной безопасности в кредитно-финансовой сфере» идеально подходит для направления, связанного с нормативным регулированием. Однако вопрос сопровождения и разработки там практически не отражён. С. Пазизин заметил, что ВТБ уже направил просьбу учесть это направление в новом стандарте.

Кроме того, при подготовке специалистов кафедры ИБ должны сами определять, какие курсы будут читаться студентам. Также должна быть конкуренция как между кафедрами, так и стандартами. При этом работодатели, как потребители, должны определять, какой вуз готовит подходящих для них специалистов.

Не стоит забывать о мерах, позволяющих оптимизировать работу имеющихся специалистов:

1. совершенствование и унификация нормативного регулирования;
2. международное сотрудничество в области противодействия киберпреступности, эффективное расследование киберпреступлений;
3. развитие защищённых облачных платформ и снятие нормативных ограничений на их использование;
4. разработка и внедрение эффективных средств защиты, в том числе для эффективной идентификации и аутентификации потребителей финансовых услуг.

Андрей Лисицын продолжил тему профессиональных квалификаций и подчеркнул, что текущие проекты стандартов концентрируются либо на технологиях, либо на регуляторных требованиях.

С 1 июля 2019 года любые оценки специалистов, которые проводятся работодателями могут осуществляться только в соответствии с Независимой оценкой специалистов.

* * *

Вывод, сделанный на круглом столе: если раньше ИБ была всё запрещающим центром затрат, то сегодня она — необходимый партнёр различных бизнес-инициатив. Конечно, есть специалисты, по-прежнему живущие старыми представлениями, но в целом ИБ активно помогает снижать риски при внедрении новых технологий и защищает деньги банка и его клиентов. Если учитывать, что по ту сторону баррикад всё больше людей вовлекается в преступную деятельность, необходимо ещё больше внимания уделять возникающим ИБ-рискам. От этого будет зависеть будущее организаций, которые вкладываются именно в цифровизацию и используют современные бизнес-стратегии.



Валерий ЕСТЕХИН
эксперт по вопросам
информационной
безопасности,
автор блога
estekhin.blogspot.ru

БАНК, ТЫ ГОТОВ?

ДОРОЖНЫЙ АТЛАС БАНКОВСКОЙ СЛУЖБЫ ИБ

Последние год-полтора российские банки испытывают сильное регуляторное давление: вступление в силу изменений в 161-ФЗ [1], новая редакция Положения № 382-П [2], новые Положения № 672-П [3] и 683-П [4]. Эти нормотворческие инициативы mnoжат текущие печали банков, готовя их к неизбежному: выполнению, начиная с 2021 года, требований ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер».

Кроме того, информационная безопасность становится ещё одним обязательным разделом отчётности кредитных организаций. Очевидно, для решения возложенных на банки как перечисленных, так и других задач (ввод в эксплуатацию АРМ КБР-Н, сбор биометрии, выполнение требований Закона № 187-ФЗ [5]) соответствующим службам надо как можно скорее определиться с приоритетами.

Чтобы добраться из точки «А» в точку «Б», необходимо знать, где вы находитесь, куда стремитесь попасть и, главное, какие препятствия вас ожидают в пути. Решению поставленных задач, надеюсь, поможет приведённый ниже дорожный атлас банковской службы информационной безопасности.

К ЧЕМУ БАНК ДОЛЖЕН БЫЛ БЫТЬ ГОТОВ С 01.07.2018

1. Обеспечить защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными Банком России (Положение № 382-П) (п. 3 ст. 27 Закона № 161-ФЗ).

2. Проводить ежегодные тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры. Осуществлять анализ уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений только с привлечением лицензиатов ФСТЭК России (абз. 3 подп. 2.5.5.1 п. 2.5 Положения № 382-П).

3. Обеспечить проведение оценки соответствия не реже одного раза в два года, а также по требованию Банка России (подп. 2.15.2 п. 2.15 Положения № 382-П).

Организация, ставшая оператором по переводу денежных средств, оператором платёж-

ной системы, оператором услуг платёжной инфраструктуры, должна провести первую оценку соответствия в течение 6 месяцев после получения соответствующего статуса.

4. Информировать Банк России, а именно Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ), об инцидентах ИБ, а также о планируемых мероприятиях по раскрытию информации об инцидентах (абз. 2 и 3 подп. 2.13.1 п. 2.13 Положения № 382-П).

5. Устанавливать ограничения на основании заявления клиента по параметрам операций, которые могут осуществляться клиентом с использованием системы интернет-банкинга (подп. 2.8.3 п. 2.8 Положения № 382-П).

6. Если принимается решение, что защита персональных данных (ПДн) будет обеспечиваться с помощью средств криптографической защиты информации (СКЗИ), — обеспечить соответствие применения средств защиты Приказу ФСБ России № 378 [6] (абз. 1, подп. 2.9.1 п. 2.9 Положения № 382-П).

К ЧЕМУ БАНК ДОЛЖЕН БЫЛ БЫТЬ ГОТОВ С 01.01.2019

По состоянию на 31.12.2018 обеспечить сбор биометрии не менее чем в 20 % офисов (Информационное письмо № ИН-03–13/40 [7]).

К ЧЕМУ БАНК ДОЛЖЕН БЫЛ БЫТЬ ГОТОВ С 27.03.2019 [8]

1. Приостанавливать исполнение распоряжения о переводе на срок не более 2 рабочих дней при выявлении операции с признаками перевода денежных средств без согласия клиента. При этом признаки перевода без согласия клиента устанавливает Банк России (п. 5.1 ст. 8 Закона № 161-ФЗ).

2. Незамедлительно возобновлять исполнение распоряжения при получении от клиента подтверждения (п. 5.3 ст. 8 Закона № 161-ФЗ) либо возобновлять исполнение распоряжения по истечении 2 рабочих дней после дня уведомления клиента банком при неполучении от клиента обратной связи (п. 9.1 ст. 9 Закона № 161-ФЗ).

3. Реализовывать мероприятия по противодействию осуществлению переводов денежных средств без согласия клиента в порядке (гл. 2 Указания № 4926-У [9]), установленном Банком России (п. 4 ст. 27 Закона № 161-ФЗ).

4. Направлять в Банк России информацию обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента по форме и в порядке, которые установлены Банком России (п. 6 ст. 27 Закона № 161-ФЗ).

5. Применять полученную от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов без согласия клиента (п. 2.1 гл. 2 Указания № 4926-У).

6. Определить в документах, регламентирующих процедуры управления рисками, процедуры выявления операций, соответствующих признакам переводов без согласия клиента, на основе анализа характера, параметров и объема совершаемых клиентами операций (абз. 9 п. 2.2 гл. 2 Указания № 4926-У).

7. Реализовывать в отношении клиента — получателя средств, в адрес которого ранее совершались операции по переводу без согласия клиента, в случаях, предусмотренных договором банковского счёта, ограничения (абз. 10 п. 2.2 гл. 2 Указания № 4926-У):

- ♦ по параметрам операций по осуществлению переводов денежных средств (электронных денежных средств) с использованием платёжных карт;

- ♦ на получение наличных денежных средств в банкоматах за одну операцию и (или) за определённый период.

8. Создать систему выявления и мониторинга переводов без согласия клиента в платёжной системе на основе информации о переводах без согласия клиента (п. 2.3 гл. 2 Указания № 4926-У).

Также должен быть определён порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента для участников платёжной системы.

К ЧЕМУ БАНК ДОЛЖЕН БЫЛ БЫТЬ ГОТОВ С 06.04.2019

(касается взаимодействия с платёжной системой Банка России)

1. ОПКЦ [10] должен разместить объекты информационной инфраструктуры, используемые при предоставлении операционных услуг и услуг платёжного клиринга участникам СБП [11], в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей. Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) ОПКЦ должен применять меры защиты информации, реализующие усиленный уровень (уровень 1) защиты, определённый ГОСТ Р 57580.1–2017 (п. 5 Положения № 672-П).

2. Обеспечить реализацию контура формирования электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП [12] с использованием разных рабочих мест, разных криптографических ключей и с привлечением отдельных работников для каждого из контуров (п. 1.1 Приложения [13] к Положению № 672-П).

3. Обеспечить, чтобы объекты информационной инфраструктуры контура формирования электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП были размещены в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформляется документально и согласовывается со службой информационной безопасности участников ССНП (п. 1.2 Приложения к Положению № 672-П).

К ЧЕМУ БАНК ДОЛЖЕН БЫЛ БЫТЬ ГОТОВ С 01.06.2019

Проводить ежегодные тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры (подп. 3.2 п. 3 Положения № 683-П).

К ЧЕМУ БАНК ДОЛЖЕН БЫЛ БЫТЬ ГОТОВ С 29.06.2019

1. Работать на ПК АРМ КБР-Н и АРМ КБР-СПФС (окончание срока миграции на ПК АРМ КБР-Н и АРМ КБР-СПФС — 28.06.2019).

2. Касается взаимодействия с платёжной системой Банка России: обеспечить формирование и подписание электронных сообщений участника ССНП и ОПКЦ в информационной инфраструктуре (автоматизированной системе) участника ССНП и ОПКЦ (п. 9 Положения № 672-П).

К ЧЕМУ БАНК ДОЛЖЕН БЫЛ БЫТЬ ГОТОВ С 01.07.2019

По состоянию на 30.06.2019 обеспечить сбор биометрии не менее чем в 60% офисов (Информационное письмо № ИН-03–13/40).

К ЧЕМУ БАНК ДОЛЖЕН БЫТЬ ГОТОВ С 01.01.2020

1. По состоянию на 31.12.2019 обеспечить сбор биометрии не менее чем в 100% офисов (Информационное письмо № ИН-03–13/40).

2. Исполнять требования к прикладному ПО [14] (сертификация ФСТЭК России или анализ уязвимостей по уровню ОУД 4 [15] с помощью лицензиата ФСТЭК России) (абз. 2 подп. 2.5.5.1 п. 2.5 Положения № 382-П).

3. Обеспечить разделение контуров подготовки и подтверждения платёжных поручений при использовании платежей через интернет. Дополнительной, а в случае, когда разделение контуров невозможно, — и компенсирующей, мерой должны быть ограничения на параметры операций, что актуально для физлиц, которые не захотят применять два устройства: одно для проведения платежей, другое для их подтверждения (подп. 1.5 п. 1 Указания № 4793-У [16]).

4. Касается взаимодействия с платёжной системой Банка России: ОПКЦ должен обеспечить защиту электронных сообщений при их передаче в Банк России с применением средств защиты информации, реализующих двухстороннюю аутентификацию и шифрование информации на уровне звена данных или сетевом уровне, в соответствии с эталонной моделью взаимосвязи открытых систем, определённой в ГОСТ Р ИСО/МЭК 7498-1-99, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности (абз. 5 подп. 14.4 п. 14 Положения № 672-П).

5. Исполнять требования к прикладному ПО (сертификация ФСТЭК России или анализ уязвимостей по уровню ОУД 4 с помощью лицензиата ФСТЭК России) (подп. 4.1 п. 4 Положения № 683-П).

К ЧЕМУ БАНК ДОЛЖЕН БЫТЬ ГОТОВ С 01.01.2021

1. Обеспечить реализацию требований ГОСТ Р 57580.1-2017 (подп. 3.1 п. 3 Положения № 683-П):

- ♦ системно значимые кредитные организации — усиленный уровень (уровень 1) защиты информации по ГОСТ Р 57580.1-2017;

- ♦ остальные кредитные организации — стандартный уровень (уровень 2) защиты информации по ГОСТ Р 57580.1-2017.

2. Проводить оценку соответствия уровню защиты информации, установленному в подп. 3.1 п. 3 Положения № 683-П, не реже одного раза в два года.

Оценка соответствия защиты информации должна осуществляться с привлечением сторонних организаций, имеющих лицензию на проведение работ и услуг, предусмотренных подп. «б», «д» или «е» п. 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого По-

становлением Правительства РФ от 03.02.2012 № 79 (п. 9 Положения № 683-П).

3. Обеспечить соответствие не ниже уровня 3 [17] согласно ГОСТ Р 57580.2-2017 (подп. 9.2 п. 9 Положения № 683-П).

К ЧЕМУ БАНК ДОЛЖЕН БЫТЬ ГОТОВ С 01.07.2021

1. Касается взаимодействия с платёжной системой Банка России: участники ССНП и СБП размещают объекты информационной инфраструктуры, используемые при осуществлении переводов денежных средств с использованием сервиса срочного перевода и сервиса несрочного перевода, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей (п. 3 и 4 Положения № 672-П).

2. Применять меры защиты информации, реализующие стандартный уровень (уровень 2) защиты информации, определённый ГОСТ Р 57580.1-2017.

3. Касается взаимодействия с платёжной системой Банка России: разработать документы, определяющие состав и порядок применения организационных мер защиты информации, а также технических средств защиты информации в рамках процессов (направлений) защиты информации, определённых ГОСТ Р 57580.1-2017 (п. 6 Положения № 672-П).

4. Касается взаимодействия с платёжной системой Банка России: проводить оценку соответствия по Методике национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 (абз. 3 и 4 п. 20 Положения № 672-П).

Оценка соответствия должна проводиться не реже одного раза в два года, а также по требованию Банка России.

5. Касается взаимодействия с платёжной системой Банка России: участники СБП и ОПКЦ должны обеспечить применение средств защиты информации, реализующих двухстороннюю аутентификацию и шифрование информации на уровне звена данных или сетевом уровне, в соответствии с эталонной моделью взаимосвязи открытых систем, определённой в ГОСТ Р ИСО/МЭК 7498-1-99, прошедших процедуру оценки соответствия требованиям (абз. 6 подп. 14.3 п. 14 Положения № 672-П).

К ЧЕМУ БАНК ДОЛЖЕН БЫТЬ ГОТОВ С 01.01.2023

1. Касается взаимодействия с платёжной системой Банка России: участники ССНП, участники СБП и ОПКЦ должны обеспечить для объектов информационной инфраструктуры, размещённых в отдельных выделенных сегментах (группах сегментов) вычислительных сетей,

уровень соответствия не ниже четвёртого согласно ГОСТ Р 57580.2–2018 (абз. 5 п. 20 Положения № 672-П).

2. Обеспечить соответствие не ниже уровня 4[18] согласно ГОСТ Р 57580.2–2017 (подп. 9.2 п. 9 Положения № 683-П).

К ЧЕМУ БАНК ДОЛЖЕН БЫТЬ ГОТОВ С 01.01.2024

Оператору значимой платёжной системы[19] необходимо обеспечить использование в аппаратных модулях безопасности СКЗИ, реализу-

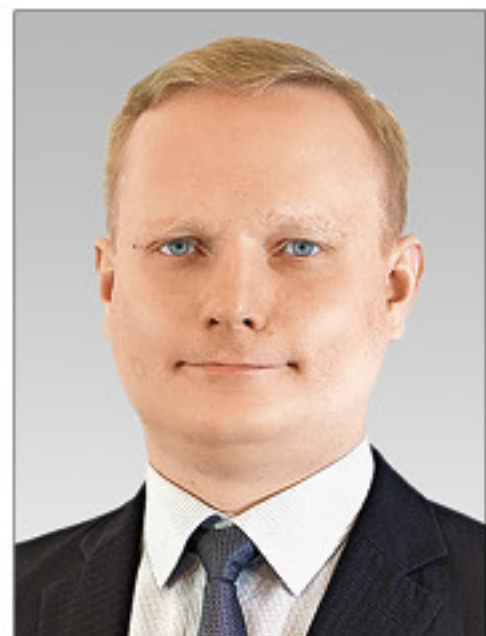
ющих иностранные криптоалгоритмы, имеющих подтверждение ФСБ России (абз. 3 подп. 1.9 п. 1 Указания № 4793-У).

К ЧЕМУ БАНК ДОЛЖЕН БЫТЬ ГОТОВ С 01.01.2021

Оператору значимой платёжной системы необходимо обеспечить использование в аппаратных модулях безопасности СКЗИ, реализующих отечественные криптоалгоритмы, имеющих подтверждение ФСБ России (абз. 4 подп. 1.9 п. 1 Указания № 4793-У).

ПРИМЕЧАНИЯ

1. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платёжной системе».
2. Положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».
3. Положение Банка России от 09.01.2019 № 672-П «О требованиях к защите информации в платёжной системе Банка России».
4. Положение Банка России от 17.05.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиентов».
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости».
7. Информационное письмо Банка России от 28.06.2018 № ИН-03-13/40 «Об особенностях применения мер к банкам при совершении ими действий, предусмотренных пунктом 5.6 статьи 7 Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма».
8. Банк России до 26.03.2019 (включительно) отложил меры воздействия на банки за невыполнение положений новой редакции Закона № 161-ФЗ (Информационное письмо Банка России от 09.10.2018 № ВН-03-56-3-2/3398).
9. Указание Банка России от 08.10.2018 № 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платёжных систем, операторами услуг платёжной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платёжных систем, операторами услуг платёжной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента».
10. ОПКЦ — операционный центр, платёжный клиринговый центр другой платёжной системы при предоставлении операционных услуг и услуг платёжного клиринга при переводе денежных средств с использованием сервиса быстрых платежей.
11. СБП — система быстрых платежей.
12. ССНП — сервис срочного перевода и сервис несрочного перевода.
13. Правила материально-технического обеспечения формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП, а также правила материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ.
14. Под термином «прикладное ПО», очевидно, подразумевается ПО, которое непосредственно участвует в переводе денежных средств, например: АБС, клиент-банк, мобильный банк, процессинг, ДБО, интернет-банк и др.
15. ОУД 4 предусматривает методическое проектирование, тестирование и просмотр. ОУД 4 применим, когда разработчикам или пользователям требуется независимо получаемый уровень доверия от умеренного до высокого в ОО (объекте оценки) общего назначения и имеется готовность нести дополнительные связанные с безопасностью производственные затраты. Это самый высокий уровень, на который обычно экономически целесообразно ориентироваться для существующих типов продуктов. Анализ поддерживается независимым тестированием ФБО (функции безопасности объекта), свидетельством разработчика об испытаниях, основанных на функциональной спецификации и проекте верхнего уровня, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций, свидетельством поиска разработчиком уязвимостей и независимым анализом уязвимостей, демонстрирующим противодействие попыткам проникновения нарушителей с низким потенциалом нападения.
16. Указание Банка России от 07.05.2018 № 4793-У «О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П».
17. Третий уровень соответствия: организационные и технические меры процесса системы защиты информации (ЗИ) реализуются в значительном количестве на постоянной основе в соответствии с общими подходами (способами), установленными в финансовой организации. Контроль и совершенствование реализации организационных и технических мер процесса системы ЗИ осуществляются бессистемно и (или) эпизодически.
18. Четвёртый уровень соответствия: организационные и технические меры процесса системы ЗИ реализуются в полном объёме на постоянной основе в соответствии с общими подходами (способами), установленными в финансовой организации. В финансовой организации в основном реализованы контроль и совершенствование организационных и технических мер процесса системы ЗИ.
19. К значимым платёжным системам можно отнести, например, Visa, MasterCard, НСПК и др.



Евгений КАРПОВ
начальник отдела
информационной
безопасности
АО КБ «Хлынов»

ЛЁГКАЯ КАВАЛЕРИЯ

МАЛЫЕ БАНКИ БЛИЖЕ К ЧЕЛОВЕКУ И ПЕРВЫМИ ВСТАЮТ НА ЕГО ЗАЩИТУ

Предлагаю остановиться на самом остром виде социальной инженерии, задевающим наших клиентов, простых людей. Сегодня почти все пользуются банковскими картами и, казалось бы, имеют достаточный опыт в обращении с ними. Но по-прежнему многие, получив звонок «из банка», доверяют звонящему, представившемуся «Василием из службы безопасности».

По опыту нашего банка, украсть деньги у неискушённого человека достаточно просто — достаточно выудить у него информацию о номере и сроке действия карты, а также код CVC на её обороте. После этого обычно заявляется, что «обнаружена мошенническая операция на 15 000 рублей — для её отмены надо ввести код из СМС». Человек, чуть раньше уже выполнивший несколько указаний мошенников, «на автомате» называет цифры из текстового сообщения и теряет указанную сумму.

ТЕХНОЛОГИЯ ОБМАНА

Что же стоит за этой простой, но стабильно работающей и эффективной операцией? Каков её механизм?

Сегодня это, опять же из опыта нашего банка, хорошо отлаженный бизнес-процесс, где:

- ◆ Чётко разделены роли.
- ◆ Продуман сценарий и алгоритм действий. Чаще несколько сценариев.
- ◆ Операторы «на телефоне» прошли обучение и уверенно играют свою роль в соответствии со сценарием.
- ◆ Подготовлены карты и счета для приёма денег.
- ◆ Готовые к снятию денежных средств соучастники дежурят у банкоматов.
- ◆ Есть координатор действий.
- ◆ Подготовлен к работе комплекс технических средств для управления звонками и денежными потоками.

Всё начинается с подготовки операторов. Они должны легко ориентироваться в сценариях. Как правило, под разные типовые профили жертв используются разные подходы.

Для привлечения «клиентов» часто в ход идут рассылки СМС. Такие сообщения обычно выглядят как информация о списании денежных средств, но, в отличие от настоящих сообщений, в них нет суммы остатка на карте. Чаще

используются просто «слепые звонки» с перебором указанного координатором диапазона номеров. Иногда общение с «оператором» предваряет текст, прочитанный роботом. Задача робота — повысить авторитет оператора, а также отфильтровать грамотных людей, которые «не ведутся» и бросают трубку. Такие люди знают, что настоящий сотрудник банка, обзванивающий клиентов, всегда обращается к ним по имени-отчеству. Это самый первый фильтр от звонков мошенников.

Если «клиент повёлся», в дело вступает Оператор, представляющийся, как правило, сотрудником службы безопасности (обычно называется самый популярный банк в регионе). Его задача рассказать клиенту, что «деньги вот-вот украдут», и провести его по всем этапам сценария.

Что Оператору важно:

- ◆ Какой банк выпустил карту — от этого зависят лимиты на операции по карте.
- ◆ Номер карты, срок действия, код CVC — нужны для перевода денежных средств.
- ◆ Примерный остаток средств на карте — это позволит украсть максимум без лишних операций.

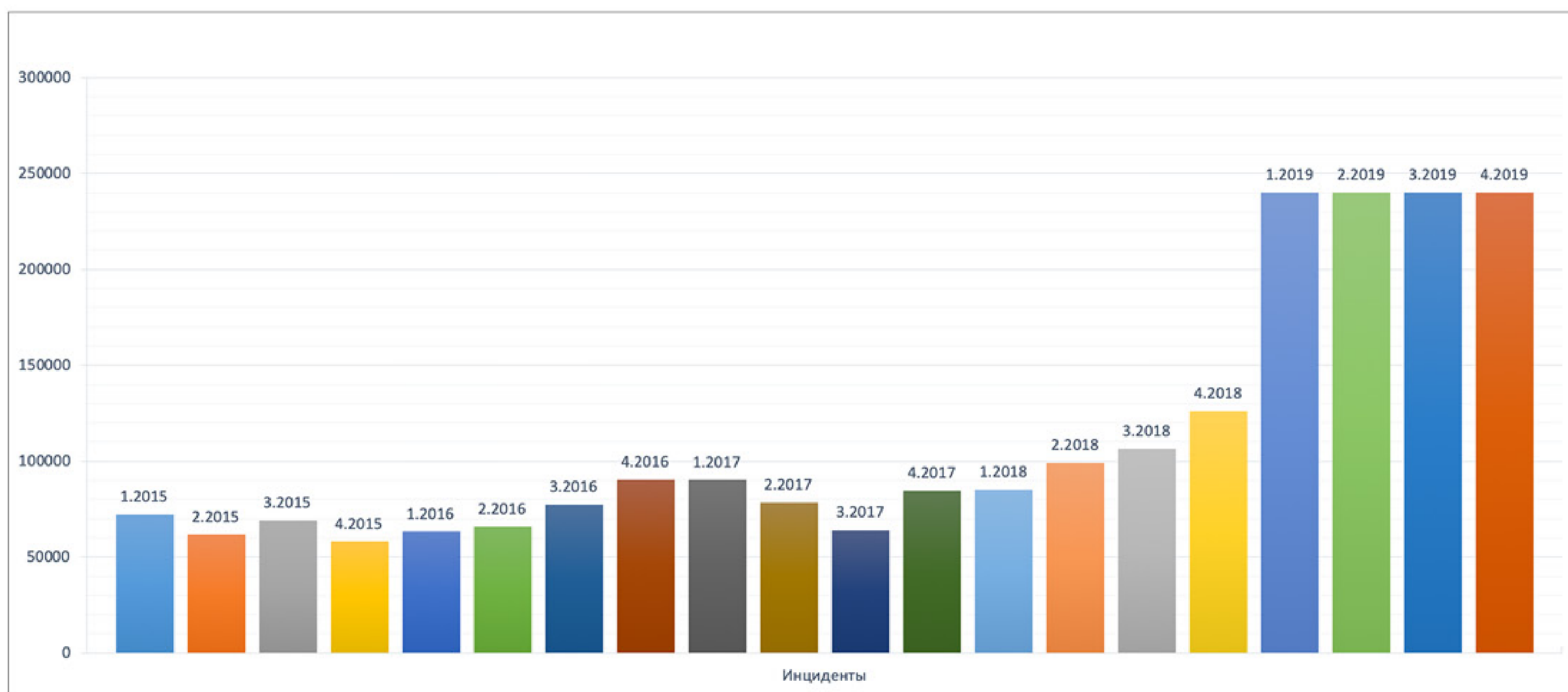
Интересный факт: при ответе, что на карте «около 100 рублей» — просто вешают трубку.

Обычно сценарии мошеннических схем условно можно разделить на виды:

- ◆ классические переводы с карты на карту;
- ◆ подключение карты к электронному кошельку;
- ◆ сброс пароля в Интернет-банке и отправка переводов от имени жертвы.

В первом случае операции повторяются до тех пор, пока у клиента есть деньги на карте. Во втором и третьем — мошенникам достаточно получить единый код, чтобы списать все деньги без дополнительных операций.

Для снижения средней суммы ущерба банки выставляют лимиты на операции. Для обхода этого мошенники используют «многоканальный» вывод денег и сразу несколько сервисов перевода с карты на карту (сервисы «не видят» операций друг друга и не могут на основании серии однотипных списаний остановить операцию). Все операции осуществляются с учётом типовых лимитов каждого конкретного банка. Где-то это 15 тыс. рублей, а где-то и 500 тыс. по конкретному виду. Обычно предельные суммы



намного выше, если клиент осуществляет операции через «свой» Интернет-банк или мобильное приложение.

Интернет-банк удобен не только пользователям, но и мошенникам. Можно увидеть точный остаток денежных средств «жертвы», использовать операции «оплатить услугу», «перевод по реквизитам счёта» и даже «закрыть вклад с переводом денежных средств на карту» или «взять экспресс-кредит у Банка».

Главная задача оператора — сформировать денежный поток на карты мошенников, ответственных за обналичивание в банкоматах. Их карты периодически меняются во избежание блокировки «по подозрению». Тут соучастником воров, как это ни парадоксально, является финтех. Дело в том, что банки не видят получателей денежных средств по переводам своих клиентов (за исключением операций в Интернет-банке). Существующая система банк-сервис-банк проигрывает мошенникам в оперативности. Поскольку данные получателя банк отправителя не видит, а видит сервис, то и заблокировать карту мошенника может только банк-эмитент такой карты. То есть, чтобы добраться до получателя денег, нужно сделать минимум два последовательных запроса.

СРЕДНЯЯ ТЕМПЕРАТУРА ПО БОЛЬНИЦЕ

Сегодня банки предоставляют информацию об инцидентах в ФинЦЕРТ Банка России в режиме почти реального времени. Подавляющее число инцидентов связаны с пластиковыми картами. Официальная сводная статистика публична, любой может ознакомиться с ней на сайте Банка России <http://www.cbr.ru/fincert/>.

Направляя информацию в ФинЦЕРТ, банки видят регистрационный номер своего инцидента. По нему можно судить о числе инцидентов на момент регистрации. В обычный день получается около 4 тыс. инцидентов, но счётчик может быть и больше (видели более 12 тыс.), и меньше — в зависимости от времени дня, активности злоумышленников и банков. Для прогноза возьмём значение 4 тыс. инцидентов в рабочий день.

Предположим, в квартале 60 дней, активность в выходные учитывать не будем, техническими сообщениями, участвующими в том же счётчике, также пренебрежём — их мало. Результат на Рисунке 1.

Цифры 2019 года — это не всплеск, это просто близкая к нижней границе информация о числе инцидентов с пластиковыми картами. Каждый наш клиент, получая письменный ответ на своё сообщение о действиях мошенников, видит регистрационный номер своего инцидента в Банке России и инструкцию по его использованию правоохранительными органами. Данный прогноз не претендует на абсолютную точность, но очень хорошо показывает и смену методологии Банка России и высокую «среднюю температуру по больнице».

ПРОБЛЕМА СЕРВИСОВ

Кто-то может купить навороченную систему антифрода, а кто-то просто грамотно настраивает систему лимитов (ограничение максимального ущерба от операций мошенников в рамках какого-то их сценария). Что мешает работе таких систем? Желание клиентов полной свободы в своих операциях и любовь к использованию первых попавшихся сервисов.

Рисунок 1. Цифры 2019 года — это близкая к нижней границе информация о числе инцидентов с пластиковыми картами

Надо понимать, что для банка важен вопрос удобства клиентов. Как, например, клиенту отправить другу 10 тыс. руб. при лимите 8 тыс.? Пока клиент выбирает вариант «вбить в поисковик и щёлкнуть по первой ссылке» для совершения любого платежа, мы получаем множество сервисов и невозможность сильно снизить сумму лимита на операцию. Банки постоянно дорабатывают свои мобильные приложения, делают свои Интернет-банки удобнее, но человеческая лень делает своё чёрное дело. Для такого разового сервиса конкретный клиент — песчинка — абсолютно незаметен. Возник и пропал, а доход сервиса в виде комиссии, как с мошенников, так и с обычных пользователей одинаков. С сервисами электронных кошельков и виртуальных карт сложнее, но как инструмент приёма платежей при переадресации они активно используются мошенниками.

КАК БОРОТЬСЯ?

К сожалению, законодательная основа для оперативной борьбы отсутствует. Борьба опирается на сами банки, их работу с клиентами и готовность операторов связи реагировать на обращения банков с просьбой прекратить работу мошенников.

Чтобы обезопасить своих клиентов мы выбрали комплексный подход:

- ◆ снизили лимиты на рискованные для клиента операции (при возможности увеличить их в офисе банка или удалённо);
- ◆ добавили механизмы защиты, реагирующие на типовые сценарии мошенников;
- ◆ добиваемся 100% информирования клиентов о действиях мошенников, о мерах безопасности. Даже делали «ковровые» рассылки СМС с предупреждениями для клиентов в самые напряжённые моменты;
- ◆ постоянно публикуем актуальные предупреждения для клиентов везде, где это возможно. Даже вывешиваем их на «первый показ» на странице входа в Интернет-банк (при всплесках активности мошенников);
- ◆ любой звонок в Информационный центр банка с сообщением о мошенниках используется для противодействия мошенникам.

Эффект есть! Мы не победили, но снизили в разы число пострадавших и сумму ущерба для каждого клиента. Своеобразный рекорд: «бригада» мошенников 1,5–2 часа «водила» клиента по различным способам хищения его денежных средств — и всё с нулевым результатом.

Но главное — это повышение грамотности клиентов. На наш взгляд, самое простое — это Стоп-Вопросы. Т.е. слышали в разговоре с «сотрудником» банка хотя бы один пункт, сразу повесьте трубку.

Стоп-Вопросы:

- ◆ Звонящий не знает ваше имя и отчество.
- ◆ Просит назвать полный номер карты (можно 2–4 последние цифры).
- ◆ Просит назвать срок действия карты.
- ◆ Просит назвать CVС код (под любым названием код с оборотной стороны карты).
- ◆ Просит назвать код из СМС.
- ◆ Просит сделать «тестовый платёж».
- ◆ Спрашивает о наличии у вас карт других банков.
- ◆ Спрашивает об остатке денежных средств на карте, даже примерно.
- ◆ Переключает вас на «службу безопасности другой организации».
- ◆ Просит вас сделать какую-то манипуляцию, смысл которой вам непонятен.

Из неожиданного. Фантазия у мошенников работает плохо: «Объединённая служба безопасности всех коммерческих банков», «Служба безопасности Хлыновского Центробанка»...

БАНК ДЛЯ ЧЕЛОВЕКА

У малых банков есть свои минусы. Нас мало, и мы не можем позволить себе «систему антифрода с искусственным интеллектом и космическими технологиями», не можем присутствовать на всех тематических конференциях...

Но есть и плюсы. Мы очень легки на подъём:

- ◆ мы можем подвинуть баннер с продажей новой линейки кредитов в пользу предупреждения об активности мошенников;
- ◆ за пару часов согласовать публикации в социальных сетях и сделать рассылку СМС по самым уязвимым клиентам;
- ◆ просто за 5 минут разработать и запустить новый шаблон реагирования на инциденты, которые только что возникли;
- ◆ немного снизить лимит по операциям в выходной день, сделав его ниже «первой попытки» мошенников, которые активизировались в пятницу;
- ◆ индивидуально отработать каждое обращение клиента по сложным случаям, предложив человеку варианты решения проблемы;
- ◆ просто разобрать для клиента какие-то операции, по которым у него есть вопросы, с изучением правил используемого им финансового сервиса — то, что никогда не сделают в крупном банке;
- ◆ для нас 2 похожих эпизода — это УЖЕ СЕРИЯ: разбираем, оцениваем, принимаем меры.

* * *

Мы видим и слышим каждого нашего клиента, а не безликую массу.

РОЛЬ СТО БР ИББС

ОДА ДРАЙВЕРУ И СТАНДАРТУ

В августе 2019 года произошло почти никем не замеченное событие, которое подвело черту под целой эпохой в банковской ИБ — эпохой Комплекса стандартов СТО БР ИББС. Финансовые организации РФ получили от Банка России письмо «О проведении оценки соответствия требованиям СТО БР ИББС-1.0–2014».

На первый взгляд, ничего сенсационного в этом письме от регулятора не было. Сообщалось, что согласно Положению БР № 683-П с 1 января 2021 года «кредитные организации обеспечивают реализацию мер защиты информации, определенных ГОСТ Р 57580.1–2017, а также предоставляют информацию об оценке выполнения требований к обеспечению защиты..., проводимой в соответствии с положениями ГОСТ Р 57580.2–2018». Исходя из этого: «направлять сведения о выполнении оценки соответствия требованиям СТО БР ИББС-1.2–2014... не требуется». А раз так, то Комплекс стандартов СТО БР ИББС, очевидно, отходит на второй план, сброшен с корабля современности и утрачивает роль драйвера развития ИБ, которую играл последние 15 лет. Заметим, играл фактически, а не де-юре, так как согласно Закону о техническом регулировании СТО БР имеет статус «Необязательный к исполнению».

ПРЕДЫСТОРИЯ

Творение Банка России — Комплекс стандартов СТО БР ИББС — симбиоз международных стандартов, лучших практик обеспечения безопасности и российских ГОСТов. Напомним, что первая редакция стандарта СТО БР ИББС-1.0–2004 (на момент принятия — просто Стандарт Банка России) вступила в действие 1 декабря 2004 года.

Банк России с завидной регулярностью обновлял этот документ:

- ♦ вторая редакция: СТО БР ИББС-1.0–2006;
- ♦ третья редакция: СТО БР ИББС-1.0–2008;
- ♦ четвертая редакция: СТО БР ИББС-1.0–2010;
- ♦ пятая редакция: СТО БР ИББС-1.0–2014.

Первые рекомендации (РС БР ИББС-2.0–2007) в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы РФ. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требова-

ми СТО БР ИББС-1.0» начали действовать с 1 мая 2007 года. Сейчас рекомендаций РС БР ИББС — восемь.

В результате финансовые организации на текущий момент имеют комплект взаимосвязанных стандартов и рекомендаций.

За 15 лет Банку России удалось создать комплект документов, содержащих единые требования по обеспечению информационной безопасности банков РФ. С появлением Стандарта направлению ИБ в кредитно-финансовых организациях придали смысл. Смысл отразился в реальных делах. Реальные дела привлекли внимание бизнеса. Бизнес наделил службу ИБ полномочиями и выделил ресурсы (дал денег и штатные единицы). У ИБ появилась обратная связь с бизнес-подразделениями. Хорошая ИБ стала одним из критериев надёжности банка.

В те времена, когда хакеры ещё атаковали не тех, кого решили, а тех, кого могли, когда ещё верилось в существование большой красной кнопки «Гарантия защиты — 100%», начинать приходилось с элементарного. С определения целей ИБ, с поиска «спонсора» ИБ в компании, с утверждения требований ИБ на уровне организации. В каждом банке началась кропотливая работа по приготовлению фирменного «блюда» — Политики ИБ, написанной по одинаковым, передаваемым из рук в руки рецептам, но уникальной в сознании каждого «блюдодела».

Стандарт Банка России СТО БР ИББС долгое время был основополагающим документом в области защиты информации для банковской системы РФ. Влияние Стандарта на финансовую отрасль сравнимо только с влиянием Закона о персональных данных (152-ФЗ).

Банки должны быть благодарны Комплексу стандартов СТО БР ИББС. Именно с него началось систематическое регулирование ИБ в банковской системе. Документы СТО БР ИББС продолжают действовать в настоящее время и могут применяться банками, как и раньше, по желанию. Более того, Банк России обновляет и дополняет этот комплект документов новыми стандартами и рекомендациями.

Валерий ЕСТЕХИН
эксперт по вопросам
информационной
безопасности,
автор блога
estekhin.blogspot.ru



Дмитрий ОРЛОВ
эксперт по ИТ и ИБ

САМИ С УСАМИ

ИСТОРИЯ ПРО АВТОМАТИЗАЦИЮ ПРОЦЕССОВ ИБ В ОДНОМ БАНКЕ

Началось всё с того, что несколько лет назад в процессе реализации мер информационной безопасности (ИБ) и внедрении требований Положения 382-П и Стандарта СТО БР ИББС-1.0, мы столкнулись с нехваткой ресурсов. На тот момент средств ИБ в банке было внедрено немного, работа подразделения ИБ выполнялась в основном вручную или с использованием Excel. Учёт велся во множестве различных файлов, в бумажных журналах, да и просто в блокнотах сотрудников. Управлять этим становилось всё сложнее, а эффективность реализуемых вручную мер безопасности и контролей оставляла желать лучшего. Ресурсов не хватало даже на реализацию ранее установлен-

ных внутренних требований ИБ, на что регулярно обращала внимание наша Служба внутреннего аудита.

Возникла потребность в автоматизации текущих задач, контрольных мероприятий, централизации учёта и управления ИБ.

В результате проведённого анализа имевшихся на рынке продуктов, готового решения по автоматизации текущей деятельности подразделения ИБ найти не удалось. Возможным вариантом была закупка отдельной системы для каждого направления деятельности, но их общая стоимость выходила за пределы разумного, да и сами эти системы были бы обособленными и не связанными между собой. Поскольку бюджет был ограничен, было решено закупить SIEM-систему и на её базе реализовать мониторинг и часть контролей, а остальное автоматизировать своими силами — навыки программирования были и с ИТ отношения были хорошими.

В итоге создали систему, в которую свели данные об инфраструктуре, антивирусной защите, автоматизированных системах, ролях, пользователях и правах доступа в них. Всё это связали с кадровой информацией о сотрудниках. Где было возможно, подключались напрямую к системам-источникам информации, для остального договорились с ИТ о регулярных выгрузках информации.

На тот момент в банке уже была внедрена SIEM-система, с ней организовали двухсторонний обмен информацией. В неё, для обогащения информации о событиях, выгружались сведения о сотрудниках, пользователях в системах и инфраструктуре, а также различные чёрные списки (IP-адреса, сайты, адреса электронной почты, получаемые от ФинЦЕРТ и ряда других источников). В обратную сторону из SIEM выгружались данные по сработавшим правилам для проведения анализа потенциальных инцидентов и фиксации информации об их обработке.

В результате получилась система, которая позволила на порядок снизить трудозатраты на реализацию текущих задач и контрольных мероприятий, а также реализовать дополнительные контроли, которые были невозможны или неэффективны без автоматизации. Ниже приведено несколько скриншотов.

Если у кого-то появилось желание узнать подробности, мы всегда готовы к общению, потому что нуждаемся в мнениях экспертов.

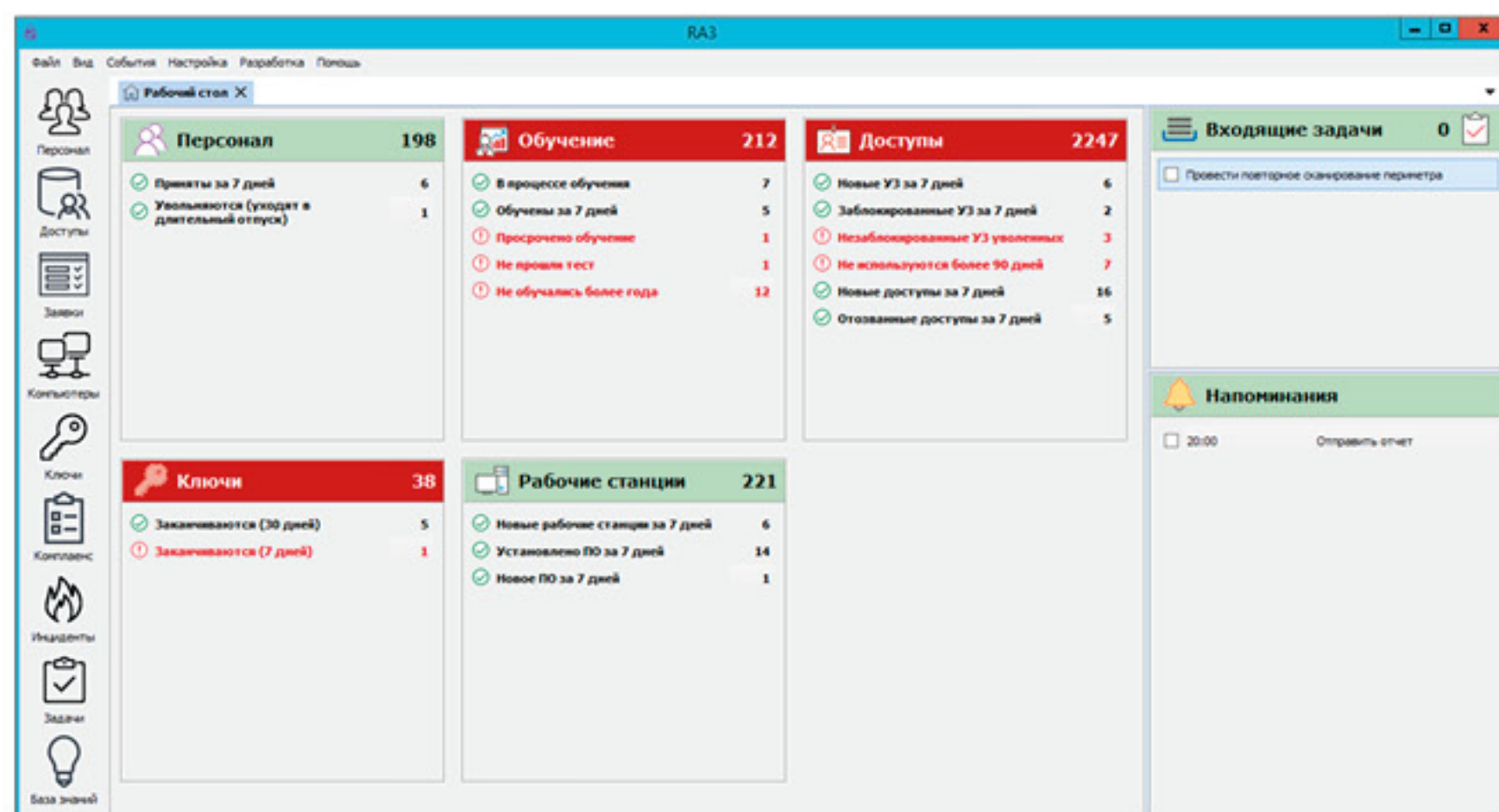


Рисунок 1. Рабочий стол и основная панель мониторинга

Департамент	Логин	Тип УЗ	Последний вход	ФИО
Система: Active Directory (5)	alek...	Пользователь	16.08.2019	К...
	ekat...	Пользователь	10.03.2019	А...
	evge...	Пользователь		М...
	kirill...	Пользователь	08.05.2019	Б...
	vyuc...	Пользователь	11.08.2019	С...
Система: Автоматизированная банковская система (4)				
Система: Кадровая система (1)				
Система: Локальные учетные записи (1)				
Система: Система электронного документооборота (4)				

Рисунок 2. Информация об учетных записях сотрудников

Номер	Дата учета	Название	Назначение	Тип	Состояние	Номера записанных ключей	Названия записанных ключей	Срок действия ключей
KEY-70/43230	27.06.2019	МДЛ-01	Отправка платежей в МДЛ	Жесткий диск	Выдан	КТ-57/24941	Отправка платежей в МДЛ	01.02.2020
KEY-71/71775	27.06.2019	МДЛ-02	Отправка платежей в МДЛ	Жесткий диск	Выдан	КТ-57/24941	Отправка платежей в МДЛ	01.02.2020
KEY-72/97650	01.01.2018	Ключевой ноутбук	Ключи подлинки для внешней сервис	Токен	Выдан	КТ-5/15292, КТ-69/03405,...	КЗП Федеральное казначейство, К...	29.12.2019

Рисунок 3. Учёт криптографических ключей



Денис АНТОНОВ
начальник отдела ИБ банка
«Народный банк»

Задумка и сам продукт действительно хороши. Такая система в состоянии покрыть до 70–80 процентов задач информационной безопасности и облегчить работу менеджменту ИБ малых и средних банков. Тот же консалтинг, учёт криптографических ключей и т.д. А самое приятное, что это полностью отечественная разработка, созданная сотрудниками, проработавшими в ИБ банковского сектора по 15–20 лет, набившими шишки и имеющими более чем полноценный опыт.

BIS-КОММЕНТАРИЙ

Безусловно, такая система незаменима именно для малых и средних банков. В крупных банках всегда есть объёмный и гибкий бюджет и нет недостатка в кадрах, а вот что делать малым и средним? У них таких возможностей нет, а задачи перед ними стоят те же самые — закон для всех един. Не раз слышал от коллег по цеху, мол, хотелось бы иметь универсальный продукт, который покроет ряд задач от консалтинга и аудита до регистрации ключей, и который был бы удобным, информативным и отвечал всем изменениям в законодательстве в сфере ИБ.

Справедливости ради стоит сказать, что на рынке подобные продукты есть, но они громоздки и заточены каждый под определённый процесс, то есть, универсальными их назвать нельзя.

Мои пожелания, чтобы данный продукт был доработан в интересах менеджмента ИБ малых и средних банков. У него есть все шансы быть доведённым до совершенно чего-то нового и стать универсальным средством, которое позволит, быстро и качественно закрывать дыры ИБ не только в банковском секторе, но и в промышленности.



Роман КОСИЧКИН
руководитель направления
аудита ИБ финансового сектора
компании «ЦИБИТ»

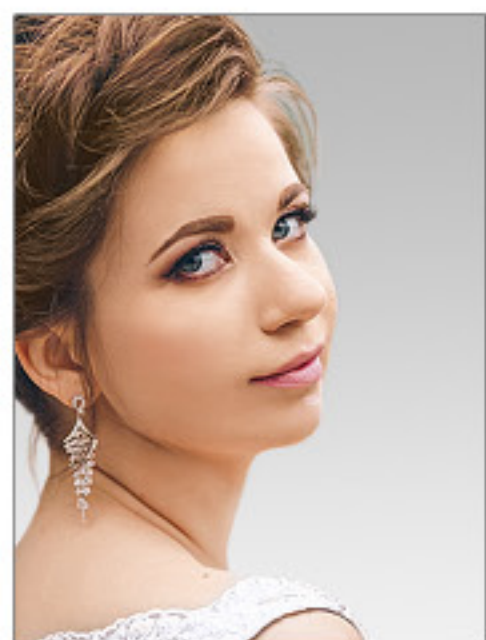
Для нас, аудиторов информационной безопасности, важно собрать как можно больше сведений об объекте, которому мы даём оценку. В качестве свидетельств аудита выступают и документы, регламентирующие систему ИБ и управление ею, и дополнительные свидетельства, такие как настройки систем безопасности, активных сетевых устройств, данные из системных журналов, организация доступа пользователей к различным информационным системам. На практике это оборачивается большими затратами ресурсов как со стороны команды аудиторов, так и со специалистов принимающей финансовой организации. Для получения свидетельств, как правило, выделяется сотрудник службы ИБ, который совместно с аудитором затрачивает много времени для сбора и подготовки данных, влияющих на итоговую оценку.

При наличии рассматриваемой системы время, затраченное на выборку этих данных, снижается в разы. Буквально со своего рабочего места аудиторы и сотрудники подразделения ИБ организации могут получить все требуемые сви-

BIS-КОММЕНТАРИЙ

детельства в режиме «реального времени». Сведения об актуальных версиях нормативных и организационно-распорядительных документов финансовой организации, о режимах доступа пользователя к информационным системам, составе программного обеспечения, настройках систем защиты на компьютерах пользователей, проведённые с ними тренинги и проверка полученных знаний доступны буквально по щелчку мыши. На основании полученных данных у аудиторов полнее складывается картина построенной системы защиты информации в любом из оцениваемых контуров. Всё это делает данную систему незаменимым помощником аудитора ИБ.

Кроме того, нельзя не отметить такой дополнительный положительный фактор, как значительная экономия ресурсов подразделений информационной безопасности. Хотя аудиторы должны сохранять объективность в отношении оцениваемых организаций, мы в ходе сбора свидетельств часто отмечаем чрезвычайно большую загруженность специалистов ИБ, особенно в малых и средних финансовых организациях. Огромная регуляторная нагрузка, необходимость работы с массой технических средств защиты, организация и проведение мероприятий по повышению осведомлённости пользователей приводят к тому, что человеческий фактор становится самым слабым звеном в защите и, следовательно, в системе ИБ появляются бреши. Безусловно, наличие системы, в которой все основные показатели сосредоточены в одном месте, резко снизит нагрузку на сотрудников подразделений ИБ, и качество защиты, а, следовательно, и итоговые оценки аудита возрастут без ущерба для объективности.



Диана КНЯЗЕВА
главный инженер
Управления
экспертизы
кибербезопасности
Сбербанка

БЕЗБУМАЖНЫЙ БАНК

ОСОБЕННОСТИ БЕЗОПАСНОСТИ РЕАЛИЗАЦИИ БЕЗБУМАЖНОЙ ТЕХНОЛОГИИ¹

Чтобы предоставить клиенту и сотруднику самый удобный, безопасный и быстрый способ безбумажного оформления операций, разработан уникальный по своей сути омниканальный модуль подтверждения операций (модуль подтверждения). Этот модуль предоставляет продуктовым системам — потребителям следующие сервисы: проверка доступности технологии БФО в зависимости от имеющихся в учётных системах сведений о клиенте, канале и месте его обращения, типе совершаемой операции; предоставление доступных клиенту способов аутентификации клиента с использованием достоверных и удобных для клиента средств, позволяющих од-

нозначно установить авторство документа; вывод электронных документов на устройства отображения с целью ознакомления с ними клиента и сотрудника банка; формирование и интеграция в электронный документ блока данных, составляющего простую электронную подпись клиента; формирование и проверка усиленной неквалифицированной электронной подписи сотрудника; вызов необходимых компонент для печати электронных документов по желанию клиента и (или) отправки их на верифицированный электронный почтовый адрес клиента; отправка сформированных и подписанных электронных документов на хранение в электронный архив.

¹ Окончание. Начало в №3 / 2019

АЛГОРИТМ РАБОТЫ МОДУЛЯ ПОДТВЕРЖДЕНИЯ

Ознакомиться с общей схемой алгоритма работы модуля подтверждения можно на рис. 4.

Процесс подтверждения, как правило, начинается с инициации отправки запроса (request) от продуктовой автоматизированной системы (АС) в модуль подтверждения. Взаимодействие между модулем и продуктовой АС осуществляется с использованием современного защищённого протокола взаимодействия TLS версии 1.2 с контролем клиентского и серверного сертификата. Предусловием для отправки данного запроса является наличие идентифицированного клиента и активной сессии обслуживания, содержащей сведения об операторе, обслуживающем клиента, клиенте и канале взаимодействия. Состояние активности клиентской сессии контролируется модулем подтверждения на всех этапах во избежание несанкционированного подтверждения операции без ведома клиента.

При приёме полученного сообщения в первую очередь осуществляется его валидация на соответствие разрешённому формату, а его содержимое — эталонной XSD-схеме. Передача данных, не прошедших проверку корректности на каком-либо этапе, категорически запрещена.



Рисунок 4. Общая схема алгоритма работы модуля подтверждения

Далее модуль подтверждения осуществляет логический контроль и анализ полученных данных для формирования соответствующего сценария поведения.

ОСОБЕННОСТИ ОПРЕДЕЛЕНИЯ ДОСТУПНОГО СЦЕНАРИЯ ПОДТВЕРЖДЕНИЯ

Во-первых, проверяется наличие у клиента подписанного ДБО. Эти сведения содержатся в тексте запроса, отправленного продуктовой АС при вызове модуля подтверждения в специальном объекте, отвечающем за предоставление полных сведений о клиенте. Если наличие подписанного клиентом ДБО не подтверждено, то проведение операции с использованием технологии БФО становится недоступным клиенту, и используется стандартный путь оформления операции с проставлением на документе собственноручной подписи клиента.

Во-вторых, анализируется возможность проведения БФО по месту обращения клиента в соответствии с установленными правилами банка. Правила параметризованы и доступны для изменения в любой момент бизнес-администратору, ответственному за процесс через специальный прикладной интерфейс. Таким образом банк может обеспечивать гибкость ведения бизнеса.

В-третьих, производится анализ способа идентификации клиента. Так, например, если идентификация клиента была произведена с использованием карты и ввода PIN, то в специальном поле, отвечающем за наличие сведений о сессии обслуживания, будут содержаться сведения об этой карте. Если идентификация клиента проведена без использования банковской карты, то дополнительно производится проверка наличия действующих карт клиента и верифицированных банком номеров мобильных телефонов клиента. Эта проверка необходима, чтобы определить приоритетный для клиента сценарий подтверждения операции, исключением являются критичные операции, где логика подтверждения определяется на основании сведений, полученных от системы фрод-мониторинга.

Дополнительно проверяются полученные номера телефона клиента на холодный период и на замену сим-карты (проверка IMSI) с целью минимизации возможного риска мошенничества. Холодный период — это время, в течение которого нельзя подтверждать операции конкретным инструментом клиента, выбранным для подтверждения (карта, смс или биометрия). Для этого производится сравнение текущего времени и даты со значением



Рисунок 5. Сценарии подтверждения операции

поля в объекте, отвечающем за дату последнего обновления номера телефона, дату выдачи карты или дату создания биометрического шаблона. После проведения вышеуказанных проверок модуль подтверждения возвращает в продуктовую АС ответ (response), который содержит список доступных в данном канале клиенту сценариев подтверждения операции, исходя из анализа сведений, полученных от продуктовой АС.

СЦЕНАРИИ ПОДТВЕРЖДЕНИЯ ОПЕРАЦИИ

На текущий момент доступны три типа сценария (рис. 5): собственноручная подпись, карта плюс PIN или смс-код либо ЭП на отчуждаемом носителе (для корпоративных клиентов или если в процессе участвуют запросы в госорганы). В ближайшее время планируется добавление нового типа сценария — биометрия, этот сценарий будет доступен клиенту при наличии подписанного согласия на обработку биометрических персональных данных клиента и актуального биометрического шаблона.

Сценарий подтверждения собственноручной подписью. Продуктовая АС формирует шаблон документа на основании введенных в

В ближайшее время планируется добавление нового типа сценария — биометрия, этот сценарий будет доступен клиенту при наличии подписанного согласия на обработку биометрических персональных данных клиента и актуального биометрического шаблона

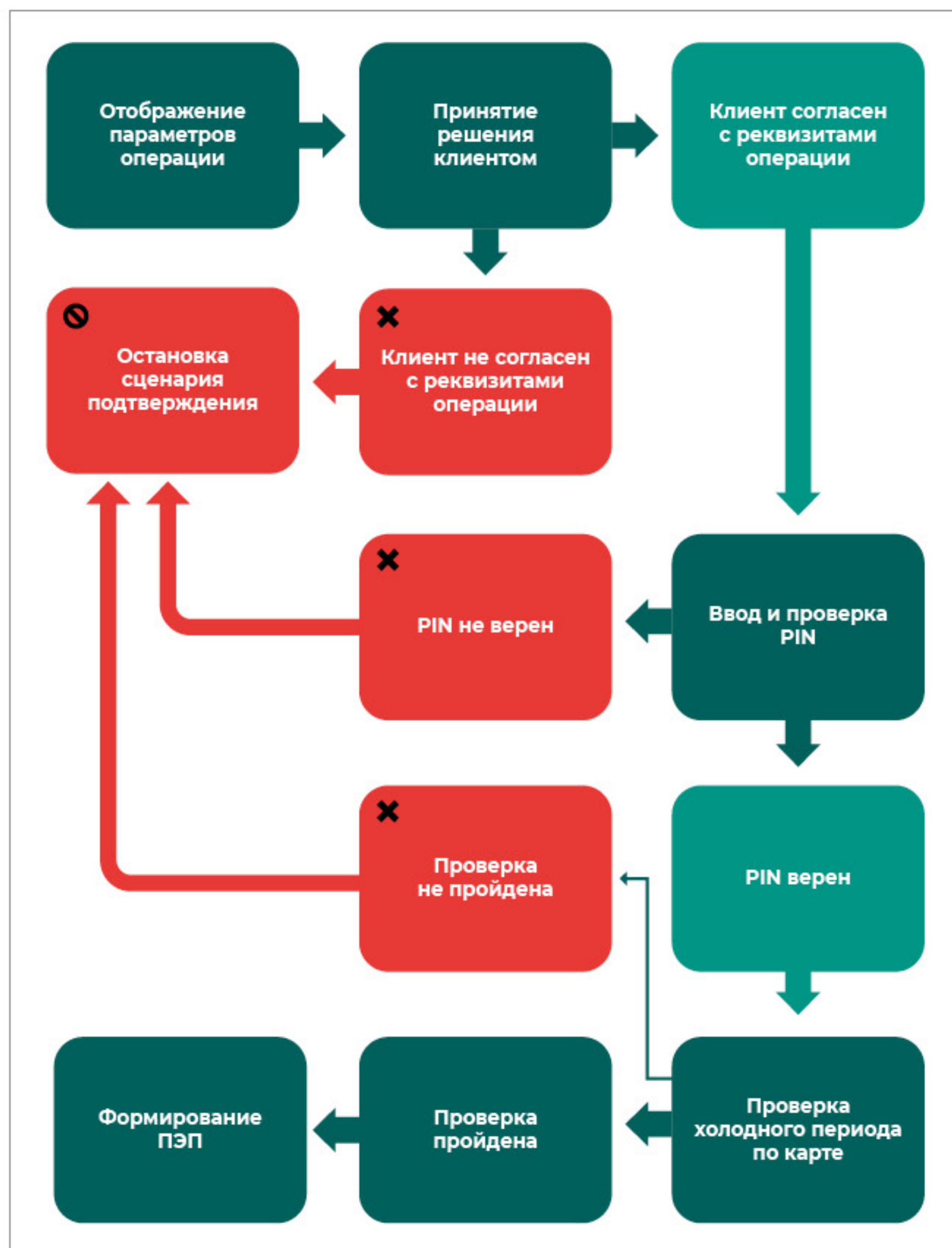


Рисунок 6. Сценарий подтверждения карта плюс PIN

систему реквизитов операции, а модуль подтверждения, в свою очередь, осуществляет вызов разработанного программного компонента печати. Синхронно с этим процессом производится запись в журнал аудита факта печати. При разработке любого программного компонента для конкретных задач необходимо учитывать потенциальную возможность его использования злоумышленником. Именно поэтому при разработке программных компонентов в их структуру добавляется обязательное правило — вызов функций допускается только из разрешённого домена, как правило, таким доменом является внутренняя сеть банка.

Сценарий подтверждения (аутентификации) карта плюс PIN. Общая схема данного сценария подтверждения представлена на рис. 6.

Продуктовая АС формирует текст с реквизитами операции для POS-терминала, который передаётся в модуль подтверждения в специальном поле. Модуль подтверждения осуществ-

ляет вызов специального компонента для взаимодействия с POS-терминалом, и параметры операции мгновенно передаются на экран POS-терминала для ознакомления с ними клиентом. Если клиент согласен, то он нажимает «зелёную кнопку» (процесс продолжается дальше), если не согласен, то нажимает «красную кнопку» (процесс приостанавливается, осуществляется возврат к выбору способа подтверждения операции, а на экране POS-терминала отображается окно с отображением соответствующей ошибки). Факт согласия и отказа клиента передаётся в журнал аудита в синхронном режиме с указанием: места и времени проведения операции; идентификатора клиента; идентификатора операции; даты и времени подтверждения или отказа по операции; способа подтверждения операции; идентификатора сотрудника, принявшего участие в формировании операции. Необходимость записи событий в журнал аудита обоснована эффективностью его использования при расследовании случаев мошенничества и формировании доказательной базы при создании той или иной операции.

Клиент нажал «зелёную кнопку» — осуществляется проверка наличия карты в POS-терминале, и если карта обнаружена, то с помощью программного компонента на POS-терминал отправляется команда для активирования функции ввода PIN. После ввода клиентом PIN POS-терминал отправляет запрос в процессинговую систему на проверку введённого PIN и возвращает полученный код ответа. Если от процессинговой системы получен код, соответствующий коду «PIN неверный», то клиенту предоставляется ещё одна попытка (максимально разрешено три попытки). Если от процессинговой системы вернулся код, соответствующий коду «карта заблокирована или срок действия истёк», то процесс приостанавливается, осуществляется возврат к выбору способа подтверждения операции, а на экране POS-терминала отображается окно с отображением соответствующей ошибки. Если от процессинговой системы получен код соответствующий коду «PIN верный», то осуществляется проверка принадлежности карты банку и идентифицированному в продуктовой АС клиенту.

Дополнительно производится обязательная проверка — находится ли карта, которой клиент подтверждает операцию, в холодном периоде. Если карта успешно прошла все проверки и не находится в холодном периоде, то продуктовая АС формирует электронный документ, соответствующий продуктовой операции и создаёт в учётной системе предварительную операцию. Модуль подтверждения, в свою очередь, фор-

мирует простую электронную подпись клиента и интегрирует её в электронный документ. Простая ЭП для данного сценария представляет собой совокупность следующей информации в электронном виде: фамилия, имя и отчество клиента и (или) его идентификатор в учётных системах банка; маскированный номер карты; дата и время операции; идентификатор операции; код авторизации, получаемый от процессинговой системы (по результатам проверки PIN).

Сценарий подтверждения (аутентификации) с помощью sms-кода. Ознакомиться с общей схемой сценария подтверждения с помощью sms-кода можно на рис. 7.

В офисах банка этот сценарий очень похож на сценарий подтверждения карта плюс PIN: так, например, реквизиты операции так же передаются на экран POS-терминала для ознакомления, клиент нажимает те же кнопки при принятии решения о подтверждении операции, ввод одноразового sms-кода производится так же через POS-клавиатуру. А в удалённых каналах подписание документа по клиентскому опыту унифицировано с процессами подтверждения операции разовыми sms-паролями.

Однако отличия всё же есть, и дело тут не только в замене системы аутентификации и способа взаимодействия с клиентом. В отличие от процессов подтверждения операции sms-паролем, при подписании документов отсутствует возможность «запросить sms ещё раз» при превышении количества неверных вводов. Другими словами, если при подтверждении операции в веб-версии Сбербанк Онлайн после трёх неверных попыток у клиента есть возможность ещё пару раз запросить новый пароль, и он будет действительно новым, то при подписании документа после трёх ошибок ввода sms-кода клиенту будет предложен другой способ подписания, или на документе будет проставлена отметка типа «отказ в подписании», и операция будет отменена (возвращена на доработку).

Как только продуктовая АС вызвала модуль подтверждения, она создаёт специальную техническую сессию, в рамках которой происходит дальнейшая отправка одноразовых sms-кодов. Контроль активности технической сессии позволяет защитить средства клиента от действий злоумышленника при атаке типа полного перебора sms-кода (brute force). Техническая сессия как объект содержит идентификатор, дату и время её создания, количество оставшихся попыток ввода sms-кода (максимально три попытки), время жизни sms-кода, количество sms, которые могут быть отправлены в рамках текущей технической сессии. Активность технической сессии

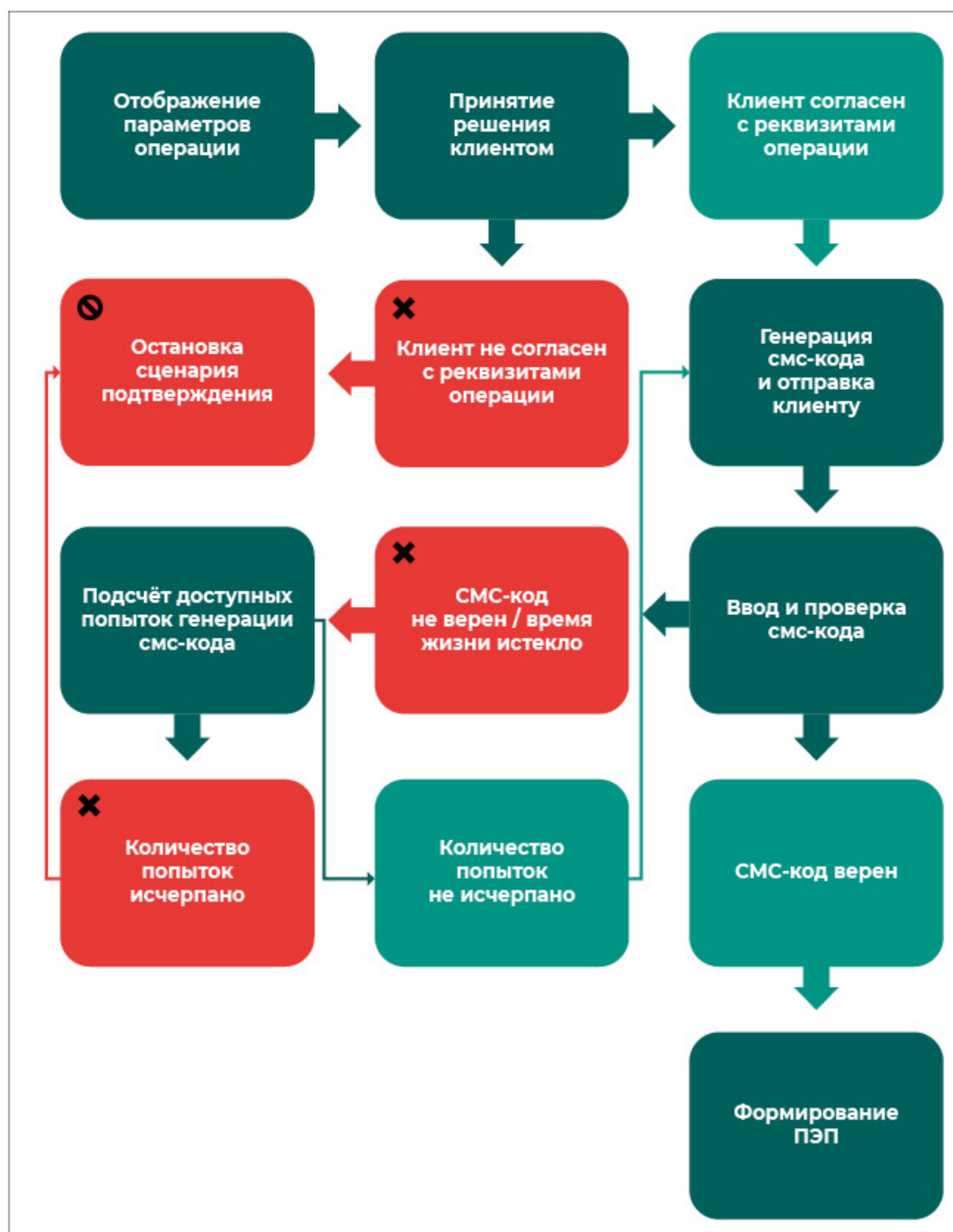


Рисунок 7. Сценарий подтверждения с помощью sms-кода

жёстко связана с сессией пользователя продуктовой АС: так, например, если сессия пользователя будет закрыта, то и техническая сессия будет принудительно разорвана.

Далее модуль подтверждения генерирует одноразовый пятизначный sms-код и вставляет его в текст сообщения, который был сгенерирован продуктовой АС. Генерация одноразового кода осуществляется с помощью модифицированного Java класса SecureRandom. Продуктовая АС осуществляет вызов модуля отправки уведомлений клиенту, который отправляет сформированное sms-сообщение клиенту через специальный шлюз доставки sms. Для обеспечения конфиденциальности передаваемого кода запросы на отправку sms-сообщений с паролями и кодами клиента всегда передаются с особым маркером типа «SecureTransfer», который сигнализирует системам банка, участвующим в отправке уведомлений клиентов, о недопустимости сохранения тела сообщения в таблицах,

Практический опыт внедрения безбумажной технологии взаимодействия с клиентом на примере Сбербанка поможет избежать основных ошибок при движении в сторону цифровой трансформации бизнеса

логах и журналах АС. А в системах защиты от НСД, наоборот, к данным запросам применяются более строгие правила контроля доступа.

После отправки кода в канал уведомления фронтальная АС ждёт ввода данного кода от клиента и осуществляет вызов модуля подтверждения для сравнения отправленного и введенного кода. Для этого на вход модуля подтверждения от продуктовой АС передаются параметры: идентификатор пользовательской сессии, идентификатор технической сессии и смс-код. Модуль подтверждения осуществляет сравнение смс-кода и возвращает ответ в продуктовую АС. Если смс-код совпадает, то продуктовая АС формирует электронный документ, соответствующий продуктовой операции, и создаёт в учётной системе предварительную операцию. Модуль подтверждения формирует простую электронную подпись клиента и интегрирует её в электронный документ. Простая ЭП для данного сценария представляет собой совокупность следующей информации в электронном виде: фамилия, имя и отчество клиента и (или) его идентификатор в учётных системах банка; номер мобильного телефона клиента; дата и время операции; идентификатор операции; код авторизации, получаемый от системы аутентификации (по результатам проверки смс-кода). Если смс-код не совпал, то простая ЭП клиента не формируется и, согласно установленным счётчикам, осуществляется повторный запрос ввода смс-кода.

ОПЕРАЦИЯ ПОДТВЕРЖДЕНА КЛИЕНТОМ. ЧТО ДАЛЬШЕ?

После успешного исполнения сценария подтверждения клиентом по карте плюс PIN или смс производится вывод электронного документа с блоком данных, составляющих простую ЭП клиента на экран устройства отображения второму подписанту — сотруднику банка. После ознакомления с текстом документа сотрудник прикладывает свой ТМ-носитель с секретным ключом к специальному считывателю. Осущест-

вляется программный вызов компонента для получения идентификатора ТМ-носителя с целью дальнейшего определения логина сотрудника и сбора детальной информации о нём в учётной АС банка. На основании полученной информации от учётной АС модуль подтверждения осуществляет следующие проверки: соответствие полученного логина сотрудника, выполняющего данную операцию, логину с ТМ-носителя с целью исключения нелегитимного использования чужого ТМ-носителя; наличие полномочий у сотрудника для подписи документов данного типа с целью исключения нарушения принципа минимальности полномочий; соответствие офиса обслуживания сотрудника офису, в котором выполняется операция, и наличие этого сотрудника в смене офиса с целью исключения несанкционированного подтверждения операции. Если все проверки прошли успешно, то документ с внедрённой простой ЭП клиента подписывается усиленной ЭП сотрудника. Полученная в результате криптографического преобразования кодированная подпись интегрируется в электронный документ. Результат формирования усиленной ЭП отображается сотруднику и передаётся в журнал аудита.

Сформированные в электронном виде документы по окончании операционного дня передаются из учётной АС в электронный архив.

В дальнейшем перед каждой операцией печати электронного документа и/или его отправки по e-mail клиента производится проверка истинности усиленной ЭП сотрудника с помощью библиотеки СКЗИ. Тем самым гарантируется, что клиент получит не модифицированный документ.

* * *

Описанный выше практический опыт внедрения безбумажной технологии взаимодействия с клиентом на примере Сбербанка поможет избежать основных ошибок при движении в сторону цифровой трансформации бизнеса. Масштабный переход традиционного бумажного документооборота в цифровую плоскость неизбежен, так как позволяет избежать значительных материальных затрат на этапе как формирования, так и хранения электронных документов, а трудозатраты по их обработке, верификации и транспортировке сводятся практически к нулю. Самое главное при выборе безбумажной технологии (разумеется, после экономического эффекта) — не забывать о вопросах соблюдения требований регуляторов и обеспечения кибербезопасности.



Антон ТИХОНОВ
технический менеджер
направления McAfee, ГК MONT

*Самое трудное в споре —
не столько защищать свою
точку зрения, сколько иметь
о ней четкое представление.*
Андре Моруа

ЗАЩИЩАЯ «НЕИСПОЛЬЗУЕМОЕ» ОБЛАКО

ОТ ДОМОХОЗЯЙКИ ДО КОСМИЧЕСКОГО БИОЛОГА

«Кто из вас использует облака?» — задал свой первый вопрос Ehab Ezzaldeen, Channel Technical Manager, Middle East & Turkey McAfee, в рамках сессии, посвященной организации безопасности облачных инфраструктур на McAfee Partner Technical Forum 2019. Примерно половина зала подняла руки. Однако Эхав на этом не остановился и задал второй вопрос: «У кого из вас с собой мобильный телефон?» Получив в ответ «лес рук», он сказал: «Я задал этот вопрос, чтобы показать вам, что вы все используете «облака» — на ваших устройствах».

Это небольшое вступление заставило меня задуматься над тем, насколько мы привыкли к возможности использования ресурсов, находящихся за пределами нашей зоны контроля, которые позволяют нам сохранить «чуть» больше фотографий и видеозаписей, чем доступно на наших устройствах. И этот факт уже давно не является чем-то из ряда вон выходящим, как для меня, так и для всех остальных, от домохозяйки до космического биолога.

ВСЕ СТРЕМЯТСЯ В ОБЛАКА

В коммерческой среде вопросы, решаемые специалистами, довольно типичны: «Как нам быстрее выводить инновационные технологии на рынок?», «Как получить инфраструктуру, но тра-

тить на неё деньги только тогда, когда она нам действительно нужна?» И фактически они подводят к тому, что использование ресурсов и инфраструктур, принадлежащих кому-то ещё, а не нам, является логичным ответом на них. Вернувшись к истокам и определению «облачных вычислений», как модели обеспечения удобного сетевого доступа по требованию к некоторому общему фонду конфигурируемых вычислительных ресурсов, которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру (Wiki), становится очевидно, что использование «облачных вычислений» — если не свершившаяся и абсолютная реальность, то, как минимум, цель, к которой стремится абсолютно каждый игрок на рынке (Рис. 1).

ВИДЫ ОБЛАКОВ

При этом совершенно очевидно, что значительная часть компаний не готова сразу перейти к полностью облачным архитектурам. Из-за этого возникают различные варианты принятия облачных архитектур, с общей классификацией которых нам снова поможет Wiki:

♦ **Частное облако** (англ. *private cloud*) — инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации), возможно также клиентами и подрядчиками данной организации. Частное облако может находиться в собственности, управлении и эксплуатации, как самой организации, так и третьей стороны (или какой-либо их комбинации), и оно может физиче-

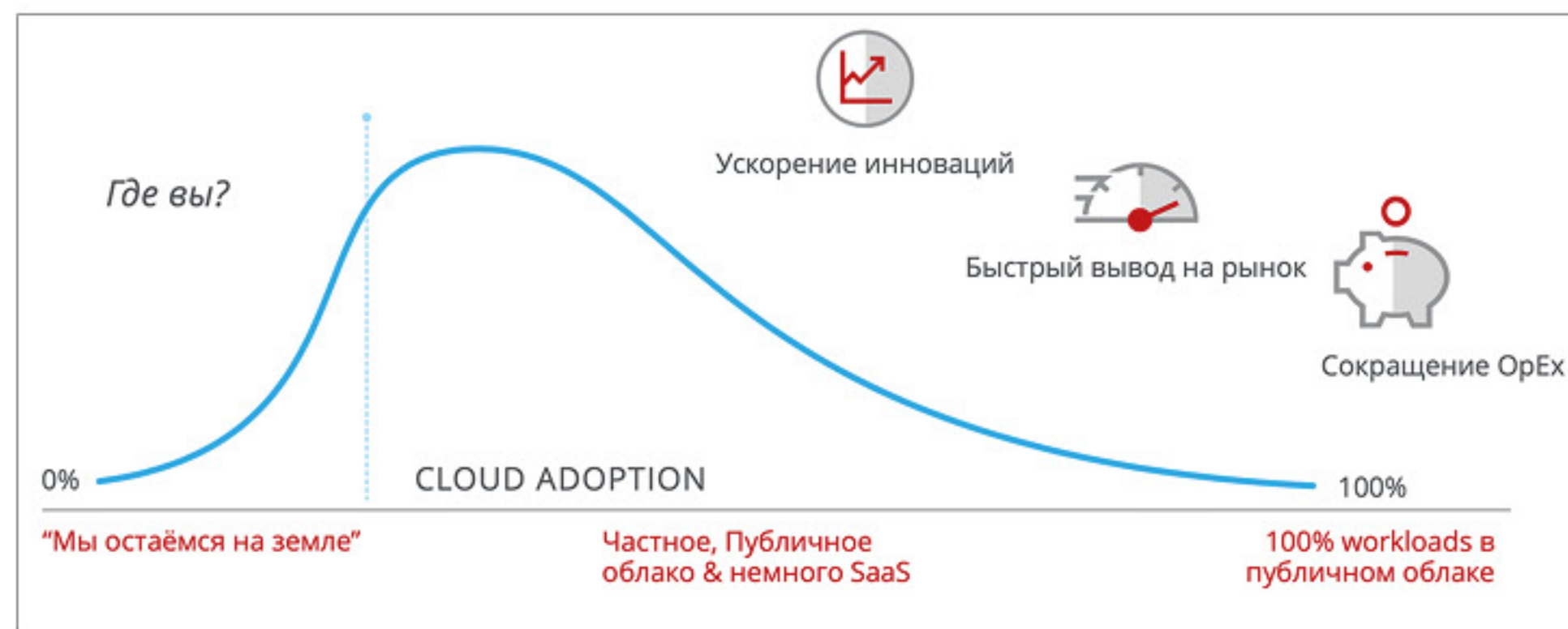


Рисунок 1. Тенденция движения компаний в «облако» по данным McAfee. Степень и скорость принятия «облачных вычислений» зависит от типа заказчика и его потребностей

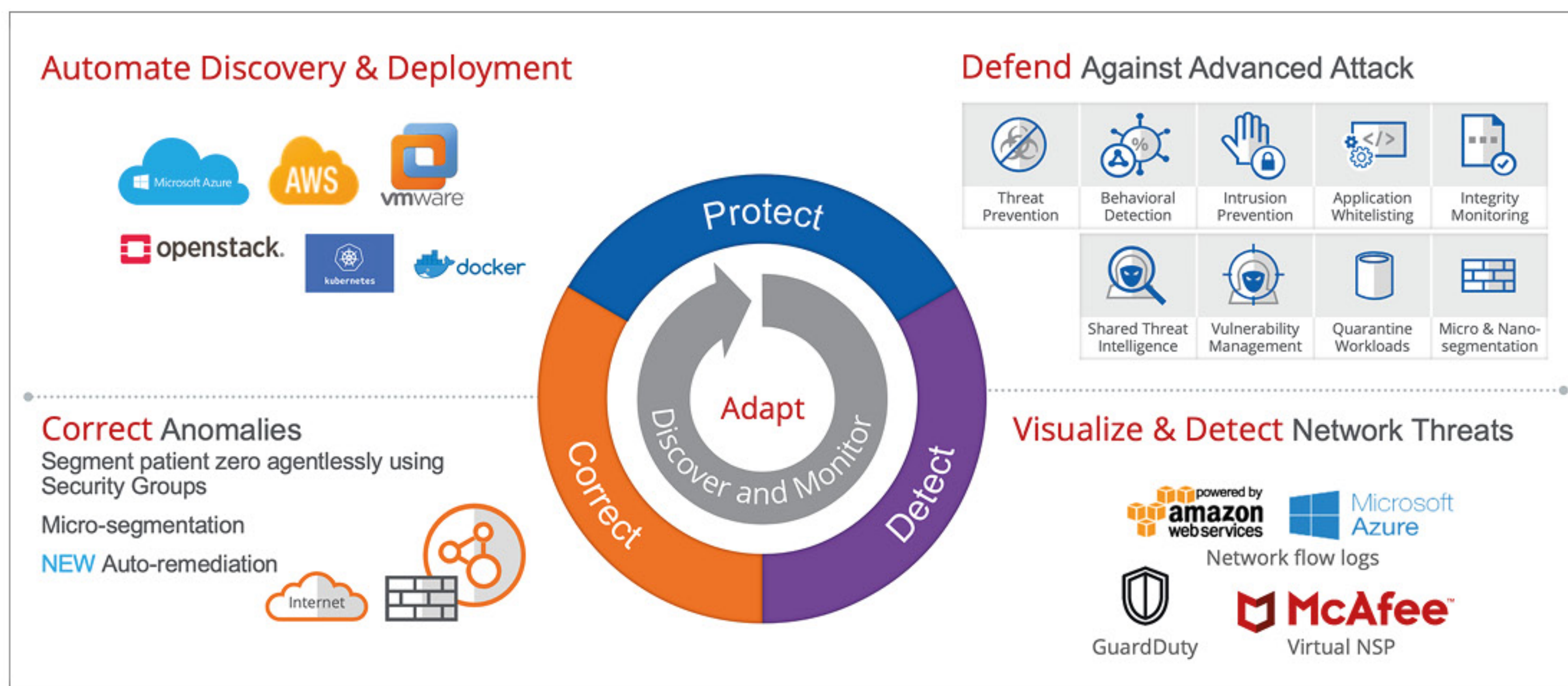


Рисунок 2. Цикл обработки угроз при использовании решения McAfee Cloud Workload Security

ски существовать как внутри, так и вне юрисдикции владельца.

♦ **Публичное облако** (англ. *public cloud*) — инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации). Публичное облако физически существует в юрисдикции владельца — поставщика услуг.

♦ **Общественное облако** (англ. *community cloud*) — вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи (например, миссии, требований безопасности, политики, и соответствия различным требованиям). Общественное облако может находиться в кооперативной (совместной) собственности, управлении и эксплуатации одной или более из организаций сообщества или третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

♦ **Гибридное облако** (англ. *hybrid cloud*) — это комбинация из двух или более различных облачных инфраструктур (частных, публичных или общественных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями пере-

дачи данных и приложений (например, кратковременное использование ресурсов публичных облаков для балансировки нагрузки между облаками).

НЕМНОГО «ПРОФЕССИОНАЛЬНОЙ ПАРАНОЙИ»

Сегодня чаще всего встречается вариант с использованием наиболее «безопасного» варианта — «частного облака». И чаще всего их владельцы могут предположить, что будет достаточно защиты трафика от устройства до «облака», т.н. South-North трафик. Но если мы добавим немного «профессиональной паранойи», сразу возникает много вопросов: всегда ли мы знаем, что происходит внутри нашего облака? Сколько workloads (они же виртуальные машины) у нас было вчера, есть сейчас и будет завтра? Применяются ли к ним политики безопасности, обновлены ли антивирусные базы? Есть ли у нас инструменты, позволяющие увидеть «east-west» трафик, т.е. тот, который движется горизонтально между узлами в самом облаке? Знаем ли мы, как и чем обмениваются узлы в облаке, если это не проходило через защищенный периметр и наш безопасный VPN туннель?

РЕШЕНИЕ ЕСТЬ!

Ответить на все эти вопросы позволяет решение McAfee Cloud Workload Security, включающее в себя инструмен-

ты для работы как с частными, так и с публичными облачными окружениями типа IaaS\PaaS (Рис. 2).

Основной подход данного решения состоит в объединении основных возможностей продуктов ИБ в части Защиты, Обнаружения и Устранения в режиме реального времени, управлении стекком продуктов через единый стандартизованный интерфейс, предоставляющий адаптивную обратную связь, посредством чего общая система безопасности обучается и развивается, со временем становясь только крепче. Решение использует и реализует в работе все фазы цикла защиты от угроз (Threat Defense Lifecycle). Принятие данного цикла позволяет организациям эффективно блокировать угрозы, обнаруживать подозрительные активности и применять быстрые ответные реакции наряду с расширением арсенала мер противодействия.

♦ **Защита** — комплекс профилактических техник, позволяющих остановить наиболее распространенные виды атак, а также противостоящих 0-day техникам проведения атак и полезным нагрузкам.

♦ **Обнаружение** — продвинутые инструменты мониторинга выявляют аномалии и нестандартное поведение для определения low-threshold attacks и поведения, которые остались бы незамеченными.

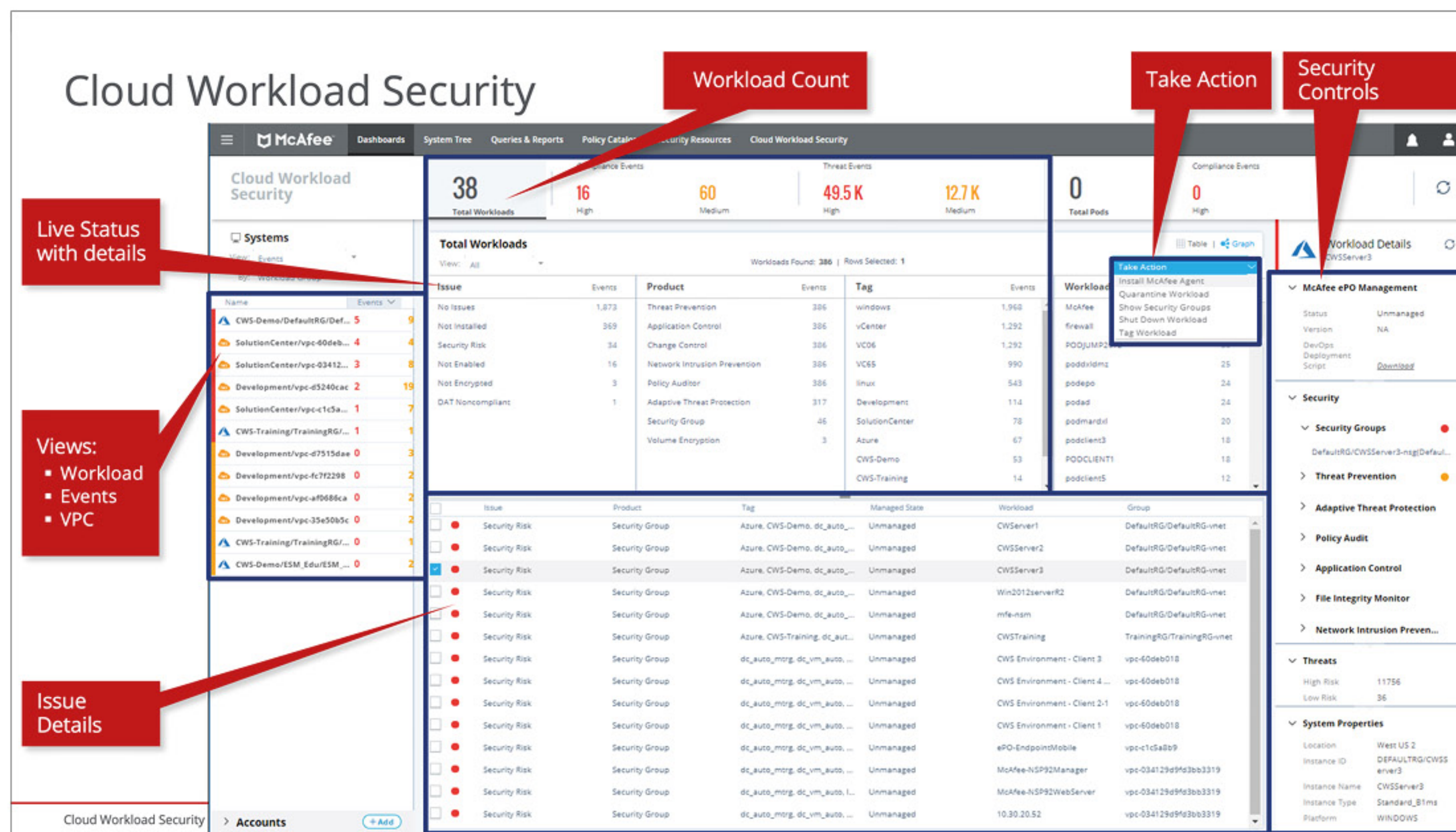


Рисунок 3. Интерфейс CWS

♦ Устранение — упрощённый подход к сортировке и обработке событий, позволяет корректно расставлять приоритеты и проводить непрерывные расследования.

♦ Адаптация — мгновенное применение информации об угрозах из общего адаптивной инфраструктуры.

ВОЗМОЖНОСТИ

Возможности решения McAfee Cloud Workload Security:

♦ Обнаружение и визуализация активности и движения Workload (VM), контейнеров и сетевого трафика.

♦ Мгновенное обнаружение всех ресурсов окружений IaaS. Быстрое обнаружение, оценка и устранение угроз.

♦ Визуализация всего ИТ-окружения вне зависимости от расположения. Контролируйте вертикальное (North-South) и горизонтальное (East-West) распространение нежелательного трафика.

♦ Защита ИТ от «устройства-до-облака» всеобъемлющим решением. Крепкая защита от продвинутых атак.

♦ Упрощённое внедрение и управление в гибридных окружениях. Централизованное, автоматизированное управление политиками публичных, частных и гибридных облаков.

На рисунке 3 приведён пользовательский интерфейс CWS и отображено перетекание информации между секциями экрана управления, позволяющее расширить зону видимости и контроля для корректного применения соответствующих реакций.

ЗАВТРА НАЧИНАЕТСЯ СЕГОДНЯ

Принимая во внимание ту сложность и комплексность современных гибридных окружений, трудно переоценить функциональные наборы, предлагаемые McAfee. Они однозначно стоят того, чтобы рассмотреть возможность их применения, ведь довольно скоро они наверняка вам потребуются для организации адаптивной системы безопасности во всех окружениях, которые вы используете сейчас и будете использовать завтра (Рис. 4).

Features	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
Centralized Management (McAfee ePO™ Platform)	✓	✓	✓
Role-based access controls allow multiple permissions in McAfee ePO	✓	✓	✓
Multiple Cloud Support (AWS, Azure, VMware)	✓	✓	✓
Use Micro-segmentation to Quarantine Workloads and Containers	✓	✓	✓
Threat Prevention: ENS for Servers OS (Windows and Linux)	✓	✓	✓
Host Intrusion and Exploit Prevention	✓	✓	✓
Cloud Encryption Management	✓	✓	✓
Native Firewall Management for AWS and Azure (Security Groups)	✓	✓	✓
McAfee Management for Optimized Virtual Environments (Agentless and Multiplatform)	✓	✓	✓
Host-based Firewall	✓	✓	✓
Import AWS and Azure tag information into McAfee ePO	✓	✓	✓
Auto-remediation to automatically quarantine workloads without security policies	✓	✓	✓
Adaptive Threat Protection with Behavioral Analysis	✓	✓	✓
Native Network Traffic Analysis for AWS and Azure	✓	✓	✓
Network Traffic Visualization	✓	✓	✓
McAfee Virtual Network Security Platform Integration	✓	✓	✓
Application Control for Servers	✓	✓	✓
File Integrity Monitoring	✓	✓	✓
Change Control for Servers	✓	✓	✓

Рисунок 4. Доступные функциональные наборы для защиты гибридной инфраструктуры



Андрей ПЕРКУНОВ
директор департамента
сетевой инфраструктуры СТИ

СТИ СОЗДАЕТ ЗАЩИТУ,

АДАПТИВНУЮ К ЛЮБЫМ УГРОЗАМ
И ДИНАМИЧНЫМ ИЗМЕНЕНИЯМ СРЕДЫ

ТРИ ВЕКТОРА

— Атаки хакеров по-прежнему направлены на крупные компании, промышленные объекты и критические инфраструктуры. Вывод денежных средств, вымогатели, скрытый майнинг, кража данных для перепродажи, промышленный шпионаж. Про всё это мы читаем в новостях. А какие новые технологии в сфере ИБ появились, чтобы противостоять всем этим угрозам? Как правильно выстроить защиту?

— В первую очередь нужно отталкиваться от типа компании и сферы её деятельности, чтобы использовать те инструменты информационной безопасности, которые направлены на киберустойчивость. Сейчас это понятие в ИБ расширилось, как и технологии, которые должны применяться для её обеспечения — это и облачная аналитика, и машинное обучение, и репутационные сервисы.

С точки зрения развития технологий, я бы выделил три основных вектора. Первый направлен на развитие технологий кибербезопасности, связанных с защитой технологических систем и сетей, и тематики Интернета вещей, а также раннего обнаружения факта компрометации ИТ-инфраструктуры (решения класса Detection). Второй вектор технологий, который актуален для коммерческих компаний, планирующих размещать свои ресурсы в публичных облачных инфраструктурах, это брокеры безопасного доступа к облачным данным (Cloud Access Security Bro-

kers), которые позволяют обеспечить контроль данных и приложений при использовании публичных облаков. Дополнительно это могут быть технологии защиты, которые предоставляются из облака, связанные с машинным обучением, искусственным интеллектом, индикаторами компрометаций и т.д.

И третий вектор развития, приобретающий всё большую актуальность, в т.ч. для государственных компаний, это Security Operation Centers и Security Awareness. Эти технологические решения позволяют построить не только полноценную систему реагирования на угрозы, но и выстроить процессы проактивной защиты бизнеса от угроз.

Задачей бизнеса является достижение такого состояния системы ИБ, которое будет адаптивно к любым возникающим угрозам и динамичному окружению. Подобная концепция абсолютно реальна. Это подтверждается опытом СТИ по созданию таких систем.

ПРО ИНТЕГРАЦИЮ

— Как на фоне глобальной цифровизации и повсеместном внедрении систем автоматизации компания может успеть всё это защитить и не подвергаться рискам утечек через новые каналы и системы?

— Сегодня перед большим количеством компаний встают задачи по консолидации, трансформации вычислительной инфраструктуры и переходу к программно-определяемым центрам обработки данных (SDDC). В России компании только сейчас начинают пе-

реход к гиперконвергентным решениям и технологиям контейнеризации. В условиях эволюции киберугроз интеграция передовых средств безопасности открывает дополнительные возможности координации и повышает их эффективность. В таких динамичных вычислительных и сетевых средах решения по кибербезопасности должны быть тесно связаны с сетевыми сервисами и ИТ-инфраструктурой для защиты критических и перемещающихся ресурсов и данных, оркестрации политик безопасности и предоставления сервисов защиты от целенаправленных атак.

В лаборатории безопасности СТИ мы демонстрируем заказчикам решения по защите, интегрированные в современную виртуализованную инфраструктуру и программно-определяемые сети на основе таких технологических стеков, как VmWare NSX, Cisco ACI, Microsoft Azure и др. Такая архитектура обеспечивает видимость и безопасность в контексте overlay/underlay сетей программно-определяемых сред, снижение затрат на построение безопасности с обеспечением защиты приложений и данных на 4–7 уровне, повышение эффективности и упрощение в настройке политик и микросегментации.

Специалистов по информационной безопасности не хватает, существует разрыв с точки зрения квалификации специалистов ИБ в отношении новых технологий, поэтому растёт популярность профессиональных интеграторов, компаний, которые более динамичны и умеют решать сложные и нестан-

дартные задачи. Также один из трендов ИТ-отрасли — это переход на аутсорсинг. СТИ не исключение, у нас есть ряд крупных заказчиков, как в медицине, так и в промышленности, которым мы предоставляем защищённые сервисы в облаке, снимая задачи защиты с персонала заказчика.

В частности, одному из клиентов СТИ оказывает услугу предоставления защищённых каналов связи с мониторингом и обеспечение соответствия этой услуги требованиям защиты персональных данных по модели MDR (Managed Detection and Response).

РЫНОК SOC

— На российском рынке про SOC сейчас не говорит только ленивый. Для заказчиков это возможность качественно повысить общий уровень информационной безопасности компании и построить комплексную эшелонированную защиту. Всё больше участников рынка отдают свои предпочтения сервисной модели подключения к центрам мониторинга и обработки событий ИБ или сделают это в ближайшие два года. Как вы видите развитие рынка SOC?

— Рынок SOC развивается не так быстро как хотелось бы, основным сдерживающим фактором для построения SOC внутри заказчика до сих пор остаётся стоимость, потому что для реализации полноценной системы требуется не только приобретение специализированных средств мониторинга и реагирования инцидентов, но и своя команда аналитиков, что для небольших и средних компаний недостижимо с точки зрения бюджета.

Поэтому основной тренд — это разделение центров реагирования на корпоративные и на SOC из облака. Крупные компании имеют проекты построения собственных SOC и выстраивания процессов внутри себя, но средние и малые компании тяготеют к использованию SOC как сервиса — подключению уже к готовому центру и передачи в него событий информационной безопасности из своей инфраструктуры, чтобы профессиональная команда обеспечивала мониторинг реагирования на инциденты. Рынок для малых и средних компаний развивается, заказчики всё больше

доверяют профессиональным интеграторам. Следующим шагом заказчиков будет переход от классической модели SOC на модель MDR, что позволит им более эффективно обеспечивать защиту бизнеса от угроз.

ТРИ МОДЕЛИ АУТСОРСИНГА

— Какое положение на рынке сейчас занимает аутсорсинг в сфере ИБ? Он применим ко всем сферам или имеет ограничения?

— Если рассматривать аутсорсинг в консалтинге ИБ, то он уже более 10 лет существует на рынке, уже тогда сформировался профессиональный консалтинговый рынок для предоставления услуг по аудиту, приведению к соответствию требованиям, аттестациям и т.д.

Другая часть аутсорсинга связана с аутстаффингом, предоставлением персонала в службу безопасности для выполнения определённых задач. Этот сегмент рынка не сильно развит, но растёт по причинам, озвученным выше — в отрасли есть дефицит профессиональных кадров, и многие заказчики используют аутстаффинг для закрытия своих временных проектных задач, либо на момент расследования инцидентов.

И третья модель, связанная с аутсорсингом, это то, что связано с сервисной моделью, когда кибербезопасность предоставляется из облака, либо инфраструктура заказчика переносится в облако, и вместе с ней ответственность за обеспечение ИБ переходит сторонним людям. Используя эту модель, необходимо обязательно прописывать время реагирования на инциденты и время их устранения, штрафные санкции при нарушении и много других параметров. Для ряда государственных или промышленных компаний такой подход к аутсорсингу может быть ограниченным или неприменимым по причинам имеющихся пробелов в нормативном регулировании сферы защиты информации.

ЧТО ПРЕДЛАГАЕТ СТИ

— СТИ предлагает управляемые услуги по информационной безопасности? В чём ценность для клиентов и считаете ли Вы что за MSSP будущее?

— Все эксперты сходятся во мнении, что потребности бизнеса в переходе от традиционной модели ИТ-инфра-

структуры к облачным сервисам влечёт за собой дополнительные риски и уязвимости, но использование облачных сервисов неуклонно растёт. Это рождает две проблемы: размывание периметра (доступ к облачной инфраструктуре возможен с любого устройства за пределами корпоративной сети) и неконтролируемое перемещение данных и информации. На сегодняшний день в мире уже 25 % корпоративного трафика обходит периметровые средства защиты, и эта цифра экспоненциально растёт.

Для решения задач защиты информации при переходе ИТ к сервисной и облачной модели СТИ предлагает набор услуг, предоставляемых по сервисной модели и предназначенных для защиты облачных данных. Мы помогаем заказчикам сразу начать использование современных решений для защиты, обеспечивая соответствие требованиям по защите персональных данных в сочетании с проактивным мониторингом сложных и распределённых информационных систем, а также оперативно реагировать на угрозы и быстрое изменение политик безопасности для превентивной защиты в случае наступления инцидента. Оповещение экспертов СТИ и/или сотрудников клиента о произошедших событиях ИБ происходит в автоматическом режиме и доступно в разных каналах. В зависимости от корпоративных политик и технических возможностей заказчика мы предлагаем различные схемы развёртывания услуг, например, полностью в облаке или гибридная.

Перед внедрением услуг мы предлагаем проведение СТИ Security Cloud Assessment, которая учитывает все аспекты безопасности при использовании облачных технологий.

Основная ценность для наших заказчиков в том, что внедрение данных услуг позволяет значительно снизить риски ИБ и кражи данных, уменьшить эксплуатационные затраты на администрирование и внедрение средств защиты, обеспечить полную видимость и безопасность данных, упростить изменение политик безопасности и повысить скорость реагирования и принятие решений.



Иван ЛОПАТИН
технический эксперт
АО «ДиалогНаука»

НА НОВОМ УРОВНЕ

ТЕХНИЧЕСКИЕ ТРУДНОСТИ РЕАЛИЗАЦИИ МОДЕЛИ СЕРВИС-ПРОВАЙДЕРА УСЛУГ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (MSSP) И ПУТИ ИХ РЕШЕНИЯ

В этой статье мы постараемся приоткрыть занавес технических проблем со стороны SIEM-систем и их компонентов, с которыми сталкиваются организации при переходе на следующий уровень развития собственного ситуационного центра (SOC) в модели сервис-провайдера услуг по информационной безопасности (MSSP, Managed Security Service Provider).

Реалии развития современных SIEM-архитектур подталкивают крупные государственные и частные компании в сторону централизации сбора событий информационной безопасности и дальнейшего расследования инцидентов в головном подразделении, где есть высококвалифицированные кадры для расследования сложных таргетированных атак.

С целью коммерциализации своей деятельности и получения дополнительной финансовой прибыли ряд компаний переводят свои ситуационные центры в модель оказания услуг информационной безопасности SaaS (Security as a Service), выступая в роли MSSP-провайдеров. При этом на первом этапе компании, как правило, начинают предоставлять услуги только для собственных дочерних предприятий, а затем уже выходят на рынок предоставления услуг для сторонних организаций.

БАЗОВЫЕ РЕКОМЕНДАЦИИ

Чтобы начать процесс построения MSSP модели, необходимо убедиться в наличии:

- ♦ квалифицированных кадров;
- ♦ документальной базы (политики ИБ, регламенты, инструкции и т.д.);
- ♦ выстроенных процессов выявления и реагирования на инциденты;
- ♦ эффективно работающей SIEM-системы;
- ♦ проверенного контента в SIEM-системе для выявления инцидентов ИБ (правила, фильтры, отчёты, дашборды и др.);
- ♦ компонентов и дополнительных программных комплексов для реализации SOC;
- ♦ шины данных и специализированных программных средств для работы клиентов MSSP.

Если Вы приняли решение начать предоставлять MSSP-услуги другим лицам и компаниям на базе вашего SOC, то мы рекомендуем учитывать следующее:

1. Масштабируемость SIEM-систем зачастую является проблемой, когда необходимо подключить несколько заказчиков и правильно распределить потоки поступающей информации.
2. Чёткое проектирование каналов связи и «кратчайших путей» до вашей входной точки в SOC будет немаловажным подспорьем при реализации MSSP модели.

3. Изучение специфики и особенностей каждого подключающегося заказчика к вашей услуге является отправной точкой к фильтрации бескрайнего количества событий, которые будут поступать к Вам. В противном случае SOC просто «захлебнётся» и не сможет обрабатывать поступающие события.

4. Организация работы первой линии уже не будет выглядеть настолько просто, что можно брать на неё студентов и людей с низкой компетенцией.

5. Каждый монитор первой линии в вашем SOC больше не может показывать «возможно-нужную» информацию — необходимость в оперативном мониторинге и качество визуализации метрик SOC будет стоять на первом месте.

6. Существующий контент в SIEM системе должен в автоматическом режиме перестраиваться под каждого заказчика и добавлять оперативную информацию в события каждого клиента.

7. Предоставление отчётности и визуализации каждому клиенту является неотъемлемой частью оказания услуги MSSP.

8. Необходимо предусмотреть механизм добавления или изменения подключённых услуг клиенту MSSP.

9. Необходимо продумать механизмы оповещения о выявленных инцидентах ИБ в ночное и нерабочее время, так как привлечение сотрудников разных подразделений (ИТ, ИБ, Network,

Руководителей проектов и др.) — задача, требующая отдельной проработки. Для организации оповещений зачастую используются механизмы интеграции со Skype, Telegram bot и другие.

10. Ведение услуг MSSP предполагает наличие руководителей проекта для клиента и заказчика, так как интеграционные работы зачастую схожи по уровню сложности с работами по внедрению компонентов SIEM.

Далее рассмотрим более подробно некоторые аспекты построения модели MSSP.

SIEM КАК УСЛУГА MSSP

На сегодняшний день большое количество владельцев SOC уверены, что они готовы принимать «на борт» нагрузку потенциальных клиентов без каких-либо трудностей. Однако их мечты в большинстве случаев обречены разбиться о входной EPS (объем событий поступающих в секунду), отсюда вытекает следующее:

Проблема MSSP № 1. Клиент зачастую сам не знает, что нужно собирать и обрабатывать.

Правило MSSP № 1. Собирать и обрабатывать следует только те события, под которые у вас есть необходимый контент в SIEM-системе.

Ваша SIEM должна быть готова обрабатывать в режиме реального времени такой объем поступающих событий, который будет достаточным и необходимым для покрытия всех пиковых значений Ваших заказчиков и клиентов.

Основным инструментом для выявления инцидентов ИБ является Ваш контент в SIEM (правила, фильтры, отчеты, дашборды и другое). Такой контент должен удовлетворять следующим требованиям:

- ♦ создан по мировым практикам реализации MSSP моделей;
- ♦ прост и удобен в эксплуатации — в случае необходимости должен быть изменен любым членом команды SOC, ответственным за контент;
- ♦ классифицирован — классификация событий и инцидентов ИБ необходима для реализации модели выявления инцидентов и их визуализация для каждого заказчика;
- ♦ оптимизирован — быстродействие работы всех компонентов SIEM-сис-

темы — это залог быстрой обработки поступающих событий. Также немаловажную роль играет отсутствие неиспользуемых ресурсов и\или ресурсов тестового назначения в продуктивной среде;

♦ разграничительным, — обладающим функциями работы для любого из заказчиков без дополнительной настройки;

♦ масштабируемый — контент должен легко масштабироваться для легкого перехода на следующий уровень развития SOC — MSSP.

На сегодняшний день на российском рынке есть несколько предложений по готовому контенту для SIEM-систем. Так, например, компания «ДиалогНаука» предлагает самодостаточный SOC-пакет правил корреляции собственной разработки, который в том числе может использоваться для реализации MSSP-модели.

МАНИПУЛЯЦИЯ УСЛУГАМИ MSSP

Необходимо понимать, что предоставляемый сервис MSSP — это возможность заказчика выбирать те услуги и компоненты, в которых у него есть потребность в данный момент, а также возможность отключать услуги в случае их неактуальности (DDoS, вирусная эпидемия).

Разработка механизма выбора услуги и её автоматической активации в случае необходимости является основной задачей разработки архитектуры, так как ручное управление клиентскими услугами уже уходит в прошлое. В данный момент аналогичные механизмы широко применяются при разворачивании виртуальных серверов и сервисов через личный кабинет облачных провайдеров. Отсюда возникает следующая проблема.

Проблема MSSP № 2. Для предоставления услуг должного уровня количество разрабатываемых и необходимых к оптимизации сервисов для MSSP возрастает в несколько раз.

Правило MSSP № 2. Использование решений с открытым исходным кодом (Open Source) в MSSP не всегда плохо, а зачастую просто необходимо (например, TheHive, Elastic Stack, Metron, Hadoop).

ОТЧЁТНОСТЬ И ВИЗУАЛИЗАЦИЯ

Необходимо понимать, что под услугой MSSP понимается весь спектр сопутствующих задач, которые клиент хочет получить от сервис-провайдера, включая визуализацию, расчёт метрик KPI, получение отчётности и оперативное оповещение об инцидентах высокой критичности.

В случае MDR-архитектуры дополнительно потребуется предоставление информации об этапности реализации атаки (kill chain), классификации угрозы и возможных объектов, находящихся в зоне риска. Отсюда можно сделать следующий вывод:

Проблема MSSP № 3. Качественная визуализация — отдельный программный комплекс, входящий в состав SOC и требующий компетентных специалистов.

Правило MSSP № 3. Отчётность и визуализация — главный инструмент для анализа эффективности работы сервиса MSSP для клиента.

Визуализация должна быть для каждого клиента индивидуальной, как и KPI. Основной проблемой будет являться быстрое разграничение доступов к ресурсам SIEM и шине данных для визуализации и отчётности без изменения большого количества правил, фильтров и других ресурсов.

Примером отчётности могут послужить уведомления об инциденте ИБ в Telegram или другой корпоративный мессенджер. Основная идея заключается в том, что при наступлении инцидента ИБ корреляционное правило запускает скрипт, который добавляет в клиентский telegram-канал всю необходимую информацию.

* * *

Мы постарались изложить свой взгляд на те проблемы, с которыми может столкнуться компания на пути трансформации в сервис-провайдера услуг по информационной безопасности. Мы искренне надеемся, что наши рекомендации позволят избежать целого ряда проблем и дадут возможность быстрее и эффективнее предоставлять услуги в рамках модели MSSP и в последующем MDR.



Алексей СИДОРОВ
генеральный директор
ООО «Пангео Радар»



Сергей РУБЛЕВ
директор по развитию
ООО «Пангео Радар»

ПЛАТФОРМА РАДАР

МЫ ГОТОВЫ ПРЕДЛОЖИТЬ ДОСТОЙНУЮ ЗАМЕНУ
ЗАРУБЕЖНЫМ SIEM-СИСТЕМАМ, УХОДЯЩИМ
С РОССИЙСКОГО РЫНКА

Генеральный директор ООО «Пангео Радар» Алексей Сидоров и директор по развитию ООО «Пангео Радар» Сергей Рублев — о функциональных и интеллектуальных возможностях Платформы Радар, разработанной для автоматизации работы центров кибербезопасности.

— Расскажите, пожалуйста, немного о вашей компании — об истории её создания и ключевых решениях.

А. Сидоров: Пангео Радар — молодая компания, созданная всего год назад специально для того, чтобы продвигать на российском рынке новый программный продукт — интересный инструмент для автоматизации работы центров кибербезопасности. Речь идёт о Платформе Радар, которую мы считаем весьма перспективной, и, как показывают наши переговоры с заказчиками, включая российские банки и финансовые компании, очень востребованной. Компании финансовой сферы давно являются целью номер один для хакеров, многие уже столкнулись с целенаправленными атаками на свою информационную инфраструктуру и,

по мнению многих аналитиков, оказались не готовы к эффективному противодействию атакующим.

— И поэтому банки и финкомпании уделяют наибольшее внимание своей киберзащите, не так ли?

А. Сидоров: Да. Плюс к этому мотивирующее воздействие на них оказывает ужесточение законодательства, в первую очередь, принятие 187-ФЗ о критической информационной инфраструктуре и ряда подзаконных актов. В этих условиях банки активно создают собственные центры кибербезопасности и, естественно, ищут оптимальные решения для автоматизации их работы.

— Почему вы считаете решение Платформа Радар оптимальным, в чём вы видите его конкурентные преимущества перед аналогичными решениями других вендоров?

С. Рублев: Наиболее близким к нашему решению являются SIEM-системы, но Платформа Радар функционально шире, поскольку реализует не только характерные для SIEM функции обработки событий кибербезопасности, но и

ряд аналитических средств для расследования инцидентов. Большим преимуществом системы является то, что она «заточена» как на работу у отдельных заказчиков, так и на развёртывание у сервис-провайдера, оказывающего услуги мониторинга информационной безопасности. И, что тоже немаловажно, Платформа Радар является масштабируемой — она может эффективно работать и в инфраструктуре небольшой организации, и в условиях большой корпорации со сложной географически распределённой структурой.

А. Сидоров: Я хотел бы отметить ещё один принципиальный момент: «Платформа Радар» наследует многолетний опыт европейских специалистов в сфере кибербезопасности, и при этом является отечественным программным продуктом. Хорошо известно, что в последние несколько лет у нас в стране последовательно проводится политика импортозамещения в ИТ-сфере, банки и компании всё чаще отдают предпочтение разработкам национальных производителей. Не только потому, что таково пожелание государства, но и в связи с тем, что использование иностранных решений с недоступными исходными кодами действительно чревато рисками, особенно в сфере кибербезопасности. «Платформа Радар», повторюсь, полностью российский продукт — включена в реестр отечественного ПО Минкомсвязи, развивается и поддерживается российскими

Большим преимуществом системы является то, что она «заточена» как на работу у отдельных заказчиков, так и на развёртывание у сервис-провайдера

программистами. При этом по качеству оказываемых сервисов и по функционалу она ничем не уступает своим зарубежным аналогам, опережая их по некоторым параметрам. Сегодня мы готовы предложить достойную замену зарубежным SIEM-системам, уходящим с российского рынка. Не будем называть их, они хорошо известны специалистам.

— **Расскажите подробнее об аналитических возможностях системы, это действительно то, что ценят все заказчики.**

С. Рублев: Есть специальный интерфейс, в котором можно проводить исследование инцидентов — создаётся специальная аналитическая среда, и в ней собираются вся информация, необходимая для проведения расследования. Плюс к этому — здесь же собираются данные по инфраструктуре, и можно наблюдать за тем, как атака отражается на различных её этапах. Отдельно хочется отметить возможности системы по построению картины рисков. Вводится понятие бизнес-сервиса и бизнес-процесса, и, благодаря модулю визуализации, можно смотреть, какие стадии бизнес-процесса находятся под угрозой. Вообще-то это лучше один раз увидеть, чем много раз услышать — специалисты с опытом работы в SOC сразу же отмечают полезность и удобство такого инструментария.

— **И чем это помогает сотрудникам банка? Понятно, что сама по себе визуализация любого процесса — положительный момент, но, положим, происходит инцидент, и что дальше?**

С. Рублев: А дальше сотрудники ИБ-департамента и других подразделений банка получают в режиме реального времени сигналы о том, какие информационные системы находятся под угрозой прямо сейчас и какие могут оказаться под угрозой при успешной реализации атаки. На основании данной картины становится ясно, какие риски необходимо устранить в первую очередь.

— **Подтверждается ли ваша высокая оценка качеств и функционала системы отзывами клиентов?**

А. Сидоров: Полноценных внедрений мы пока не имеем: как я уже ска-

зал, компания работает на российском рынке меньше года. К настоящему моменту у нас проведено несколько «пилотов», и отзывы компаний-заказчиков очень положительные. У одного из клиентов проводилось «пилотирование» системы в условиях, максимально приближённых к боевым. Мы развернули нашу платформу в рамках центра ИТ-мониторинга и продемонстрировали весь процесс обработки инцидентов от выявления до закрытия с полной детализацией картины атаки. В рамках испытаний демонстрировались возможности системы для различных ролей сотрудников: аналитик 1-й линии, руководитель смены аналитиков, специалист по расследованию инцидентов, руководитель SOC.

— **Если ваше решение является, как вы сами сказали, уникальным по некоторым параметрам, то оно наверняка относится к разряду дорогостоящих. Насколько доступным оно является для компаний с небольшим бюджетом на информационную безопасность?**

А. Сидоров: События последних нескольких лет показывают, что экономить можно на всём, но только не на собственной киберзащите. Особенно хорошо это понимают компании, столкнувшиеся с последствиями успешно реализованных атак. Это первый момент, который я хотел бы отметить. А второй момент заключается в том, что создание центра кибербезопасности — сам по себе весьма недешёвый процесс, ведь речь идёт не только о приобретении серверов и софта, но и о формировании специализированного подразделения ИБ, найме высококвалифицированных специалистов, которых расхватывают с рынка как горячие пирожки. Для эффективной работы центра требуется разработка и отладка процессов реагирования, чтобы они работали как часы, зачастую — изменение бизнес-процессов предприятия. Компаниям, создающим SOC, в любом случае приходится «раскошелиться». С каждым годом растёт число участников рынка, понимающих, что ущерб от успешных кибератак — причём и финансовый и репутационный ущерб — зачастую оказывается намного выше, чем все затраты на создание и работу центров киберзащиты.

— **Ценовой фактор имеет значение, но не меньшее значение имеет и фактор времени. Как быстро может быть развернута Платформа Радар?**

С. Рублев: В данном случае не всё зависит от нас. У крупных компаний достаточно сильно «закручены гайки» во всём, что касается информационной безопасности. А поскольку наша система агрегирует данные из других установленных систем, то требуются права доступа, настройки учётных записей и т.д. Поэтому процесс первичной установки системы может занимать от двух месяцев до полугода — в зависимости от того, насколько быстро решаются перечисленные мной вопросы на стороне заказчика.

— **Это нормальный срок.**

С. Рублев: Да. Как показывает опыт, в более короткие сроки никто «не укладывается». Хотел бы особо подчеркнуть, что речь идёт именно о процессе первичной установки системы. А полноценное внедрение с реорганизацией бизнес-процессов, с обучением персонала и т.д. в среднем занимает от полугода до года.

— **В начале нашей беседы вы сказали, что ваша компания рассматривает Платформу Радар как ключевой для себя продукт. Планируется в ли в дальнейшем расширение продуктовой линейки компании за счёт включения в нее других продуктов, или же совершенствование Платформы Радар?**

С. Рублев: Мы сейчас ведём работу по доработке функционала, чтобы он соответствовал каждой букве постоянно меняющихся требований в области защиты КИИ. И понятно, что нет предела развития по количеству поддерживаемых источников событий и интеграций с инфраструктурными решениями. Кроме того, мы развиваем центр компетенции по киберугрозам: поскольку паттерны кибератак меняются со временем, мы стараемся своевременно выпускать правила, «заточенные» на актуальные техники атакующих. Это интеллектуальная составляющая нашей системы, призванная помочь заказчикам эффективно противодействовать угрозам для их инфраструктуры.



Максим ПАВЛУНИН
Руководитель Центра
киберустойчивости ACRC,
Angara Professional Assistance

КАК СТАТЬ АНАЛИТИКОМ SOC

В мире информационной безопасности (ИБ) существует много различных направлений деятельности. В статье мы разберём, что такое SOC и какими компетенциями должен обладать аналитик.

ЧТО ТАКОЕ SOC

Security operations center (SOC) — центр обеспечения информационной безопасности. Основными задачами SOC является осуществление мероприятий по мониторингу и реагированию на инциденты ИБ.

Выявление инцидентов ИБ производится путём анализа различных событий, генерируемых системами корпоративной инфраструктуры: системами защиты информации, информационными системами, сетевым оборудованием, технологическим оборудованием, рабочими станциями пользователей, серверами и т.д.

В крупных организациях приходится обрабатывать десятки и даже сотни миллионов событий в день, поэтому мониторинг в таком объёме без автоматизации невозможен. Как правило, в качестве ядра комплекса программного и аппаратного обеспечения используются системы класса SIEM.

Security Information and Event Management (SIEM) — это централизованная система сбора, анализа и хранения событий. SIEM позволяет визуализировать данные, выявлять нарушения по определённым правилам и оповещать ответственный персонал.

Современные системы защиты информации не способны отразить 100% возможных атак, поэтому требуется постоянный контроль квалифицированными специалистами за уровнем информационной безопасности в корпоративной сети.

КТО ТАКОЙ АНАЛИТИК SOC

Аналитик SOC — человек, занимающийся анализом событий, выявлением и реагированием на инциденты ИБ.

Существует два основных сценария мониторинга событий ИБ: Alerting и Hunting.

Alerting — метод, при котором поиск признаков различных атак осуществляется по разработанным правилам. Основную задачу по выявлению осуществляют средства защиты информации (СЗИ) либо SIEM. Результатом работы систем является событие о возможном инциденте ИБ с определённой точностью — подозрение на инцидент ИБ. Оно требует ручной обработки аналитиком SOC с целью подтверждения или опровержения конкретного события.

Hunting — метод анализа событий путём выявления нетипичной активности в работе определённых информационных систем, сетевом трафике и прочих событиях, обрабатываемых при мониторинге. Осуществляется преимущественно «вручную» опытными специалистами. Основная цель — выявление инцидентов ИБ, которые не могут определить текущие средства защиты информации (СЗИ) в автоматическом режиме.

При выявлении инцидента ИБ аналитик осуществляет его классификацию и регистрацию в системе учёта. Процесс реагирования в общем случае преследует цели:

- ♦ подтвердить или опровергнуть факт инцидента ИБ;
- ♦ осуществить сдерживающие мероприятия: отключение хостов от сети, ограничение доступа атакующих к системам и прочее;
- ♦ собрать подробную информацию об инциденте, определить все источники и цели;
- ♦ устранить инцидент ИБ;
- ♦ определить степень влияния инцидента ИБ на затронутые бизнес-процессы;
- ♦ составить отчётность по инциденту ИБ;
- ♦ сформировать перечень рекомендаций по исключению подобных инцидентов в будущем и принять участие в их реализации.

КОМПЕТЕНЦИИ АНАЛИТИКА SOC

Какими же знаниями и навыками должен обладать аналитик SOC для выполнения своих должностных обязанностей?

Во-первых, необходимо знание нормативных документов в области ИБ, а также общих принципов действия и способов защиты от современных видов угроз для определения рисков и принятия решений при анализе подозрений на инцидент.

Во-вторых, понадобятся знания различных векторов атак и принципов их

выявления. Несомненное преимущество даёт практический опыт в проведении тестов на проникновение (Penetration testing).

В-третьих, требуется понимание принципов работы и технических возможностей множества систем защиты информации.

Все инциденты так или иначе связаны с различными нарушениями при работе корпоративной сети или информационных систем, поэтому потребуются знания:

- ♦ принципов работы компьютерных сетей;
- ♦ модели OSI и основных протоколов TCP/IP;
- ♦ принципов работы клиент-серверных приложений;
- ♦ администрирование ОС;
- ♦ управление доменом Active Directory.

При выполнении работ по анализу данных часто помогают навыки программирования, они способствуют автоматизации рутинных операций и развитию алгоритмического мышления.

ПРОБЛЕМАТИКА ПОДБОРА ПЕРСОНАЛА

Одной из моих задач является подбор и обучение персонала SOC, чем я занимаюсь уже больше 5 лет. В год я провожу около 30–80 собеседований, что позволяет выделить определённые тренды рынка персонала ИБ.

Как правило, основными кандидатами на должность аналитика SOC являются выпускники профильных вузов и специалисты с опытом работы в различных областях ИТ и ИБ. Из-за общего дефицита специалистов в отрасли ИБ крайне сложно найти опытного аналитика.

Основной критерий отбора — опыт и знания. Для развития практических навыков достаточно интересоваться тематикой и постепенно развивать свои умения.

КАК СТАТЬ АНАЛИТИКОМ SOC

Стремительное развитие тактик и инструментов нападения провоцирует непрерывный процесс обучения специалистов SOC на всех этапах

На этапе обучения все новые сотрудники проводят базовый цикл атак на тестовую инфраструктуру, анализируют собираемые события, выявляют следы данных атак и практикуются в расследовании инцидентов

карьерной лестницы. Необходима постоянная актуализация знаний.

Начинать самообразование стоит с корпоративных сетей, используя программы для моделирования, которые позволяют тестировать различные сценарии работы.

Полезные материалы по теме: «Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND 2 200–101. Маршрутизация и коммутация», Уэндел Одом. В качестве системы моделирования можно использовать Cisco Packet Tracer.

В организациях, как правило, используются операционные системы семейства Windows и Linux, поэтому нужно поддерживать свои знания по их администрированию и управлению. Наиболее полезны книги Марка Русиновича и Брайана Уорда.

В подготовке по всем процессам современного SOC помогут материалы MITRE, в матрице MITRE ATT&CK (attack.mitre.org) есть информация о методах и средствах нападения.

Для развития своих знаний по выявлению различных атак в корпоративной сети помогут практические навыки в тестировании на проникновение. Отработать владение инструментами и тактиками проведения атак можно на площадках lab.pentestit.ru или hackthebox.eu. Начинающим специалистам будет интересно участвовать в различных CTF-соревнованиях, где предстоит решать различные головоломки и использовать свой опыт в области ИТ и ИБ.

ОПЫТ РАЗВИТИЯ ПЕРСОНАЛА В ANGARA

При наборе персонала в подразделение SOC Angara Cyber Resilience Center (ACRC) важнейшим критерием успешного прохождения интервью является

заинтересованность кандидата в развитии. Знания можно подтянуть при вводе в должность.

В процессе внутреннего обучения используется индивидуальный подход к каждому сотруднику, проводится тестирование, где выявляются сильные и слабые направления, и подбирается программа. Теоретические и практические занятия проводятся под руководством опытного наставника. Этот подход реализовывает отработку важных навыков, ведь работа аналитика SOC не может сводиться к простому следованию инструкциям.

Внутреннее обучение для аналитика обычно занимает несколько месяцев в зависимости от его начальной подготовки.

В обучении акцент ставится на развитие практических навыков, для чего используется тестовая среда. В ней сотрудники могут упражняться в разворачивании и настройке различных систем защиты информации и инструментов, познакомиться с возможностями используемых платформ, решать задачи по администрированию и настройке различных информационных систем и другое.

На этапе обучения все новые сотрудники проводят базовый цикл атак на тестовую инфраструктуру, анализируют собираемые события, выявляют следы данных атак и практикуются в расследовании инцидентов. После прохождения обучения, аналитик приступает к решению «боевых» задач, но на этом его развитие не останавливается.

* * *

Основное оружие аналитика — это умение строить и проверять гипотезы, а эти умения нужно постоянно тренировать.

«АЙТИ БАСТИОН» + DLP = СОГЛАСИЕ

ИНТЕГРАЦИЯ WALLIX BASTION С DLP В СТРАХОВОЙ КОМПАНИИ «СОГЛАСИЕ» ПРОШЛА УСПЕШНО

Компания «Айти БАСТИОН» успешно провела интеграцию Wallix Bastion с DLP-системой FORCEPOINT по протоколу ICAP на инфраструктуре страховой компании «Согласие».

Работу современной крупной компании сложно представить без организации удалённой работы для разработчиков и штатных сотрудников. На рынке достаточно решений, помогающих технически организовать удалённый доступ, но почти всегда остаётся открытым вопрос контроля за обработкой конфиденциальной информации.

В «Согласии» проект по организации удалённого доступа к ресурсам компании включал задачу организации контентного анализа потоков данных, обрабатываемых при удалённом подключении. Техническое решение должно позволять анализировать события по существующим в компании политикам безопасности и, при необходимости, блокировать доступ или утечку информации.

Для выполнения поставленных задач оптимально подошла система Wallix Bastion (WAB). Система WAB имеет функцию интеграции с DLP-системами по протоколу ICAP. В такой схеме Wallix Bastion работает аналогично прокси-серверу, подключённому к DLP-системе. В системе контроля доступа создаются конкретные политики безопасности на классификаторах/регулярных выражениях/словарях. Политика позволяет определять поведение системы в случае нарушения политики заданного сценария.

В условиях передачи больших объёмов информации (например, во время обновления ПО) любые дополнительные операции проверки могут вызывать заметное увеличение необходимого времени работы, а также создавать дополнительную нагрузку на вычислительные средства. Эти и другие особенности данного механизма разработчикам «Айти БАСТИОН» пришлось исследовать, учесть при разработке и

протестировать в лабораторных и «боевых» условиях.

По мнению специалистов страховой компании «Согласие», Wallix Bastion хорошо показал себя в повседневной работе. Интерфейс ПО имеет широкие возможности кастомизации под задачи, система показала хорошую стабильность. Функция интеграции с DLP-системой значительно расширила возможности по реализации политик информационной безопасности в части контроля передаваемых через РАМ-систему данных.

Страховая компания «Согласие» планирует и в дальнейшем использовать Wallix Bastion, чтобы решать задачи по администрированию информационных систем, удалённого доступа контрагентов и разработчиков и масштабировать решение для организации удалённых рабочих мест штатных сотрудников.



Дмитрий МИХЕЕВ
технический директор
ООО «Айти БАСТИОН»

«Проверка файлов, передаваемых в рамках сессий администрирования через ICAP, необходима для защиты инфраструктуры от возможного вредоносного кода, а также от возможных утечек конфиденциальной информации. Так как протоколы удалённого администрирования, как правило, криптографически защищены, в обычной ситуации DLP-системы и антивирусы не могут легко получить эту информацию для контроля.

При этом необходимость дополнительного взаимодействия со средствами защиты может вызывать дополнительные задержки в работе администраторов, чего нам хотелось бы избежать, чтобы наша система минимально влияла на интерактивную работу специалистов. Это задаёт довольно жёсткие требования к архитектуре РАМ-системы, и мы старались (и стараемся) выполнить механизмы интеграции таким образом, чтобы системой можно было продолжать пользоваться, даже если через неё передаются большие объёмы файловых данных».



Дмитрий СЛОБОДЕНЮК
коммерческий директор ARinteg

АНТИФРОД В РОССИЙСКИХ РЕАЛИЯХ

Развитие антифрод-систем в России происходило, как и во всём мире, постепенно. Основными катализаторами стали зафиксированные инциденты. Нет худа без добра. События 2011–2012 гг., когда произошла массовая серия атак на ДБО, поначалу затронувших преимущественно юридических лиц и впоследствии распространившихся на физических лиц, банковский троян «Lurk» в 2014–2015 гг. и другие вредоносные программы способствовали развитию российских антифрод-решений.

Позже подключились законодатели. В 2018 г. был принят Федеральный закон от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств», касающийся представителей кредитно-финансового сектора.

На тот момент было ощущение, что для некоторых финансовых организаций потери от фрода были невелики — меньше стоимости самих антифрод-решений.

Однако, в том же 2018 году Сбербанк опубликовал статистику, согласно которой с помощью внедрённой антифрод-системы удалось сохранить более 32 млрд рублей, принадлежащих вкладчикам. В том же докладе сделан особый

упор на то, что большая часть инцидентов связана с социальной инженерией и так называемыми самопереводами. 86 % из всех случаев социальной инженерии составили «самопереводы» денежных средств под влиянием мошенников.

На текущий момент большое влияние на внедрение и развитие антифрода оказывает не только 167-ФЗ, а целый ряд законов, постановлений и положений ЦБ РФ, направленный на противодействие мошенничеству в банковской сфере и глобально на развитие информационной безопасности в этом секторе. Например, 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём и финансированию терроризма» не связан напрямую с кражей денег с расчётных счетов кредитных организаций, однако действия, описанные в нём, вполне можно отслеживать и пресекать с помощью автоматизированных средств — AML и антифрод-систем.

ВИДЫ АНТИФРОДОВ

Транзакционный антифрод обрабатывает те потоки данных, которые находятся внутри банковской системы, в частности, внутри ДБО. Выявляет транзакции, не соответствующие типичным действиям клиента, и анализируют платёж по «чёрным спискам». Зачастую транзакционный антифрод уже интегрирован в ДБО его разработчиком.

Другим примером транзакционного антифрода является решение компании WhyHarpen — резидента Сколково. Именно это решение было успешно внедрено компанией ARinteg в АО «Морской Банк» в 2019 году.

Антифрод WhyHarpen позволяет осуществлять транзакционный анализ и через систему сбора и обработки данных коррелировать те события, которые с точки зрения банковских аналитиков нелегитимны, выявлять признаки реализации как уже известных мошеннических сценариев, так и

В 2018 году Сбербанк опубликовал статистику, согласно которой с помощью внедрённой антифрод-системы удалось сохранить более 32 млрд рублей, принадлежащих вкладчикам



фиксировать аномалии в поведении клиентов или сотрудников, приостанавливать подозрительные операции и/или информировать о них.

Анализ проводится по платёжным операциям, которые генерируются клиентом в различных каналах обслуживания: интернет-банк, мобильный банк, оплата картами в магазинах и в Интернет, обслуживание в дополнительных офисах банка, операции в банкоматах и пр. И по неплатёжной активности клиента, которая фиксируется в банковских системах, например, успешные или неуспешные попытки входа в ДБО, характер перемещения пользователя по страницам личного кабинета, смена контактной информации, время и геолокация проведения операции и ещё целый ряд параметров. На базе таких параметров может формироваться «вектор», характеризующий поведение клиента, строится его типовой профиль и фиксируются отклонения (аномалии). Кросс-канальный анализ, сочетающий оценку платёжного профиля и неплатёжного поведения клиента позволяет выявлять сложные схемы мошенничества или операции клиентов с признаками сомнительности (ПОД/ФТ), используя для этого максимум информации.

Сессионный антифрод позволяет отслеживать параметры пользовательской сессии и определять мошенническую активность на банковском сервисе. Собирая обезличенные данные о пользователе, устройстве, его окруже-

нии, поведении с цифровых каналов в рамках сессии, система фрод-мониторинга на основе машинного обучения и настроенных правил формирует уникальный профиль пользователя. Данные по денежным транзакциям пользователей банка (объёмы операций, реквизиты, получатели и прочее) не собираются. В основе анализа также лежат ретроспективные данные по прошлым сессиям пользователя. Обычно в процессе внедрения сессионного антифрода рекомендуется закладывать около трёх недель на обучение системы на трафике банка для профилирования пользователей и повышения качества обнаружения. Главная задача — выявить нетипичное, аномальное поведение пользователя на протяжении сессии, основываясь на многих факторах: с какого устройства выполняется вход, как пользователь двигает мышкой или водит пальцем по экрану смартфона, GPS-координаты, используются ли средства удалённого управления, ведётся ли постороннее подключение к сессии, заражено ли устройство и многое другое. Анализируются десятки параметров. Пример сессионного антифрода — Kaspersky Fraud Prevention. В 2018 году эксперты ARinteg успешно интегрировали решение Kaspersky Fraud Prevention в одном из крупнейших российских банков.

Важно отметить, что системы сессионного фрод-мониторинга применимы не только для обнаружения мошеннической активности с пользовательски-

ми учётными записями в интернет- и мобильном банкинге. Оценка риска заявки на выдачу кредита, выявление мошенничества на P2P и C2C-переводах, в случаях, когда пользователь даже не авторизован в системе — также востребованные сценарии в банковской сфере. И сессионный антифрод решает эти задачи. Ещё один отдельный и серьёзный вопрос, который может закрыть антифрод (не каждый!) — выявление фродовых случаев, связанных с отмыванием денежных средств через различные учётные записи с использованием разных устройств и комбинаций скомпрометированных аккаунтов юридических и физических лиц. При этом легитимный пользователь может не знать, что его учётная запись онлайн-банка была скомпрометирована и используется в преступных целях.

Комбинированный антифрод сочетает сессионный и транзакционный анализ.

КАКИЕ РИСКИ ЗАКРЫВАЮТ АНТИФРОД-СИСТЕМЫ

Любая система безопасности направлена на снижение тех или иных рисков. Банки и финансово-кредитные организации, помимо прочего, сталкиваются с двумя типами рисков: потеря денежных средств (своих или клиентов) и регуляторный риск. При этом требования регуляторов для банков зачастую строже, чем требования безопасности, т.к. штрафные санкции могут быть значительными.

Антифрод-системы позволяют реализовать как защиту от угроз информационной безопасности в банке, так и обеспечить выполнение требований регулятора, т.е. управлять регуляторным риском.

Нельзя забывать и про репутационный риск в случае инцидентов безопасности и освещения их в СМИ, социальных сетях. Негативный опыт даже одного пользователя может спровоцировать отток лояльных клиентов, уменьшение объёма новых клиентов, снижение уровня доверия к банку, повышение затрат на восстановление репутации бренда.

Банк обязан наблюдать за платёжным поведением клиента. Согласно Федеральному Закону 161-ФЗ «О национальной платёжной системе» при приёме к исполнению распоряжения клиента оператор по переводу денежных средств обязан удостовериться в праве клиента распоряжаться денежными средствами. В рамках реализуемой им системы управления рисками оператор по переводу денежных средств определяет процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера, параметров и объёма совершаемых его клиентами операций (осуществляемой клиентами деятельности).

В соответствии с Положением 382-П Банка России оператор по переводу денежных средств, банковский платёжный агент (субагент), оператор услуг платёжной инфраструктуры обязаны обеспечить выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации.

В случаях, если нарушения организацией требований законодательства влияют на бесперебойность функционирования платёжной системы либо на услуги, оказываемые участникам

платёжной системы и их клиентам, Банк России применяет одну из следующих мер принуждения:

1. направляет предписание об устранении нарушения с указанием срока для его устранения;

2. ограничивает (приостанавливает) предписанием оказание операционных услуг, в том числе при привлечении операционного центра, находящегося за пределами Российской Федерации, и (или) услуг платёжного клиринга.

Сама возможность такой санкции, как ограничение оказания операционных услуг, например, запрет на приём вкладов от физических лиц и ограничение выдачи кредитов юридическим лицам, требует от кредитной организации уделять значительное внимание вопросам, связанным с противодействием мошенничеству.

В качестве наказания ЦБ может также перевести банк на ежедневную отчётность на срок от полугода до нескольких лет.

Один раз в два года банки обязаны проходить независимый аудит инфраструктуры платёжных систем — документированную независимую экспертизу состояния защищённости платёжных систем в соответствии с требованиями Положения ЦБ от 09.06.2012 № 382-П.

Банк обязан выявлять факты отмыывания денежных средств. Отмыывание денег является серьёзной проблемой и влияет на национальную безопасность, так как подобная деятельность помогает финансировать организованную преступность, способствует коррупции и усиливает социальные разногласия. В таких мошеннических схемах финансовые организации становятся невольными жертвами.

В Положении Банка России 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыыванию) доходов, полученных преступным путём, и финансированию терроризма» перечислены факторы, влияющие на оценку риска клиента, к которым в том числе относится совпадение идентификатора устройства клиента с устройством из списка подозрительных. Финансовая организация обязана уведомлять Банк России о мо-

шеннических аккаунтах и устройствах, задействованных в схемах по отмыыванию средств.

Все указанные регуляторные риски успешно закрываются своевременным внедрением системы антифрода.

Вывод

Банковское мошенничество само по себе никуда не денется. Но внедрение организациями лучших практик и систем по борьбе с фродом и соблюдение требований регулятора могут существенно повлиять на всю кредитно-финансовую экосистему. Тем более, что российские разработчики предлагают достойные и конкурентоспособные антифрод-решения.

Внедрение системы антифрода является необходимым, но недостаточным условием для эффективного противодействия мошенничеству и выполнению требований регулятора. Помимо внедрения самой системы, необходимо выстроить процессы мониторинга и реагирования, взаимодействия с клиентами и смежными подразделениями внутри банка, а также с другими кредитными организациями. Необходимо поддерживать в актуальном состоянии базу правил антифрод системы, постоянно её модернизировать с учётом текущей ситуации, опыта других банков и появления новых мошеннических схем.

* * *

Также нужно отметить, что внедрение любой кросс-канальной антифрод-системы — это ещё и довольно сложный интеграционный проект, т.к. необходимо собирать и анализировать данные из различных каналов обслуживания клиентов и банковских ИТ систем. Здесь и системы Интернет-банкинга, АБС, CRM, процессинг, шлюзы на поставщиков услуг и т.д. Поэтому такие проекты, зачастую, выполняются в партнёрстве между производителем антифрод-решений и системными интеграторами. В рамках такого партнёрства, компании могут предложить оптимальное решение и привнести опыт других заказчиков и опыт работы экспертов, экономя время, деньги и усилия для кредитной организации.



Куаныш ТАЛГАРОВ
директор департамента
информационных технологий
АО «ИО «Казахстанская
Ипотечная Компания»

«ЗА ВРЕМЯ ПЕРВОГО ЭТАПА ПРОЕКТА МЫ ПОДКЛЮЧИЛИ К 1IDM ШЕСТЬ СИСТЕМ»

«Казахстанская Ипотечная Компания» — один из крупнейших финансовых операторов государственной политики в области обеспечения доступности жилья населению Республики Казахстан через механизмы ипотечного кредитования и предоставления арендного жилья. Компания подотчётна регулятору — Национальному Банку Республики Казахстан, который регламентирует деятельность всех финансовых организаций в стране. В числе прочих требований регулятора есть требования по информационной безопасности в части организации процесса учёта прав доступа, за несоблюдение которых следуют штрафные санкции. Для внедрения новой системы в качестве вендора была выбрана российская платформа 1IDM.

На вопросы BIS Journal отвечает Директор департамента информационных технологий АО «ИО «Казахстанская Ипотечная Компания» Куаныш Талгаров.

— Куаныш, расскажите, о каком требовании регулятора в данном случае идёт речь?

— Казахстанская Ипотечная Компания подотчётна регулятору — Национальному Банку Казахстана, который регламентирует деятельность всех финансовых организаций в нашей стране. И одно из требований касается информационной безопасности в части организации процесса учёта прав доступа к данным компании.

— Как часто у вас проходят проверки регулятора? Насколько строги его требования? Какие штрафные санк-

ции грозят компании в случае невыполнения требования?

— Проверка проводится примерно раз в три года. Требования довольно строгие — существует несколько нормативных документов, которые необходимо выполнять. В данных документах очень подробно определено, как должна быть организована система информационной безопасности финансовой организации. Штрафные санкции могут быть применены в сумме до 1 136 000 тенге (примерно 190 000 рублей), а также вплоть до приостановки действия лицензии на финансовую деятельность.

— Какие цели и задачи стояли перед вами в ходе данного проекта?

— В первую очередь, это централизация всего управления доступами, контроль соблюдения внутренних политик, аудит учётных записей, смена паролей,

BIS-КОММЕНТАРИЙ

Роман Федосеев, генеральный директор компании 1IDM:

— Проект имеет свои особенности, а именно: у заказчика кадровый учёт ведётся на казахском языке, т.е. из кадрового источника загружаются сотрудники с ФИО на казахской кириллице. Далее по сценарию для сотрудника необходимо создать учётную запись в управляемой системе MS Active Directory с логином, сформированном на английском языке и заполненными атрибутами учётной записи на русском языке.

В итоге «особенность» решается штатными средствами из интерфейса 1IDM, благодаря возможности ведения нескольких таблиц транслитерации, их настроек, а также возможности настройки правил формирования атрибутов учётных записей управляемых систем.

создание единого веб-интерфейса. До начала реализации проекта в Компании создание и изменение учётных записей в каждой системе проводилось отдельно, что создавало определённые неудобства в работе. Для организации рабочего места нового сотрудника необходимо, чтобы администратор каждой системы создал для него учётную запись и предоставил доступы в соответствии с занимаемой должностью. В этих целях создаётся, как минимум, учётная запись в AD и почтовый ящик. Также в зависимости от функциональных обязанностей сотрудника, необходимо создать дополнительные учётные записи в 3–4 системах. При изменении должности сотрудника в каждой системе необходимо менять права доступа. Всё это приводит к лишним трудозатратам и повышает риск появления «забытых» учётных записей, либо учётных записей с некорректными правами. Также в каждой системе необходимо было настраивать свои парольные политики, в соответствии с требованиями безопасности. Сейчас этот проблемный вопрос снят путём внедрения новой системы.

— Вы выбирали партнёра исключительно на российском рынке или же рассматривались компании на рынках других стран?

— Мы рассматривали разные решения и искали партнёров не только на

российском рынке. Мы изучили предложения по платформам и стран дальнего зарубежья и российские: IBM, One Identity, Solar, Avanpost. И в итоге пришли к единому мнению — решение 1IDM нам наиболее подходит.

— Из каких этапов состоит проект? Возникали ли по его ходу какие-то сложности?

— Проект состоял из двух этапов — внедрение в подготовительной среде и апробация, и второй — перевод в продуктив. Больших сложностей не возникало, в основном работа проводилась с Active Directory — необходимо было настраивать определённые политики и устанавливать требуемое системное ПО. Но все эти технические сложности были решаемы. Наши системные администраторы установили или обновили необходимые компоненты, и апробация прошла гладко. Никаких глобальных проблем не возникло.

— Почему всё-таки ваш выбор остановился на компании 1IDM, какие факторы на это повлияли? Как быстро приняли решение о сотрудничестве?

— При выборе поставщика всегда играют роль два фактора: цена и качество. В компании 1IDM используется ПО от фирмы 1С. Соответственно, стоимость выбранного решения была ниже, чем у других аналогов, во-первых. Во-вторых, важным для нас плю-

сом является наличие технической поддержки на русском языке. В-третьих, наличие партнёра с необходимым опытом в Казахстане. Кроме того, среди факторов, которые повлияли на наш выбор, я бы выделил простоту системы, наличие готовых коннекторов к имеющимся в компании системам, особенно 1С, поскольку аналоги из дальнего зарубежья не поддерживают 1С «из коробки».

Решение о сотрудничестве было принято на основании тендерных процедур примерно в течение одного месяца.

— Могли бы вы рассказать, сколько и каких систем вы подключили к 1IDM за 3 месяца? Обычно проекты по подключению 2–3 систем занимают по полгода и больше.

— За время первого этапа проекта мы подключили к 1IDM 6 систем: 1С Зарплата и управление персоналом, 1С Бухгалтерия, Active Directory, MS Exchange, файловый сервер на базе MS Windows Server 2012, а также СУБД Oracle в режиме «Отключённое приложение». Также была настроена передача информации из 1IDM в SIEM-систему Компании.

— Удовлетворены ли Вы сотрудничеством с 1IDM?

— Вполне. Компания оперативно реагирует на все наши запросы, быстро и качественно выполняет все работы.

BIS-КОММЕНТАРИЙ

Айхан Абдильдинов, менеджер по работе с ключевыми заказчиками ТОО «NewTech Distribution»:

— Партнёром 1IDM на казахстанском рынке выступила компания ТОО «NewTech Distribution», которая выказала интерес к российскому продукту и изъявила желание эту компетенцию у себя наращивать, видя её в качестве нового направления бизнеса. Другим клиентам ТОО «NewTech Distribution» это решение также может стать полезным и интересным.

Мы получили запрос от потенциального клиента на выбор решения для создания системы управления учётными записями и правами доступа. Нашими специалистами совместно с представителями заказчика был произведён отбор подходящих решений, среди которых было российское решение фирмы 1IDM.

В течение месяца были проанализированы все решения и был сделан выбор в пользу решения 1IDM. 1IDM имеет в своём составе все необходимые коннекторы, кроме того, идеально интегрируется с системами 1С, которые представлены у заказчика. В кратчайшие сроки провели пилотное тестирование и продемонстрировали заказчику функциональность ПО. В ходе пилота были сняты все остававшиеся вопросы.

ТОО «NewTech Distribution» имеет достаточный опыт в интеграции программного обеспечения. Благодаря совместным усилиям со специалистами 1IDM сложностей в реализации непосредственно проекта не возникло. Мы довольны сотрудничеством с компанией 1IDM: все вопросы, возникавшие в период проведения проекта, решались оперативно.



РКИ-ФОРУМ 2019

ИНФРАСТРУКТУРНЫЕ ПРОЕКТЫ, ЗАКОНОТВОРЧЕСТВО
И ТРАНСФОРМАЦИЯ ОТРАСЛИ

В сентябре в Санкт-Петербурге прошла XVII Международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи — РКИ-Форум. Среди важнейших тем на повестке форума в этом году значились поправки к закону об электронной подписи 63-ФЗ и развитие отраслевого законодательства в целом, опыт трансграничного электронного документооборота и отечественных инфраструктурных проектов, использование РКИ в финансовой сфере и др.

НА ПОВЕСТКЕ

В течение трёх дней в рамках официальной части РКИ-Форума состоялись

пленарная дискуссия, шесть тематических сессий и два круглых стола. В приветственном слове первый заместитель генерального директора АО «НИИАС» Владимир Матюхин выразил уверенность в том, что благодаря уникальным условиям Форума будут найдены подходы к целому спектру актуальных и злободневных вопросов отрасли: например, нормативному регулированию юридически-значимого электронного документооборота в рамках программы «Цифровая экономика РФ», изучению технических и организационных условий для формирования цифровой среды доверия, условий трансграничного взаимодействия, выработаны совместные стратегии для развития бизнеса участников рынка.

В своём пленарном докладе статс-секретарь-заместитель министра цифрового развития, связи и массовых коммуникаций РФ Олег Пак, в частности, подчеркнул авторитетность площадки РКИ-Форума и обозначил делегатам актуальные вопросы развития отрасли, на которые по результатам конференции хотелось бы получить ответы. В первую очередь, это вопрос о том, кто должен проводить первичную идентификацию граждан при получении сертификатов ключей проверки подписи, а также вопрос о том, кто должен выдавать сертификаты ключей проверки электронной подписи гражданам для электронного паспорта.

По мнению директора правового департамента Министерства цифрового



Статс-секретарь-заместитель министра цифрового развития, связи и массовых коммуникаций РФ Олег Пак

развития, связи и массовых коммуникаций РФ Романа Кузнецова, проблемы развития отрасли, стоящие на повестке дня, могут быть решены рядом законодательных инициатив, находящихся сегодня в разной степени готовности.

НАКАНУНЕ ИЗМЕНЕНИЙ

Участники дискуссии признают, что трансформация рынка электронных подписей назрела и должна быть проведена в короткие сроки. Необходимо, прежде всего, обеспечить возможность однозначной идентификации и аутентификации удостоверяющими центрами заявителей на изготовление сертификатов ключей проверки подписи, запретить возможность использования простой формы доверенности для получения сертификата ключа проверки подписи на юридическое лицо, создать систему аудита деятельности удостоверяющих центров по мировым стандартам качества, обеспечить корректное архивное хранение электронных документов с электронной подписью, ввести в УК РФ и КоАП РФ ответственность за правонарушения с использованием электронной подписи. Омбудсмен по цифровой экономике Илья Димитров отметил и ещё один аспект, который должен сопровождать изменения: их экономическую целесообразность. Организации не должны столкнуться с оптимизацией «для галочки», когда ор-



Выступление директора правового департамента Министерства цифрового развития, связи и массовых коммуникаций РФ Романа Кузнецова

ганизационные перемены не приносят никакой пользы с точки зрения эффективности процессов, повышения уровня безопасности для пользователей и экономии ресурсов.

ДВА СТАНДАРТА

Говоря о стандартизации, как неотъемлемой составляющей технологического развития, стоит упомянуть прежде всего о появлении первых двух стандартов из плана по развитию системы национальных стандартов: ГОСТ Р «Идентификация и аутентификация. Общие положения» и ГОСТ Р «Уровни доверия к результатам идентификации». Они были разработаны при участии Технического комитета по стандартизации «Защита информации» (ТК 362), — сообщил представитель комитета Алексей Сабанов. А в рамках ТК 26 готовятся методические рекомендации «Информационная технология. Криптографическая защита информации. Инфраструктура Открытых Ключей. Доверенная третья сторона. Протокол сервиса валидации».

ОПЫТ КРУПНЫХ КОМПАНИЙ

Электронный документооборот стал неотъемлемой частью как внутренних, так и внешних бизнес-процессов организаций, это особенно важно для крупного бизнеса, где во взаимоотношения вступают сотни юридических лиц, партнё-

ров, контрагентов, подрядчиков и т.д., а поддерживают эти процессы сотни и тысячи автоматизированных систем. С этой точки зрения интересен, например, опыт ОАО «РЖД», где внутренний безбумажный документооборот достиг объёма 2 млн документов в год, активно развиваются проекты по безбумажным технологиям грузоперевозок на основе электронных документов с юридической силой, а также по единой аутентификации пользователей на базе открытого стандарта OAuth 2.0.

В свою очередь, проект внедрения кастомизированного решения «Аванпост PKI», обеспечивающего работу корпоративного удостоверяющего центра, продемонстрировал «МегаФон». «Мы обеспечили выполнение жёстких SLA, дали возможность более чем 40 тысячам сотрудников компаний «МегаФон» и «МегаФон Ритейл» оперативно получить сертификаты ключей проверки электронной подписи, снизили различные регуляторные риски и уменьшили трудозатраты операторов УЦ», — подвёл итоги проекта руководитель удостоверяющего центра ПАО «МегаФон» Игорь Поздняков.

Целые отрасли всё активнее становятся пользователями решений, связанных с открытыми ключами и электронными подписями, сервисами идентификации и аутентификации. Экспертный совет «Электронные до-

кументы — эффективная экономика» ECR-RUS провёл исследование закономерностей при использовании электронных подписей в ритейле и высказал рекомендации для регулятора. Всероссийский центр экстренной и радиационной медицины им. А. М. Никифорова МЧС России — одно из передовых лечебных учреждений, реализующее принципы безбумажного документооборота в медицине. В банковской сфере наступают ещё более существенные изменения: для удалённой идентификации и получения банковских сервисов теперь действует Единая биометрическая система, распознающая клиента по голосу и изображению лица. Об особенностях её внедрения и применения рассказали представители оператора биометрической системы — «Ростелеком»: директор проекта Проектного офиса «Единая биометрическая система» Дмитрий Улыбин и главный инженер проектов «Ростелеком-Solar» Максим Добровольский.

ДЛЯ ЧАСТНЫХ ЛИЦ

Основная инновация в сегменте частных лиц, которая может во многом трансформировать рынок электронных подписей, — введение электронных паспортов граждан взамен бумажных. Выдачу карты из многослойного пластика, содержащей бесконтактную микросхему, с фотографией владельца и QR-кодом, планируют начать уже в 2020 году на базе инфраструктуры системы «МИР», — прокомментировала системный архитектор НИИ «Восход» Мария Вдовина. По сути, вместе с ней каждый житель страны получит собственную электронную подпись и доступ к более широкому пулу госуслуг.

А КАК ЗА РУБЕЖОМ?

Организаторы мероприятия не обошли вниманием зарубежный опыт законодательных инициатив и проектной деятельности в области PKI и электронного документооборота. К примеру, были рассмотрены общеевропейский опыт развития коммерческого рынка услуг удостоверяющих центров и других сервисов доверия в соответствии с Регламентом № 910/2014 Европейского парламента и Совета Европейского Союза «Об электронной идентифика-



Сессия «Использование PKI-технологий в финансовой сфере»



Круглый стол «Нормативные и технологические аспекты архивного хранения ЭД»



Вручение дипломов победителям в ежегодных номинациях PKI-Форума за 2019 год



Сессия «PKI и ЭП в инфраструктурных проектах России»

ции и удостоверительных сервисах...» (eIDAS), система управления полномочиями на основе атрибутивных сертификатов и опыт построения трансграничного пространства доверия в Республике Беларусь. Кроме того, был представлен опыт создания трансграничного пространства доверия в сегменте B2B в интересах биржи вагонов «РЭЙЛ КОММЕРС» на основе сервиса доверенной третьей стороны Республики Казахстан и сервиса проверки электронных подписей аккредитованного удостоверяющего центра «УЦ ГИС» в Российской Федерации.

СОЦИАЛЬНЫЕ АСПЕКТЫ

Особую роль на форуме играли круглые столы, участники которых при активном взаимодействии с залом обсудили социальные аспекты применения электронной подписи (например, тенденционное освещение в СМИ преступлений, совершённых путём незаконного использования квалифицированной

электронной подписи), нормативные и технологические нюансы архивного хранения. В рамках круглого стола Наталья Храмцовская, ведущий эксперт по управлению документацией компании «Электронные Офисные Системы», поделилась практикой судебных решений по делам, связанным с мошенничеством при использовании усиленной квалифицированной электронной подписи.

ПОБЕДИТЕЛИ ГОДА

PKI-Форум был организован при поддержке Медиа Группы «Авангард», Минкомсвязи и ФСБ России. Генеральным партнёром мероприятия в этом году выступил федеральный оператор цифровых сервисов «Ростелеком», официальными партнёрами стали компании «КриптоПро» и «Газинформсервис».

В официальную часть вошло также вручение дипломов победителям в ежегодных номинациях PKI-Форума за 2019 год. В номинации «Организа-

ция года» победила Ассоциация «Разработчики и операторы систем электронных услуг» (РОСЭУ). «Регионом года» стала Москва; «B2G проектом года» — Фонд социального страхования РФ с «Электронным листком нетрудоспособности»; «Корпоративным проектом года» — «Безбумажная клиника» ФГБУ ВЦЭРМ им. А.М. Никиторова МЧС России; «Продуктом года» — программный комплекс «Litoria Desktop 2» ООО «Газинформсервис»; «Законодателем года» — Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26).

PKI-Форум 2019 посетило около трехсот человек, для которых, помимо официальной части, была организована яркая и запоминающаяся культурная программа в прекрасном осеннем Санкт-Петербурге.

ОСЕННЯЯ СЕССИЯ УРАЛЬСКОГО ФОРУМА 2019

ВЕРШКИ ИЛИ КОРЕШКИ?

Добрую память о сентябре в Москве оставила не только тёплая сухая погода. Осенняя сессия Уральского форума под эгидой Банка России порадовала добрым профессиональным общением и полноценными ответами на вопросы безопасников. Банк России, официально перешедший в весовую категорию мегарегулятора в сфере ИБ, также получил информацию для размышлений.

ПРО ЕБС

Острых вопросов было много. Отвечая на некоторые, даже непоколебимый Андрей Выборнов, заместитель директора Департамента информационной безопасности Банка России, был вынужден брать тайм-ауты для выработки позиции. По сути Осенняя сессия стала для Андрея Выборнова своеобразным бенефисом — он модерировал работу двух заседаний и задал тон дискуссии «Информационная безопасность Единой биометрической системы».

Дискуссия эта проходила на фоне слайда, обобщающего сведения из 38 банков РФ (обслуживающих более 80% «физиков») о текущей ситуации с ЕБС и, на первый взгляд, свидетельствующей о ЕБС-саботаже. Пока совсем немногие сочли возможным довериться этой системе. Тем не менее, дискуссия сосредоточилась не на доверии к ЕБС, а на

обсуждении «подъёмности» и оправданности затрат на внедрение и эксплуатацию биометрической компоненты ДБО на основе требований мегарегулятора.

Некоторые вопросы остались без ответа. Например, если биометрию планируется использовать не только для предоставления финансовых, но и «других услуг», то каких «других»? И какая инфраструктура должна быть для этого создана? И как она будет стыковаться с финансовой инфраструктурой?

БЕЗ ВОПРОСОВ

Единственным мероприятием Осенней сессии, которое не только не поставило вопросов перед мегарегулятором, но и дало конкретные ответы залу, была сессия «Реализация требований по защите каналов с использованием отечественных средств криптографической защиты».

Доклад Алексея Данилова из «ИнфоТеКС», представившего линейку программно-аппаратных комплексов для защиты информации в сетях на основе отечественной криптографии, подсказал, как защитить свои каналы, не обращаясь к зарубежью.

А доклад Валерия Конявского представил как идею, так и реальные внедрения компьютеров с т.н. «новой гарвардской» архитектурой. Особенности этой архитектуры, предложенные и запатентованные докладчиком и вопло-



щённые в «железе» ОКБ САПР, не позволяют вредоносному ПО закрепиться и работать в ущерб системе. Компьютеры на основе такой архитектуры не только защищают каналы с использованием отечественных средств криптографической защиты, но и работают в автоматике на железнодорожном транспорте, в планшетах некоторых министерств.

ПРО СОЦИАЛЬНУЮ ИНЖЕНЕРИЮ

На этой сессии вопросы возникли. Рассматривая проблему социальной инженерии, зал сломал немало копий, обсуждая доверчивость и наивность «простых» людей, но так и не задался вопросом, почему социальная инженерия успешно сработала и для многих представителей «высшего общества», утративших свои накопления в известных банках? Уж наивными и доверчивыми этих людей никак не назовёшь!

А ведь если бы аудитория задумалась, то не требовала бы так рьяно от Банка России больше социальной рекламы для населения, и обсуждала бы не вершки, а корешки проблемы социальной инженерии. Можно предположить,



что корень зла в том, что современное общество не культивирует честность. Тиражирование цитат из откровений нынешних кумиров о невозможности отчитаться за первый миллион — это явно не тот корешок, который питает сохранение банковской тайны.

Что же касается повышения осведомленности персонала, то чего только стоит упоминание Алексея Лукацкого о том, что даже в Cisco 1 % сотрудников службы ИБ (службы ИБ!) регулярно попадает на «удочку» (во время контрольных проверок бдительности).

Зал, к сожалению, пропустил мимо ушей реплику Алексея Лукацкого о возможности подкрепления обороны финансовых институтов от социальной инженерии техническими методами. Уточнить подробности этого предложения по свежим следам не удалось. Влекомый модератором, зал распалялся, требуя ужесточения наказаний для «чёрных» социальных инженеров и делясь личными наблюдениями о покушениях на психологию держателей банковских карт.



Артем Сычев, первый заместитель директора ДИБ Банка России



Андрей Выборнов, заместитель директора ДИБ Банка России



Дискуссия «Практика борьбы с социальной инженерией в системах ДБО»

ORACLE SYSTEMS ADVANTAGE FORUM

УЧИСЬ У ЛУЧШИХ!

Встроенный ИБ-иммунитет для кого-то — перспектива. Для Oracle — это «10 лет инноваций». Эта компания заложила основы своего авторитета как создатель высоконадёжной и высокопроизводительной СУБД, вышла на новый уровень, приобретя активы легендарной Sun Microsystems, и сегодня её базовая платформа именуется Машина баз данных. В сентябре компания провела в Москве Oracle Systems Advantage Forum.

АППАРАТНЫЙ ПОДХОД

Машины от Oracle неплохо себя чувствуют за охраняемым периметром КИИ, но уверенно защищают «цифровые активы» организации и при прорыве внешней линии ИТ-обороны. Технология Security in Silicon для противодействия заражению вредоносным ПО обнаруживает и предотвращает недопустимые операции над данными и работает быстрее, чем традиционные программные средства.

Аппаратный подход вообще занимает важное место в технологиях Oracle. Аппаратно — на серверах хранения оборудования Exadata, а не в ПО серверов СУБД, — производится дешифрование и декомпрессия данных. А оптимальная организация процедур сжатия и шифрования данных работает ещё и на повышение быстродействия.

УВЕРЕННОСТЬ ЧОНГ ХЕНГ ХАНА

При уважительном отношении к роли аппаратных средств обеспечения ИБ, Oracle уделяет пристальное внимание «зачистке» потенциальных дыр в программном обеспечении. В первую оче-

редь это касается минимизации компонентов в ОС Linux и использовании расширений этой операционной системы, которые позволяют устанавливать обновления системы безопасности без перезагрузки ОС.

Полагаю, что приведённые факты в немалой степени способствовали уверенности Чонг Хенг Хана, старшего вице-президента Oracle Systems в регионе ЕМЕА, АРАС и Япония, в том, что при нынешней напряжённой обстановке в киберпространстве (атаки происходят в среднем каждые 39 секунд) эффективнее фокусировать усилия по защите ключевых активов, обрабатываемых КИИ, в ядре инфраструктуры. Это утверждение старший вице-президент высказал на открытии форума.

ПОМНИ ОБ ЭКСПЛУАТАЦИИ!

На фронтальных панелях флагманских вычислительных машин наименование Oracle соседствует с ещё одним уже упомянутым знаковым словосочетанием — Sun Microsystems. «Sun Microsystems! Не Sun Microstorage и не Sun Microchips, и не Sun Micro-operating Systems, и не Sun Micromiddleware... Мы ищем деятельных и старательных СІО, которые просто устали заниматься интеграцией и предпочтут купить цельную систему... Многие же другие очень любят накопить «лучшие в отрасли изделия» от 800 поставщиков, сэкономя на их стоимости, и абсолютно не интересуясь стоимостью последующей эксплуатации».

В этих тезисах — гимне методологии высокой готовности — нет упоминания кибербезопасности лишь потому,

что слова эти были сказаны во времена, когда войны в киберпространстве ещё только проектировались. Уже тогда Oracle подхватила базовые технологические и моральные ценности Sun Microsystems и объединила их со своими ноу-хау.

СБЕРБАНК И ВОДОКАНАЛ ПОЛУЧИЛИ ПОДАРКИ

Встроенный аппаратный ИБ-иммунитет машин Oracle открывает разнообразные возможности безопасной работы в киберпространстве для тех отечественных потребителей, кто имеет такую возможность. Среди них разные организации, например, Сбербанк и Мосводоканал даже удостоились на форуме специальных наград за успехи во внедрении машин Oracle в свои бизнес-процессы.

Кроме чествования лучших, форум анонсировал новинку — машину Exadata X8 — и изложил ИТ-стратегии развития бизнеса с использованием аппаратных решений Oracle для частного и гибридного «облака». Консультанты российского офиса компании представили возможности создания ИТ-инфраструктуры для развития и применения технологий машинного обучения с учётом важнейших требований ИБ, а также такие ключевые для ИБ технологии, как резервное копирование и восстановление данных. На мероприятии было рассказано, как машины Oracle позволяют использовать возможности сетей 5G на полной скорости этой телекоммуникационной технологии.

Тем же в родном Отечестве, кто хочет или обязан рассчитывать на импортозамещение при построении своих сегментов КИИ, можно порекомендовать включить в свой арсенал системные инженерно-методические подходы Oracle&Sun Microsystems к созданию отказоустойчивых и киберзащищённых вычислительных машин с высоким уровнем доступности. Скачок в развитии обеспечен.

При нынешней напряжённой обстановке (атаки происходят в среднем каждые 39 секунд) эффективнее фокусировать усилия по защите ключевых активов, обрабатываемых КИИ, в ядре инфраструктуры

MOBILE FORENSICS DAY

СБРОСИТЬ НЕЛЬЗЯ РАСШИФРОВАТЬ

Мobile Forensics Day 2019 — конференция по мобильной криминалистике — была сугубо технологической, если не считать доклада представителя Следственного комитета «Использование методов OSINT для расследования преступлений». Это про то, как информация, оставляемая людьми в открытых источниках (по большей части — в интернете), позволяет собирать доказательства для раскрытия преступлений, совершенных и готовящихся.

ДОБРОВОЛЬНО И ПРИНУДИТЕЛЬНО ОДНОВРЕМЕННО

Интересным аспектом темы, раскрытой представителем СК, является добровольность выставления людьми на всеобщий обзор личной, а зачастую и интимной информации.

Но оказывается, гуманитарная добровольность «душевного стриптиза» сегодня тесно граничит со «стриптизом» технологически принудительным. Как следовало из доклада «Ваш собственный шпион: что может рассказать о вас ваше мобильное устройство», смартфоны и сопряжённые с ними гаджеты в виде, например, фитнес-браслетов, передают в «облака» разнообразную информацию о перемещениях, здоровье, покупках, социальной активности и т.д. их добровольных носителей.

По сути упомянутый доклад не многое добавил к совокупной информации от штатных «диванных аналитиков». Зато был насыщен впечатляющими личными историями. Например, как докладчик обнаружил, что информация об его частной жизни, оказывается, уже препарирована и содержится в «облаках» на глубину, как минимум, в десять лет. Именно тогда он совершил сугубо частную зарубежную поездку, и только недавно, исследуя профессиональные ресурсы и технологии, обнаружил отчет, в том числе и видео-, о передвижениях

по той стране. Как следили и зачем — этого докладчик, по его словам, так и не понял.

СЕРЬЕЗНЫЕ ФОКУСЫ

Не добавили оптимизма и другие доклады. В докладе «Атаки на мобильные устройства: тактики и техники злоумышленников» названия этих тактик и техник заняли страницу формата А4 при написании шестым кеглем. В докладе «Сбросить нельзя расшифровать: современное шифрование данных Android-устройств» список уязвимых процессоров в современных смартфонах произвел не меньшее впечатление. И только практические демонстрации вскрытия информации на смартфонах на стенде «Мобильный криминалист эксперт» немного подняли настроение — уж очень было похоже на выступление фокусников.

СОЧЛИ ЗА ТРУД

Не лучше ситуация и с приложениями ДБО. Доклад на тему уязвимости этой банковской технологии с примерами реальных «дыр» (нескольких десятков!), не позволил ни одному из 5 банков, входящих в ТОП-10, заслужить высший балл. Среди попавших «под раздачу» этого исследования лишь один банк получил 3,5 балла из пяти, а два — заслуженную «единицу». При этом, по мнению докладчика, многих ошибок можно было избежать, если бы разработчики не сочли за труд ознакомиться с рекомендациями некоторых несекретных международных стандартов.

...ТОЛЬКО ЩЕПКИ ЛЕТАЮТ!

Наряду с докладами об угрозах, были представлены сообщения, что называется, «общего назначения». Например,

доклад о современных тенденциях и предпочтениях в области выбора паролей. Это выступление, безусловно, вызвало интерес не только у ценителей «высокой моды» в этой сфере, но и у тех, кто пароли взламывает.

Интересным был и рассказ о проекте, триггером для запуска которого стала утрата конфиденциальности маркетингового исследования, стоившего несколько миллионов рублей. Финал проекта — тотальный контроль личных персональных устройств в организации. Хотя причиной исходного инцидента оказались не мобильники сотрудников, а несоответствия в ИБ-политике конфиденциальности и её реализации.

КАРТА «ДЫР»

Параллельно с докладами проходили мастер-классы, которые продемонстрировали новые возможности инструментов для компьютерно-технической экспертизы в криминалистике. Спектр их довольно широк: от нишевых инструментов вроде ПО для подбора паролей до комплексного решения «Мобильный криминалист эксперт».

Под занавес конференции представитель компании «Электронное облако» набросал своеобразную карту «дыр» безопасности в рабочих ИТ-технологиях современной бытовой и деловой мобильности, сопроводив их живыми и актуальными примерами и рекомендациями по части преодоления угроз.

Закончилась же конференция на позитивной ноте — розыгрышем призов и афтерпати с напитками и душевными беседами «за ИБ».

Оказывается, гуманитарная добровольность «душевного стриптиза» сегодня тесно граничит со «стриптизмом» технологически принудительным



Александр БАРАНОВ
заведующий кафедрой ИБ
НИУ ВШЭ, доктор физико-
математических наук, академик
Академии криптографии РФ

«БУДЕМ С УЖАСОМ СМОТРЕТЬ...»

ПОЧЕМУ ГОСУДАРСТВЕННИК АЛЕКСАНДР БАРАНОВ
ИЗМЕНИЛ ТОЧКУ ЗРЕНИЯ НА ИМПОРТОЗАМЕЩЕНИЕ

Предлагая Александру Павловичу Баранову принять участие в дискуссии по импортозамещению¹, мы ожидали вполне определенной, твердой централизованной позиции. Услышали же совсем другое.

— Один из участников нашей дискуссии считает, что для создания суверенной ИТ-экосистемы в России необходимо организовать что-то вроде профильного Госплана...

— А вы знаете, что даже Советский Союз не смог реализовать эту тему?

— Руки не дошли или время кончилось?

— Потому и кончилось, что руки не дошли. Тут все связано. В Советском Союзе интернет придумали еще в 50-е годы, а в 60–70-е по всей стране создавалась Общегосударственная система автоматизированной системы учета и обработки информации. Система АСУ должна была объединить все крупные предприятия и образовать такую кибернетическую систему управления экономикой. Руководил этим академик Виктор Глушков и поначалу успешно. АСУ было создано очень много. А знаете, почему в СССР все рухнуло?

— Почему?

— Потому что вранье было сплошное. В Госплан поступали искаженные

данные. Их подтасовывали под рапорты, под ведомственные интересы, получали ордена, медалики... В результате этого вранья невозможно было сложить реальную картину, Госплан не мог нормально планировать. И вот эта глобальная система АСУ — советский а-ля интернет — должна была исправить положение — свести объективную информацию непосредственно с производств в единый центр. Не получилось.

— Почему?

— Якобы не договорились Госплан с Минфином. Минфин в случае реализации проекта существенно терял полномочия. Вот и не дал денег. Ведомственная система в то время многое погубила, в том числе и саму себя.

— Давайте вернемся к импортозамещению.

— Я прочитал статью, о которой вы говорите². Отличная, правильная статья в духе советского управленческого менталитета. Лет десять назад я подписался бы под ней обеими руками. Но так получилось, что с импортозамещением я столкнулся лет 15–20 назад, когда мы с Валентином Васильевичем Соломатиним участвовали в работе по созданию МСВС. Тогда, в начале двухтысячных, речь об импортозамещении шла только в аспекте операционной си-

стемы для военных. Просто все понимали, что к железу и не подступиться. А более широко и предметно обсуждение началось лет десять назад. Тогда я тоже придерживался концепции централизованного управления.

Но за эти десять лет, работая, как практик и, как теоретик, в Высшей школе экономики, я пришел к выводу, что централизованная система, пожалуй, и не сможет решить эту задачу. Слишком она масштабная, многофакторная, проблемная. Конечно, можно воспользоваться опытом Лаврентия Павловича Берии. Как ни крути, а в космос мы полетели и бомбу сделали, хотя и с большими издержками.

— Менеджмент на костях?

— Да, не дай нам Бог такого менеджера еще раз получить. Но и не дай Бог еще раз решать такого сорта задачи и в таком же авральном режиме. А чтобы жить без авралов нужно всё делать вовремя. И вот, участвуя в обсуждении импортозамещения больше десяти лет, я пришел к некоторым выводам.

МАСШТАБ ПРОБЛЕМЫ И СХЕМЫ ВЗАИМОДЕЙСТВИЯ

Помню, как на конференциях все это время обсуждалось импортозамещение программного обеспечения, а об остальном — тишина. На самом деле, и ПО, и железо — все это связано, оторвать одно от другого невозможно.

¹ BIS Journal №2-3/2019

² BIS Journal № 2/2019. Карл Сумманен, «ИТ-импортозамещение в России. Пути дальнейшего совершенствования», стр. 42–49

А вот моделировать и представлять в виде схем взаимодействия не только можно, но и нужно. Это, пожалуй, единственный способ, как вообще нам эту проблему осознать и, соответственно, с ней справиться. Потому что за эти годы, если что-то и стало понятно, так только то, что проблема огромная.

Ну, начиная с того, что сопротивление, простые электрические сопротивления в радиодеталях, вместе с этими радиодеталями в любом компьютере присутствуют. И конденсаторы, и транзисторы, и микросхемы под 25 нанометров, а то и меньше. И много чего другого. Это со стороны железной части, а с другой, программной: биосы, операционки, которые уже срослись с биосами, прикладное ПО и тоже много-много другого... И вот всё это вместе образует такой огромный клубок, ком, на который некоторые смотрят с ужасом. Как все это импортозаместить?!

ПРО НАУКУ

На что опереться? Конечно, на науку. Но тут приходится констатировать, что как наука компьютерные технологии ещё не состоялись. Простой пример: имеется ли общепризнанная классификация прикладного ПО? Нет! Также не существует классификации железа. Известно, конечно, что есть железо для телекоммуникации и для вычислительных процессов. То есть два крайних класса, а что там между ними творится — не систематизировано. Теория информационной безопасности — тоже пока еще псевдонаука, как и теория компьютерных систем. Экспериментальных фактов много набрали, а дальше не двинулись. Как все отрасли наук развиваются? По наукометрии так: сначала экспериментальный этап — сбор информации, затем классификация, дальше прогнозирование и, наконец, подтверждение прогнозов. Если на четвертом этапе всё сходится, то это — наука. Вот и выходит, что тут мы на начальной стадии.

Да, накопленные экспериментальные факты существуют в виде прикладных программ и операционных систем. Операционных систем уже больше тысячи, а программ так и вообще под миллион. Одних фотошопов сколько! И за этим массивом, конечно, уже многое про-

сматривается: закономерности, методики... То есть опора все-таки есть, и её нужно развивать и укреплять.

МОДЕЛЬ УГРОЗ — КАРТА ПОТРЕБНОСТЕЙ

С чего начинается информационная безопасность для любой компьютерной системы? С модели угроз. Об этом все знают, и если кто-то не сразу делает, то рано или поздно к этому приходит. А что такое импортозамещение, если не способ обеспечения информационной безопасности чего? Сформулировать с ходу сложно, так как много аспектов, но можно поставить вопрос по-другому: не для чего, а для кого? И сразу станет проще. Во-первых, для военных и гостайны. Во-вторых, для госаппарата и крупных компаний. И в-третьих, для гражданского оборота.

Сразу понятно, что требования для этих трех групп разные. Для военных очень жесткие, для госаппарата и крупных компаний менее или выборочно, например, требования по устойчивости только для отдельных частей. А для гражданской сферы таких серьезных требований не требуется, ну, разве, в отдельных особых случаях. Соответственно и приоритетные задачи для каждой из этих областей будут разные. И их нужно четко сформулировать.

Почему я это говорю? Потому что дальше идут производственные вопросы, собственно импортозамещение. Когда мы сформулировали эти разные приоритетные задачи, начинается формирование конкретного заказа по потребностям — для реализации этих задач. И наверняка то, что требуется для военных, окажется ненужным для госаппарата, а то, что востребовано госаппаратом, будет ни к чему для гражданских.

Имея на руках такую ясную, понятную картину, и заказчикам, и подрядчикам будет легче ориентироваться на

рынке. В том числе и решать это пресловутое противоречие между отечественным и импортным, защищенностью и широтой прикладных функций. Это противоречие объективное, и не будем прятать голову в песок, никогда и никуда не денется. Но жить с ним можно.

РЕАЛИЗАЦИЯ. NBI

Мы живем при капитализме, а при капитализме главное — реализация продукции, продажи. Без этого нет развития, но почему-то именно на это у нас обращают мало внимания. Вот наш отечественный производитель создал замечательный, очень нужный продукт. И что? Его кто-то тут же купит? Ничего подобного.

Поэтому, чтобы не задушить нашего производителя, нужно определить и регулировать порядок реализации. Сегодня на конкурсах наше отечественное ПО имеет 15 процентов преимущества перед импортным. Но что такое 15 процентов? Это же мало, это никуда не годится. Производители-монополисты могут сделать дисконт в разы, в 100 процентов, и это всем известно. 15 процентов — это просто смешно.

В то же время, если на рынке останется только отечественное, тоже будет неправильно. Это сразу затормозит развитие, научно-технический прогресс. Поэтому порядок реализации для разных сфер должен быть разным. Для военных один, для госаппарата другой, а для гражданского оборота, возможно, это будет просто скидочная какая-то система.

И это направление — самое важное — оно у нас наименее проработано. Тут вот рыночники-маркетологи и должны поломать голову, придумать эти механизмы — не такие, как сейчас, слабые, а такие, чтобы машина рынка заработала в полную мощь, вывезла отрасль. Повторюсь, не будет эффективных ме-

Приходится констатировать, что как наука компьютерные технологии ещё не состоялись. Простой пример: имеется ли общепризнанная классификация прикладного ПО? Нет! Также не существует классификации железа



ханизмов — не будет реализации, а не будет реализации — и никакого импортозамещения не будет.

Вот, например, сегодня нужен абсолютно надежный, эффективный отечественный коммутатор для интернета. Сколько я ни разговаривал с производителями, слышу одно и то же: сделаем любой степени надежности, любой, так сказать, степени отечественности, но только если нам гарантируют сбыт. И я не сомневаюсь — сделают, и хорошо сделают, но как гарантировать сбыт — вот этого никто не знает. И это проблема. При социализме она решалась просто — приказали, и готово. Но такой подход обернулся застоєм и отставанием в тех же самых компьютерных технологиях. Сегодня нужны другие подходы.

ПРО ГОСУДАРСТВЕННУЮ ПРОГРАММУ

— Александр Павлович, скажите, а когда писалась государственная программа импортозамещения, всего это разве не знали?

— Не хочу трогать эту тему. Я дал себе слово: больше не критиковать. Раньше, каюсь, критиковал очень много, но пришел к выводу, что это контрпродуктивно. Надо предлагать, и не только идеи, но и как их реализовывать. К сожалению, я не могу предложить, как бороться с этими 15-ю процентами. Казалось бы,

взять и увеличить порог до 45–50 процентов, и одно это уже было бы неплохо. Но, думаю, там много чего можно правильного придумать, если поговорить непосредственно с производителями и продавцами. Там ведь серьезные противоречия между продавцами импортных и отечественных продуктов. И между ними нужно соблюдать баланс — нельзя, чтобы тех совсем уж не было. Но на то и существуют маркетологи, это их сфера.

А программа, на мой взгляд, всё-таки не учла десятилетнего опыта и фактически свелась к списку задач, но без приоритизации. Четкой дорожной карты вы там не увидите.

Наша беда в том, что мы перечисляем все возможное — все, что знаем, чем озабочены, валим в одну кучу. А нужно среди этого выделить — с болью, кровью — самое главное. Два-три пункта — и добиться по ним выполнения. А потом следующие два-три пункта. А по-другому не получится. Ну, нельзя потянуть все сразу! Вот я выделил три направления — военные, госаппарат и гражданский оборот. По каждому из них нужно определить две-три — даже одну-две первоочередные задачи. И выполнить их. Например, в области интернета задача понятна совершенно определенно — построение надежного отечественного коммутатора. Давайте это сделаем и двинемся дальше.

В СФЕРЕ ИБ

— А в сфере информационной безопасности?

— За эти десять лет выявилось еще одно заблуждение — мол, если отечественное, значит, безопасное. Но это не так. В наших продуктах, если они делаются бесконтрольно, без последующей аттестации и сертификации, обнаруживаются те же дыры, прорехи, остатки ветвей программирования, заглушек и т.д. — типичные ошибки программистов. По отношению к американским продуктам можно говорить, что это не ошибки, а закладки. Не буду отклоняться, тем более что конспирологические теории редко оказываются продуктивными, но факт остается фактом: многие отечественные продукты назвать безопасными нельзя. И в этом смысле постановление Правительства № 555 от 11.05.2017 г. совершенно правильная, обязательная вещь.

Его суть в том, что нельзя выделять деньги на сопровождение систем, построенных в интересах госорганов, если они не прошли аттестацию по информационной безопасности. И ФСТЭК уже определил достаточно разумный порядок, ничего там сверхъестественного нет. На начальном этапе нужно согласовать либо модель угроз, либо техническое задание. В основном все, конечно, выбирают модель угроз, потому что

техническое задание охватывает гораздо больше, чем информационная безопасность, и его сложно отстаивать. Обычно модель угроз согласовывают с ФСТЭКом, потом по техническому заданию эти угрозы блокируются, а в итоге, при аттестации, проверяется соответствие угроз и блокировок. Такой вот простой понятный путь. Выполнение этого замечательного постановления, на мой взгляд, — одна из важнейших задач для наших компьютерных продуктов.

Следующее, что стало понятно за эти десять лет. У нас есть замечательные ГОСТы, которые предполагают высокий уровень документирования и фиксации разработок. Но разработки у нас, как известно, ведутся нелинейно, особенно на длительных сроках. Планируемое изделие по ходу дела меняет свой облик, характеристики, и к завершению от первоначального замысла мало что остается. А ГОСТами корректировка технического проекта не предусмотрена. Такие вот они, эти ГОСТы — хорошие, но немного застывшие, неэластичные. И в результате получается, что документация не отражает действительности.

А фиксировать процесс разработки необходимо, особенно если она выполняется за государственный счет. Ведь в чем ценность этих ГОСТов, зачем их делали? Их делали для того, чтобы потом можно было воспроизвести изделие по сопровождающей его документации. Иногда это удается даже по советской документации, тут показательный пример — самолет ТУ-160. Кроме того, документация необходима при текущей эксплуатации, модернизации продукта. Однако, к сожалению, часто описание с какого-то момента ведется формально или вообще не ведется, особенно по программному обеспечению. Даже наличие исходных текстов не спасает, при отсутствии достаточных комментариев, детализаций и среды компиляции. В результате программы работают пока работают, а как они работают — неведомо. Поэтому назрела необходимость переработать эти ГОСТы, причем, с учетом потребностей и особенностей действующих организаций. Понятно, что такую работу бизнесу не поручишь, это дело институтов, имеющих соответствующий опыт.

К сожалению, часто описание с какого-то момента ведётся формально или вообще не ведётся, особенно по программному обеспечению. В результате программы работают пока работают, а как они работают — неведомо

ПРО АИС

Есть еще один аспект. Необходимо законодательно запретить принимать в эксплуатацию АИС без полной документации. Причем делается это не из прямого корыстного интереса, а скорее косвенного: чтобы остаться в проекте, оказаться незаменимым. Но вот что-то случилось: была фирма-разработчик, и нет её. Как быть? Где брать это ПО, как сопровождать систему, как модернизировать?

Понятно, что на Майкрософт у нас не будет такой документации, но там гарантом выступает гигантский, колоссальный монстр, у которого все что нужно есть, и он всегда окажет техническую поддержку. И это хорошо. Но у нас другая ситуация, у нас разработчики не такие устойчивые и надежные.

ПРО ЖЕЛЕЗО

Помните эйфорию, когда начали покупать заводы? Самые яркие иллюстрации — Микрон и Ангстрем, рассчитанные на массовое производство. А в результате обещанного чипового производства как не было, так фактически и нет. Есть у нас, конечно, предприятия, которые могут осуществлять разные разработки, иногда достаточно сложные, но небольшими тиражами.

Тут все та же проблема. Нужно идти от реальной модели угроз, точно формулировать задачи, соотносить возможность с необходимостью. А когда мы рисуем модель, которую невозможно выполнить, толку от нее никакого, только убытки. И выполнение задачи не должно быть обязательно линейным. Ну, не можешь ты решить ее техническими мерами — решай другими, например, организационными или еще какими-то. Главное, не надо фантазий. За эти десять лет мы наслушались

столько обещаний и красивых слов! Лучше пусть будет не так красиво, но зато реально.

Давайте посмотрим шире. Нет у нас заводов на 25 нанометров и, судя по всему, не будет. Но у китайцев это направление тоже весьма проблематично. Американцы построили им заводы на 25 нанометров, а завтра захотят прижать и не дадут следующую технологию на 12 нанометров. И все, через 2–3 года эти заводы окажутся ненужными. Потому что они ориентированы на чудовищную серийность и только в этом случае рентабельны. И китайцы окажутся в том же положении, что и мы с Микроном.

Но китайцы не стонут, а действуют. Например, развивают технологию фэблеса. У нас она тоже применяется, но очень скромно, хотя именно в нашей ситуации она может стать палочкой-выручалочкой.

ПРО ДЕНЬГИ

— Александр Павлович, я слышал много ваших выступлений на форумах, семинарах. И всегда в них референдом проходило «Дайте миллиард, и сделаем все что угодно: операционную систему, суперкомпьютер и т.д.». Смысл вполне определенный: государство должно быть заинтересовано и подтверждать это действием. А сейчас вы про деньги не сказали ни слова. Почему?

— Концепция изменилась: давайте сначала разберемся в хозяйстве, и будем ориентироваться на реальные потребности. Нечего, глядя вперед, питаться иллюзиями. Опыт, конкретный опыт, он позади.

— И что он показывает?

— Вот Леонид Дододжонович Рейман — один из эффективнейших руководителей — получил кредит для модернизации завода «Ангстрем» на

Импортозамещение — это широчайшая, полифоническая программа, затрагивающая чуть ли не половину населения страны. И она не может быть выполнена методами Лаврентия Павловича Бери

производство современных чипов и микросхем. Где результат? Результата нет! Почему? Ну, просто задача крайне трудная. Это показывает, что деньги сами по себе в таких масштабных и наукоемких проектах еще не все решают.

Свежий пример. Фирму, которая производит коммутаторы, выставили на продажу. Простят около 2 млрд рублей. Причем там все может быть отечественным, с полным комплектом документации по этим коммутаторам. Импортозамещение в чистом виде. А поскольку я интересовался именно надежными коммутаторами, я знаю, что обычно проблема в микросхемах физического уровня ASIC. А у них и эта проблема решена. Только сертифицируй, аттестовывай и производи. Вы знаете, не нашлось у нас покупателей на это.

— Почему?

— Всех волновало только одно: а кто гарантирует спрос? Поэтому я про деньги и не говорю. Деньги найдутся, это буквально все говорили: ну, да, 2 млрд рублей — это конечно большая сумма, но не критичная.

Конечно, просто так выкинуть 2 млрд — на это никто не решится. Для сравнения, мост в Крым стоил 300 млрд. И они нашлись. То есть дело не в деньгах, а в том, что нужно продумывать с другого конца. А так... Ну, купите вы заводик, начнет он что-то там шлепать, чего никто не будет покупать. Он быстро устареет, не будет модернизироваться и умрет. У Реймана, похоже, так и получилось. Поэтому я про деньги ничего и не говорил.

ОПЫТ И ОПЫТ...

— Вы говорите, десятилетний опыт, новое понимание экономики...

— А давайте мы не будем смотреть, как у нас, десять лет — не срок. Да-

вайте посмотрим там, где капитализм существует 200 лет. Финансирует ли государство подобные проекты? Да, финансирует. Но частично, выборочно, точно. А в первую очередь оно эти проекты организывает: продумывает, планирует, выставляет приоритеты. И запускает машину: тут конкурсы, там скидки, где-то ставит блоки, меняет ценовую политику, принимает законы, преференции. Добивается результата.

Мне Диффи, один из изобретателей открытого ключа, рассказывал, как в США организована работа с учебными институтами. АНБ (Агентство национальной безопасности США) объявило конкурс на создание криптографической системы без предварительного развоза ключей по абонентам. На грант была выделена обычная по меркам американцев сумма. Когда работу выполнили, приняли и грант оплатили, по условиям их контрактов были возможны два исхода. Первый — результат и все материалы становятся собственностью государства, авторы получают премию около 1 млн долларов и теряют все права на дальнейшее использование. Второй — государство работу не выкупает, премия не выплачивается, но авторы вольны использовать результаты по своему усмотрению. АНБ открыт ключ не выкупило. Авторы, как показала жизнь, не прогадали.

А у нас, как только деньги на научные проекты появляются, это самое финансирование, сразу начинается что-то несусветное — проекты не движутся, а наоборот тормозятся, идет борьба за будущую интеллектуальную собственность... Что происходит, толком никто не понимает... Поэтому я и не хочу этого обсуждать.

— Давайте подведем итог.

— Давайте. За эти десять лет, по крайней мере, у меня, сложилось твер-

дое убеждение, что импортозамещение компьютерных технологий — это задача не менее сложная, чем ядерный проект в 45-м году прошлого столетия. А может быть, даже более сложная. Тот проект был достаточно локализованный и решался не такими массовыми коллективами людей. Конечно, создавались урановые шахты, организовывалась добыча, работали научные институты, конструировался и запускался реактор... Но это был все-таки монопродукт, а импортозамещение — это широчайшая, полифоническая программа, затрагивающая чуть ли не половину населения страны. И она не может быть выполнена методами Лаврентия Павловича. Тут нужны другие подходы.

ЕСТЬ ОПАСЕНИЕ

Но есть опасение. Если мы потеряем еще десяток лет, то у нас некому будет осуществлять этот проект. Я восемь лет руковожу магистерской программой в ВШЭ и вижу, как развивается (не хочу использовать слово «деградирует») наша образовательная система. Если раньше я спрашивал у выпускников бакалавриата, сколько будет $\frac{1}{2} + \frac{1}{3}$, и не всегда получал правильный ответ, то теперь вынужден задавать другой вопрос: 4 факториал (4!) — это сколько? И не единожды получать ответ — 4 внимание. Потому что факториал обозначается знаком восклицания. То есть, поступив в магистратуру, они не знают, что такое факториал. Это чудовищно. И источник этого точно известен — ЕГЭ.

Поэтому нужно торопиться и решать вопрос с управлением программой импортозамещения. Оно должно быть другим — не тактическим, как сейчас, а стратегическим. Выбор стимулирующих мер — это стратегическая вещь, а не тактическая. Через нее начинается движение на рынке — развитие или деградация. Выберем правильные меры — будет и промышленность, и импортозамещение. Выберем неправильные — получится как с ЕГЭ. Будем с ужасом смотреть на то, что сотворили.

— Спасибо.

Беседовал Игорь Некрасов



Наталья КАСПЕРСКАЯ
президент ГК InfoWatch,
председатель правления
АРПП «Отечественный софт»

ШАГ ЗА ШАГОМ, ПОСТЕПЕННО...

НАТАЛЬЯ КАСПЕРСКАЯ СЧИТАЕТ, ЧТО
ИМПОРТОЗАМЕЩЕНИЕ ИДЁТ... СВОИМ ЧЕРЕДОМ

В IS Journal попросил представить свой взгляд на импортозамещение одного из ключевых участников этого процесса — Наталью Касперскую.

СИТУАЦИЯ

— Давайте зафиксируем ситуацию. Что, на ваш взгляд, на сегодняшний день представляет импортозамещение в сфере ИТ/ИБ в России?

— Буду говорить только про софт. Ситуация с «железом» тоже интересная, там идут свои подвижки, но за «железо» отвечает Минпромторг, а за софт Минкомсвязь. Мы работаем с Минкомсвязью, и тут я картину лучше вижу.

Четыре года назад Ассоциация разработчиков программных продуктов «Отечественный софт» (АРПП) вместе с Минкомсвязью выработали критерии для отечественного ПО, на этой основе в 2015 году был создан Единый Реестр российских программ для ЭВМ и баз данных, сейчас в нём уже больше 5 тыс. отечественных продуктов. Продукты в Реестр отбирает экспертный совет, в котором примерно половина — чиновники, представители Минкомсвязи, «Сколково», других институтов развития, а половина — люди из индустрии. В основном из АРПП, потому что именно участники АРПП эти программные продукты и создают.

Правительство выпустило два постановления: одно предписывает закупать

ПО из Реестра госорганам, другое — госкомпаниям. Потом были «директивы Силуанова», предписывающие покупать отечественные продукты госкомпаниям.

— И как идут закупки?

— Конечно, ситуация не везде одинаковая. Там, где у нас собственные продукты были ранее представлены на рынке, проблемы с импортозамещением нет. Например, в сфере ИБ в стране работает порядка 300 компаний. Они производят практически все типы софта по информационной безопасности, и это продукты хорошего мирового уровня: антивирусы, решения по защите от утечек (тут у нас семь производителей!), межсетевые экраны, средства защиты от вторжений, системы шифрования и т.п. Эти решения и раньше занимали значительную долю российского рынка, а с началом политики импортозамещения и вовсе вытеснили иностранцев, поскольку корпорации, как правило, начинают процесс импортозамещения с внедрения ИБ.

Но в других сферах всё не так замечательно. В частности, с трудом идёт импортозамещение офисного софта. Что греха таить, большинство компаний и организаций привыкли к Microsoft Office и менять его не хотят, а чтобы не менять, используют целый ряд трюков.

ПРО ТРЮКИ

— Про трюки интересно, расскажите...

— Первый трюк — закупают программные продукты под видом услуг. Закупают, например, услуги по поддержке информатизации, а для функционирования этих услуг вписывают иностранный софт. Второй трюк — закупка программно-аппаратных комплексов с предустановленным ПО, естественно, иностранного производства. Третий — это когда иностранное пытаются протаскать под видом отечественного, этим обычно производители грешат. Создают российскую компанию, получают от иностранцев ограниченные (или даже неограниченные) права на доработки, вносят незначительные изменения. И продают иностранный, слегка модифицированный, софт, как отечественный. Да ещё и пытаются вписать его в Реестр. Мы, конечно, стараемся отслеживать и блокировать такие попытки, но это непросто.

ПРО САНКЦИИ

— То есть российские госорганы и госкомпании импортозамещаться не хотят?

— Тем не менее, процесс идёт. Тут в прямом смысле слова «не было бы счастья, да несчастье помогло». Компании волнует не столько государственная регуляторика, сколько попадание

в какие-нибудь санкционные списки Запада, после чего привычный софт просто перестаёт работать. Те, кто попал под санкции, как-то сразу понимают необходимость импортозамещения. Только тогда это гораздо сложнее, чем если бы этот процесс был грамотно спланирован в спокойной обстановке.

— Кого-то можете назвать?

— ВПК практически весь, дочки Газпрома, предприятия Ростеха... Либо отдельный регион: в Крыму, например, база Oracle не поддерживается. Да и Microsoft, если не ошибаюсь, откуда уходил, но потом вернулся.

ПРО ЗАДАЧИ И КЛАССЫ

— Изменились ли за последние годы цели и задачи импортозамещения?

— Цель точно осталась прежней — заместить импортные продукты отечественными. В программу «Цифровая экономика РФ» импортозамещение включили как отдельное направление, по которому разработчикам полагается прямое субсидирование. Сейчас как раз идёт бурная дискуссия на тему: кому, как, зачем, сколько? Поддержка предполагается по девяти классам разработки: ОС, СУБД, офисные приложения, САПР, ERP, инжиниринговые системы и т.д. Мы очень надеемся, что удастся увеличить объём финансовой поддержки на эти классы.

— По какому принципу выбирали эти классы?

— В рамках нацпрограммы было сделано исследование, где выделены классы ПО, необходимые стране и при этом не способные развиваться чисто за счёт рынка. Например, операционные системы. Ну, невозможно продать ОС в современном мире, когда есть Microsoft Windows, или офисное ПО при наличии Microsoft Office!

ПРО МАСШТАБ И ОТЧЁТНОСТЬ

— Можно ли оценить реальный масштаб импортозамещения на сегодняшний день?

— Сложный вопрос. С одной стороны, импортозамещение идёт, и Минкомсвязи рапортует о больших успехах. А с другой, объёмы закупок софта в этом году резко упали.

— Почему?

— Дело в том, что компании закупили ПО на пять лет вперёд, потратили выделенные на это бюджетные деньги, и всё — они на пять лет с рынка исчезли. Но это одна сторона, есть и другая: что они с этим софтом делают — никто не знает. Часто просто кладут на полку, мол, долг перед Родиной оплатили, с нас взятки гладки. И продолжают пользоваться привычным Microsoft'ом. Поэтому сейчас Минкомсвязи планирует изменить условия отчётности, чтобы в зачёт шли не только закупки, но и использование. Для этого вводится так называемый коэффициент о реальном проценте использования ПО.

— А достижения есть?

— По некоторым классам мы хорошо продвинулись. Про информационную безопасность я уже говорила, могу добавить по DLP. Пять лет назад по этому классу доля иностранцев на нашем рынке была 20–23%. Сегодня их доля стремится к нулю. Получается, заместили. Про другие классы мне сложно судить, потому что реальных цифр нет. Я не знаю, как Минкомсвязи считает свою статистику. Но по разговорам с коллегами понимаю, что в большинстве областей нам ещё надо много работать.

О ТОРМОЗАХ

— Главный тормоз в импортозамещении, на ваш взгляд?

— Главное — это нежелание компаний. Один из аргументов, который они используют — «У вас продукт не такой

качественный, вы сначала сделайте качественный, а мы потом его закупим». Это ложное рассуждение. Во-первых, большинству клиентов, — а речь идёт о корпоративных клиентах, — не нужны те 152 функции, которые есть в Microsoft Office. Им надо отослать почту, поработать с документами, сохранить и т.д. То есть, нужны 3–5, ну, 10 функций, но никак не 152!

Но они пишут, и это, кстати, ещё один трюк, что нам, мол, нужен полный функционал, и пока вы его не реализуете, мы у вас покупать не будем. Во-вторых, невозможно сделать продукт качественным для абстрактного клиента. Продукт всегда делается под кого-то, у клиента обязательно появляются конкретные «хотелки», и эти «хотелки» разработчик исполняет. Если разработчик сидит рядом, в том же городе, ему проще это сделать, чем иностранцу, который где-то там, за морями, и ещё не известно, как понимает потребности нашего клиента и как на них реагирует. Вот поэтому нужен нормальный процесс: заказчик должен сначала купить ПО, а потом давать разработчику дорабатывать. Тогда это будет правильный, поступательный процесс.

А для того, чтобы сначала сделать, как Microsoft Office, нужно иметь денег, как у этой корпорации. Как это сделать, если объём всего нашего рынка — меньше, чем одна эта корпорация? И подход «вы сначала нам сделайте» — просто нереализуем.

— То, что компании-заказчики будут сопротивляться, было предсказуемо...

— Позицию заказчика понять можно. «У меня сейчас всё работает, а поставим ваш софт, и всё сломается. Кто будет нести ответственность?» Я постоянно с крупными заказчиками на эту тему разговариваю. Это довольно естественные опасения. Наша задача, как разработчиков, снизить эти опасения, идти заказчику навстречу, быстро исправляя ошибки и решая его проблемы.

В МЕЖДУНАРОДНОМ МАСШТАБЕ

— Скажите, а имеет ли наше импортозамещение какие-то аналоги в международном масштабе?

— Импортозамещение сейчас идёт во всех странах, которые хотят быть или,

Невозможно сделать продукт качественным для абстрактного клиента. Продукт всегда делается под кого-то, у клиента обязательно появляются конкретные «хотелки», и эти «хотелки» разработчик исполняет



по крайней мере, казаться самостоятельными. Чтобы быть независимыми, надо делать своё. Например, Германия. Хотя она и член Евросоюза, но выпустила предписание: закупать для госорганов немецкий софт. Не европейский даже, а немецкий. Нельзя сказать, что это прямой аналог нашего импортозамещения, у них нет таких жёстких законодательных требований. Но тенденция такая есть, и не только в Германии, и в Казахстане, и в Китае и других странах.

— А что в основе этой тенденции?

— У всех стран мотивация одна. Все современные технологии имеют удалённое управление. Получается, что управляет технологиями не тот, кто их покупает, а тот, кто производит. Никому это не нравится, все хотят иметь возможность управлять своими технологиями самостоятельно — вот и всё. Такие примеры, как удалённое отключение энергии в нескольких штатах Венесуэлы, здорово всех отрезвляют. Да и те методы давления, которые оказывают на Россию, когда Oracle и Microsoft заявляют о непредоставлении поддержки на следующий период... Все думают: «О-о-о! Они и с нами так могут...».

Если 15–20 лет назад мы наблюдали процесс глобализации, этакое слияние в общем технологическом экстазе, то сегодня все поняли, что у технологий есть обратная сторона, и надо как-то защищаться. И начался обратный процесс.

ДИАЛОГ С ПРЕЗИДЕНТОМ

— Скажите, имел ли продолжение ваш диалог с президентом во время прямой линии?

— Так уж у нас устроено: чтобы дело двинулось, нужен пинок сверху. Да, после этого была встреча с министром связи, было предписание усилить импортозамещение. И сейчас, насколько я знаю, и в правительстве готовятся документы, и в Минкомсвязи... В том числе и о том, чтобы при сборе статистики считать не объём закупок, а объём реального использования. Это очень важно.

ПРО ПЛАНИРОВАНИЕ

— Участники дискуссии об импортозамещении, которая идёт в BIS Journal, говорят о необходимости создать что-то вроде Госплана в сфере импортозамещения. Согласны ли вы с таким предложением?

— Любая корпорация, даже такая небольшая, как InfoWatch, составляет планы на 3–5 лет, иначе она просто не сможет развиваться. А у государства такого плана нет, и это странно.

Конечно, план в сфере импортозамещения должен быть: что, как, с какой скоростью и в какой последовательности мы замещаем. Возможно, и в форме Госплана — закончим импортозамещение, будем планировать новые задачи.

— А кто его должен создать?

— Думаю, отрасль разработчиков вместе с ответственными федеральными органами: Минкомсвязи и Минпромторгом. Собственно, в 2014 году, когда мы программу импортозамещения запускали, то что-то подобное — план-не план, скорее схему, — мы писали.

— Извините, не понял, кто писал?

— Ассоциация разработчиков программных продуктов «Отечественный софт». Мы составили классификатор софта, сделали анализ, что у нас есть, а чего нет, и сделали план: что, в какие сроки и какими ресурсами может быть замещено. Классификатор был положен в основу Единого Реестра россий-

ских программ для ЭВМ и баз данных, а план был использован для приоритизации направлений поддержки, о которых я говорила выше.

ПРО АРПП

— АРПП «Отечественный софт» играет заметную роль в процессе импортозамещения. Каковы реальные масштабы деятельности ассоциации?

— АРПП, как собственно и любая подобная ассоциация, создана для того, чтобы лоббировать интересы разработчиков. В ней 160 членов, в основном из Москвы и Петербурга, но постепенно идёт расширение в регионы. Направлений работы у нас много, импортозамещение — одно из них. Есть ещё направления поддержки экспорта, финансовой поддержки компаний, помощи в продвижении компаний... Сейчас появилось новое направление — образовательное. Работаем с вузами и школами.

— Давайте всё же об импортозамещении...

— Без ложной скромности именно мы были инициаторами импортозамещения в стране. Мы создали АРПП в 2009 году — ровно 10 лет назад — под идею импортозамещения, хотя тогда и слова-то такого ещё не было. Мы называли это «поддержкой отечественных разработчиков».

После Советского Союза, когда в стране было всё своё, маятник качнулся в сторону всего иностранного. В 90-е и начале «нулевых» отечественный ИТ-бизнес ещё как-то развивался, но после кризиса 2008 года компании стали умирать. Денег не было, а иностранцы уже проникли во все структуры и сверххрущевски лоббировали свои интересы.

Мы стали рассказывать о том, что иностранные технологии управляют удалённо, как это опасно для страны, что мы убиваем собственную технологическую ДНК... Нас слушали, кивали, но ничего не происходило. Помню, в 2012 году я встретила в Новосибирске с премьер-министром — им тогда был Владимир Путин — и донесла ему эту мысль. Владимир Владимирович идею поддержал, дал поручение... Но всё продолжало идти со страшным скрипом. Не знаю, сколько бы оно ещё

так скрипело, если бы в 2014-м году против нас не объявили санкции. И тут все чиновники встрепенулись, зашевелились. И началось собственно импортозамещение.

ПРО INFOWATCH

— Можно ли назвать компанию InfoWatch образцово-показательным примером в области импортозамещения? Если да, то почему?

— С импортозамещением у InfoWatch действительно всё в порядке. Этому я вижу две причины. Первая — высокое качество продукции. Мы входим в квадрант Гартнера, который по технологическим характеристикам называет наши продукты одними из лучших. Единственное, за что они нам снизили оценку, — мировое присутствие. Но это объяснимо: западный рынок из-за политики для нас практически закрыт. Ну, будем развивать Азию и Африку.

Вторая причина в том, что в сфере ИБ люди хорошо понимают опасность удалённого управления. Если вашу конфиденциальную информацию защищает американская корпорация, то где гарантия, что ваши данные не утекут? Все видят, как беззащитно ведут себя Facebook и Google. Понятно, что корпоративные клиенты не хотят такого к себе отношения, да и просто боятся. Поэтому они при прочих равных делают выбор в пользу отечественных продуктов.

И не обязательно, кстати, в пользу InfoWatch. Другие российские компании тоже выросли, а доля американских Symantec и Forcepoint упала.

ПРО СОВМЕСТИМОСТЬ

— Давайте перейдём к вопросам наших читателей — участников дискуссии. Алексей Смирнов из «Базальт СПО» спрашивает: «Государство требует закупать ПО преимущественно из Единого реестра отечественных программ, но в Реестре тысячи программ разного качества, и они не всегда между собой совместимы. Да и ссылка из Реестра на сайт производителя не всегда ведёт на документацию к программе. Как быть заказчику?»

— Про ссылку — это вопрос к Минкомсвязи. Действительно, есть такая проблема, ну, я думаю, не самая большая — сайт они подлечат.

Что касается разного качества и совместимости ПО, то Алексею, как никому, известно, что в АРПП создан комитет по интеграции. То есть мы сами решили не ждать, пока заказчики будут мучиться, совмещая наши решения, а составили карту совместимости и планируем выпустить каталог (первый выйдет к десятилетию АРПП), где эта совместимость показана. Мы прекрасно понимаем, что в Реестре 5 тыс. продуктов, и в них сам чёрт ногу сломит. Тут я согласна, облегчать жизнь заказчику надо.

И ПРО ИНВЕСТИЦИИ

— Для импортозамещения ПО требуется развитие отрасли разработки ПО, то есть инвестиции. Как государство может этому способствовать? Нужны ли прямые инвестиции со стороны государства в разработку ПО?

— В рамках программы «Цифровая экономика РФ» первоначально планировалось выделить из бюджета 5 млрд руб. на поддержку разработчиков ПО. Но когда рабочая группа проанализировала потребности разработчиков по девяти классам ПО, которые нуждаются в поддержке (я об этом уже говорила), то стало понятно, что денег нужно больше. Минкомсвязь нас в этом поддерживает. АРПП планирует просить правительство о расширении масштабов поддержки. Не все деньги пойдут на поддержку функционала разработчикам, часть пойдёт заказчикам — на компенсацию при закупках ПО, на снижение налогов...

— То есть, денег ещё нет?

— Да, денег, как всегда, ещё нет...

БОЛЬНАЯ ТЕМА

— Вопросы от Карла Сумманена: «Что делать, если после внедрения какого-либо ПО из Реестра, производитель этого ПО прекратил существование или перестал его развивать и поддерживать? В этом случае, согласно действующим требованиям, такое ПО должно быть исключено из реестра, после чего в отчётности показываться как не отечественное. На мой прямой вопрос Алексей Соколов¹ ответил, что придётся переходить на дру-

¹ Соколов Алексей Валерьевич — заместитель министра цифрового развития, связи и массовых коммуникаций Российской Федерации

гой продукт. Не слишком радостная перспектива, учитывая небольшой в среднем размер российских компаний и непростую экономическую ситуацию. Вопрос на обсуждение: Что может сделать государство, чтобы обеспечить длительный гарантированный период «активной» жизни ПО, включённого в Реестр?»

— Хороший вопрос. Тут речь, как я понимаю, в основном об операционных системах (ОС) — тема болезненная. Сейчас в Реестр включено около 45 ОС, но что такое отечественная операционная система? Как правило, это клон Linux, который немножечко «подпилен» и имеет русское название. Есть и проприетарные, но их мало.

Соответственно и поддержка для них должна быть разной. Для проприетарных нужна поддержка функционала и экосреды, чтобы писать приложения, т.к. операционная система определяется в первую очередь числом приложений. А что касается Linux-клонов, то тут мы и с Соколовым, и с Массухом² сходимся: нет резона их все поддерживать. Надо поддерживать самые продвинутые, где есть реальные команды разработки, методики, заделы, версияльность... А таких всего-то 5–7. Туда и пойдёт часть денег, которые удастся выбить из «Цифровой экономики» — на поддержку настоящих разработчиков, чтобы они не вымерли. Тогда, надеюсь, проблема и снимется.

ЧИСТКА РЕЕСТРА

— Причиной для изъятия ПО из Реестра может быть введение новых требований. Такие новые требования уже принимались. Были также случаи исключения ПО из отдельных классов в Реестре. Например, ОС Альт и ОС Астра, сертифицированные ФСТЭК по безопасности, были исключены из класса «средства защиты информации». Как вы прокомментируете такие случаи?

— Да, сейчас идёт чистка Реестра, т.к. в нём много ошибок. Поначалу очень торопились — Реестр должен был начать жить, а заявок приходило до 600

² Массух Илья Иссович — директор Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий (ЦКИКТ)

Трудно понять глубину импортозависимости, а производители пытаются пропихнуть своё ПО во все классы. Естественно, они не удовлетворятся классом «импортозависимое ПО», такой класс заказчикам не нужен. Поэтому в своё время такой подход и не был принят

штук за раз. В таких условиях не избежать ошибок.

Что касается ОС Альт и Astra Linux, они просто не туда попали. Это операционные системы, а не средства защиты информации, поэтому их и исключили из этого класса. Но из реестра их не изъяли. Хотя изъятий было много, в том числе и связанных с новыми правилами, согласно которым отечественное ПО должно поддерживать отечественные же СУБД. Хотели замахнуться и на «операционки», но отложили — сами разработчики просили этого не делать, потому что просто не успевают адаптировать свой софт под всё отечественное. Тем не менее, требования будут постепенно ужесточаться и дальше. Следующим шагом будет отечественная ОС. Потом — отечественный процессор.

ШАГ ЗА ШАГОМ

— Доля стопроцентно отечественного ПО довольно невелика. Практически любое отечественное ПО использует иностранные компоненты. Предложение на обсуждение: разрешить признание отечественным ПО российского происхождения, использующего зарубежные компоненты. Выделить его в реестре специальным признаком «импортозависимое ПО». Такой подход позволит обеспечить более плавное, поэтапное импортозамещение. Что мешает воплощению такого подхода?

— Этот подход многократно обсуждался. Тут засада в чём? Трудно понять глубину импортозависимости, а производители пытаются пропихнуть своё ПО во все классы. Естественно, они не удовлетворятся классом «импортозависимое ПО», такой класс заказчикам не нужен. Поэтому в своё время такой подход и не был принят.

ПРО РЫНОК И СОСЕДЕЙ

— Рынок в чистом виде — это довольно медленный эволюционный процесс с отсевом неудачных вариантов и постепенной монополизацией рынка выжившими особями. Для решения задачи импортозамещения рыночные процессы не годятся, т.к. во-первых, это медленно, а время у нас ограничено; во-вторых, это дорого из-за создания и отсева неудачных вариантов, а денег у нас немного. Предложение: подумать, что могут сделать государство и профильное профессиональное сообщество, чтобы скоординировать и ускорить процессы создания отечественного ПО? Возможно, нужна какая-то модель «регулируемого рынка»? Можно посмотреть на опыт наших соседей, которые нас немного обогнали. Как вы относитесь к такому подходу?

— Реестр — это и есть инструмент регулирования рынка. Просто нужно его совершенствовать и использовать с умом и для пользы дела.

А какие соседи имеются в виду?

— Китай, наверное.

— У китайцев своя история. Но с точки зрения импортозамещения, у них не всё так радужно, как нам кажется. Например, я знакома с их ситуацией с антивирусами. В государственный реестр там допущено пять антивирусных программ. Из них одна американская, одна российская, одна румынская и две китайских. Где тут, скажите, импортозамещение?

Но дружить с китайцами надо. Риски, конечно, есть, но... это другие риски.

— Спасибо.

Беседовал Игорь Некрасов

Валерий ХУРМАТУЛЛИН

кандидат экономических наук, член-корреспондент РАЕН

Андрей КОЛЕСНИКОВ

магистрант МАИ (национального исследовательского университета)

Дмитрий КОЛЕСНИКОВ

руководитель направления ПАО «Сбербанк»

Евгения КОЛЕСНИКОВА

студентка Института дополнительного образования СПбПУ Петра Великого



НА ОСНОВЕ ПАТЕНТОВ

ПРАКТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ АИС
УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ,
В ТОМ ЧИСЛЕ В БАНКОВСКОЙ СФЕРЕ

В статье приводится обзор и анализ автоматизированных информационных систем управления интеллектуальной собственностью (АИС УИС), выполненный на основе патентных документов. Приводится классификация АИС УИС по их функциональному назначению.

ВВЕДЕНИЕ

Характерной чертой сегодняшнего времени является широкое использование автоматизированных систем управления в различных сферах человеческой

деятельности. Особый интерес вызывает применение автоматизированных информационных систем управления результатами интеллектуальной деятельности в самых различных сферах — автоматизированных информационных систем управления интеллектуальной собственностью (АИС УИС). Интеллектуальная собственность выступает нематериальным активом в финансово-хозяйственной деятельности организаций, учреждений различных форм собственности. Понятие «интеллектуальная собственность», используемое в отечественной практике,

приводится в статье 1225 четвертой части Гражданского кодекса Российской Федерации. В целом, данное понятие совпадает с терминологией Всемирной организации интеллектуальной собственности. В обобщенном виде интеллектуальная собственность (ИС) может быть определена как система институтов исключительных прав, относящихся патентоспособным или регистрируемым в особом правовом порядке объектам, или к нерегистрируемым объектам, но охраняемым от незаконного копирования или присвоения.



Мировая практика использования АИС УИС, в том числе, в банковской сфере, представлена многочисленным классом такого вида и назначения систем.

Обзор и анализ патентных документов с описанием изобретений и полезных моделей различных АИС УИС производился по результатам патентного поиска. Полнотекстовый формализованный поиск производился в отечественных и зарубежных поисковых системах, в частности, системах «Информационные ресурсы ФГУ ФИПС свободного доступа и платные базы данных» и ru.espacenet.com. Поиск проводился по ключевым словам «интеллектуальная собственность» и «intellectual property», с ретроспективой поиска 2001–2019 гг.

КЛАССИФИКАЦИЯ ПРИМЕНЯЕМЫХ АИС УИС

В результате проведённого поиска выявлено 46 патентных документов — описания к патентам на изобретения и

полезные модели, описания к заявкам на изобретения. Выполненный анализ позволил разделить массив запатентованных АИС УИС на следующие группы:

- ◆ АИС УИС для целей инновационной деятельности;
- ◆ АИС УИС для целей анализа, обработки патентных документов;
- ◆ АИС УИС для целей оценки эффективности патентов;
- ◆ АИС УИС для целей патентной охраны и поддержания патентов в силе;
- ◆ АИС УИС для целей мониторинга правового статуса;
- ◆ АИС УИС для целей управления правами, уступки, передачи прав на ИС, лицензий;
- ◆ АИС УИС для целей коммерциализации;
- ◆ АИС УИС для банковских целей;
- ◆ АИС УИС для целей управления цифровой интеллектуальной ИС.

АИС УИС ДЛЯ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Описания технических решений к патентам на изобретения и полезные модели, которые используются, как основы инновационной деятельности предприятий и организаций приведены в [1–5, 16]. Данные системы УИС представляют собой автоматизированные системы обеспечения и управления процессами инновационной деятельности предприятий и организаций в самых различных сферах деятельности.

АИС УИС ДЛЯ АНАЛИЗА И ОБРАБОТКИ ПАТЕНТНЫХ ДОКУМЕНТОВ

АИС УИС, используемые в целях анализа, обработки патентных документов приведены в патентных документах [10, 12, 14, 17, 23, 26, 29, 32].

Данные автоматизированные системы осуществляют обработку и анализ патентных документов путём сопоставления аннотаций патентов, авторских прав, товарных знаков, лицензионных соглашений с заданными шаблонами запросов. В варианте осуществления системой такого рода обработки, анализатор интеллектуальной собственностью

подключает интерфейс, один или несколько информационный модулей — идентификатор, генератор отчетов, модуль связи.

АИС УИС ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПАТЕНТОВ

АИС УИС, используемые в целях анализа и оценки эффективности патентов, приводятся в патентных документах [8, 9, 11, 28, 31, 36].

Основное направление применения использования данного класса АИС УИС — прогнозирование эффективности внедрения изобретений в технические разработки. Это обеспечивается посредством сравнительного анализа частных относительных показателей эффективности внедрения изобретений и их обобщённых показателей за установленный период. По его результатам для формирования отчёта и аналитики производится расчёт индекса эффективности управления интеллектуальной собственностью. Предложения по управлению интеллектуальной собственностью основываются на информации об интеллектуальной собственности, хранящейся в системе. Расчёт вознаграждения или оплаты создателям и (или) правообладателям производится согласно показателям использования интеллектуальной собственности. Системы данного вида обеспечивают компьютерный способ оценки интеллектуальной собственности для целей лицензирования, уступки, дарения, а также определение стоимости нарушения.

АИС УИС ДЛЯ ПАТЕНТНОЙ ОХРАНЫ И ПОДДЕРЖАНИЯ ПАТЕНТОВ В СИЛЕ

АИС УИС, применяемые для целей патентной охраны и поддержания патентов в силе, приведены в [19, 22, 24, 25, 27, 28, 35, 38].

Основная задача такого вида АИС УИС — обеспечение патентной охраны и поддержание патентов в силе. Заявка на патент может быть подана в электронном виде в патентное ведомство. Такая процедура обеспечивает доступ к автоматическое отслеживание различных сроков действия патентов. Автоматизированная система управляет информацией, связанной с интел-

лектуальной собственностью и автоматизированными процессами защиты прав интеллектуальной собственности организации-заявителя. Различные пользователи, такие как изобретатели, бизнес-менеджеры и адвокаты по интеллектуальной собственности, могут в электронном виде создавать, совместно использовать связанные с патентами документы и хранить их в общей базе данных или репозитории.

АИС УИС ДЛЯ МОНИТОРИНГА ПРАВОВОГО СТАТУСА

АИС УИС для целей осуществления мониторинга правового статуса приведены в [17, 20, 21, 37].

АИС УИС данного класса осуществляют поддержку мониторинга правового состояния и управления правами интеллектуальной собственности. Такого вида АИС агрегируют и анализируют данные, относящиеся к владению активами в виде прав интеллектуальной собственности, и правовыми обременениями из соответствующих патентных ведомств. Они позволяют анализировать данные и осуществляют передачу данных в реестр интеллектуальной собственности. Заявитель или его представитель может отслеживать правовое состояние объекта интеллектуальной собственности и осуществлять такие операции, как внесение платы за поддержание в силе патентов, продление срока действия, налоговые и иные платежи.

АИС УИС ДЛЯ УПРАВЛЕНИЯ ПРАВАМИ

АИС УИС, применяемые для целей управления правами (уступки, передачи прав на ИС, лицензий), приведены в патентных документах [7, 39, 40, 41, 42, 45, 46].

АИС УИС данного класса позволяют аккумулировать информацию о правах на интеллектуальную собственность, о владельцах прав на интеллектуальную собственность и сохраняют агрегированную информацию на заранее определённом носителе (носителях).

Системы могут использоваться для предоставления пользователям сети информации об интеллектуальной собственности, их владельцах и обеспечивают передачу прав интеллекту-

альной собственности путём уступки, лицензии, франчайзинга. При этом, для подготовки лицензионных договоров рассчитываются такие платёжные показатели такие, как роялти.

АИС УИС ДЛЯ КОММЕРЦИАЛИЗАЦИИ

АИС УИС, используемые при коммерциализации интеллектуальной собственности приведены в источниках [6, 13, 15, 18, 33, 34, 43].

АИС УИС такого назначения являются системами, применяемыми для маркетинговых целей. Интеллектуальная собственность анализируется для определения маркетинговой оценки. По результатам принимается решение о том, продавать ли актив интеллектуальной собственности, основываясь, по крайней мере, на маркетинговой оценке. Если маркетинговая оценка соответствует заранее установленному порогу коммерческого спроса, то актив интеллектуальной собственности может быть предложен на рынке.

АИС УИС ДЛЯ БАНКОВ

АИС УИС, используемая для банковских целей, приведена в патентном документе [30].

АИС УИС данного назначения реализует способ и техническое решение, позволяющие принимать решение о возможности предоставления кредита с использованием дополнительно в качестве обеспечения нематериального актива в виде интеллектуальной собственности. Это позволит сделать такой кредит более привлекательным для кредитора. При этом осуществляется оценка значимости и жизнеспособности нематериального актива для определения соответствия актива и заявителя кредита минимальным квалификационным критериям.

Если это соответствие подтверждается, то проводится более подробный анализ, в котором приводятся выводы относительно различных факторов риска, связанных с историческим, текущим и перспективным состоянием рынка такого вида ИС. При этом, для применения данного вида актива также учитываются идентичные или смежные сегменты рынка, в которых планирует-

ся использовать ИС в качестве обеспечения кредита.

АИС УИС ДЛЯ УПРАВЛЕНИЯ ЦИФРОВОЙ ИС

АИС УИС, применяемая при управлении цифровой интеллектуальной собственностью, приведена в патентных документах [44, 45].

Системы для управления правами на цифровую интеллектуальную собственность основаны на адаптивном агенте, соответствующем цифровому контенту. Способы его предоставления предназначены для гибкой защиты цифрового контента и точного управления цифровым контентом в соответствии с со статусом правообладателей и потребностями пользователей.

* * *

Резюмируя, можно сделать вывод, что выполненный обзор и проведённый анализ автоматизированных информационных систем управления интеллектуальной собственностью показывают развивающуюся в настоящее время тенденцию автоматизации процессов, связанных с созданием интеллектуальной собственности, регистрацией прав на интеллектуальную собственность, приобретением и предоставлением прав на интеллектуальную собственность, коммерциализацией интеллектуальной собственности в качестве нематериального актива. Следует отметить, что данный массив патентных документов является выборочным. Он не в полной мере показывает возможность широкого применения автоматизированных информационных систем управления интеллектуальной собственностью в такой сфере, как банковская. Предполагается, что в перспективе в ближайшем будущем собственно «банковская» интеллектуальная собственность, являющаяся достаточно специфичной категорией интеллектуальной собственности, будет создаваться, охраняться и использоваться с повсеместным применением автоматизированных информационных систем управления интеллектуальной собственностью.

СПИСОК ПАТЕНТНЫХ ДОКУМЕНТОВ

1. Патент РФ на изобретение № 2638773 «Система управления направленностью и внедрением интеллектуальной собственности». МПК G06F 17/00 (2006.01), опубликовано 12.2017 г. Бюл. № 35.
2. Патент РФ на изобретение № 2602972 «Система для управления интеллектуальными ресурсами предприятия». МПК G06F17/00 (2006.01), G06Q10/06 (2006.01), опубликовано 20.11.2016 г. Бюл. №
3. Патент РФ на изобретение № 2601135 «Устройство для управления интеллектуальными ресурсами предприятия». МПК G06F17/00 (2006.01), G06Q10/06 (2006.01), опубликовано 10.2016 г. Бюл. № 30.
4. Патент РФ на изобретение № 2578798 «Система управления процессом направленностью и внедрением интеллектуальной собственности». МПК G06F17/00 (2006.01), опубликовано 03.2016 г. Бюл. № 9.
5. Патент РФ на изобретение № 2569574 «Информационно-аналитическое устройство управления эффективностью инновационного развития предприятия». МПК H04B17/00 (2015.01), опубликовано 2015 г. Бюл. № 33.
6. Патент РФ на полезную модель № 108175 «Конкурсно-ориентированная система выявления, регистрации и продвижения на рынок результатов интеллектуальной деятельности». МПК G06Q30/06 (2006.01), G05BQ15/00 (2006.01), опубликовано 10.9.2011 г. Бюл. № 25.
7. Патент РФ на изобретение № 2355023 «Способ поддержки создания интеллектуальной собственности с помощью кооперативной системой управления интеллектуальной собственностью, система поставки информации с функцией управления сублицензией и компьютерная программа». МПК G06F12/14 (2006.01), опубликовано 10.05.2009 Бюл. № 13, публикация РСТ: WO 2005/114510 (01.12.2005).
8. Заявка на изобретение № RU 2009120227 (A) «Способ прогнозирования эффективности внедрения изобретения в технические разработки». МПК G06F17/00 (2006.01), публикация заявки 10.2010.
9. Патент WO2016157214 (A1) «Intellectual property management system and tool». МПК G06F17/00, G06F9/06, G06F9/44, опубликовано 2016-10-06.
10. Патент KR 20150114142 (A) «Apparatus and method for analyzing intellectual property». МПК G06F17/00, G06F9/06, G06F9/44, опубликовано 2015-10-12.
11. Патент CN 103098045 (A) «Intellectual property scoring platform». МПК G06F17/00, G06F17/30, опубликовано 2013-05-08.
12. Патент US 2013047066 (A1) «Method and system for annotation and/or linking documents and data for intellectual property management». МПК G06F17/00, G06Q10/10, опубликовано 2013-02-21.
13. Патент US 2013041803 (A1) «Method for aggregating and valuing intellectual property in an exchange». МПК G06Q40/04, опубликовано 2013-02-14.
14. Патент WO2011136413 (A1) «Apparatus and method for configuring a comprehensive intellectual property rights star network by detecting patent similitude». МПК G06F17/00, G06Q50/00, опубликовано 2011-11-03.
15. Патент TW201025156 (A) «Intellectual property management method and intellectual property bank system». МПК G06F17/00, G06Q30/00, опубликовано 2010-07-01.
16. Патент TW200834436 (A) «Intellectual property service systems». МПК G06F17/00, G06Q10/00, опубликовано 2008-08-16.
17. Патент US 2011072518 (A1) «Automated screening of content based on intellectual property rights». МПК G06F17/00, опубликовано 2011-03-24.
18. Патент CN 101861586 (A) «Aggregation, analysis, and presentation of intellectual property and financial information». МПК G06F17/00, опубликовано 2010-10-13.
19. Патент US 2009327005 (A1) «Systems and method for preparation of an intellectual property filing in accordance with jurisdiction- and/or agent-specific requirements». МПК G06F15/16, G06F17/00, G06Q10/00, опубликовано 2009-12-31.
20. Патент US 2009164278 (A1) «System for reducing risk of maintaining intellectual property» МПК G06F17/00, G06Q40/00, опубликовано 2009-06-25.
21. Патент US 2009030713 (A1) «System and method of reviewing ownership of and encumbrances on intellectual property assets». МПК G06F17/00, G06F17/30, G06F7/10, опубликовано 2009-01-29.
22. Патент US 2008294683 (A1) «Systems and methods for managing intellectual property». МПК G06F17/00, G06Q10/00, опубликовано 2008-11-27.
23. Патент WO2011136413 (A1) «Intellectual property notes-based commenting system». МПК G06F17/00, опубликовано 2011-11-03.
24. Патент WO2008127340 (A1) «Intellectual property application drafting, preparation, and submission tools». МПК G06F15/00, G06F17/00, G06F17/30, опубликовано 2008-10-23.
25. Патент WO2007079313 (A2) «Intellectual property portfolio management method and system». МПК G06F17/00, опубликовано 2008-05-15.
26. Патент WO2006110832 (A2) «System for extracting relevant data from an intellectual database». МПК G06F17/00, опубликовано 2008-03-08.
27. Патент US 2008040356 (A1) «Web site automating transfer of intellectual property». МПК G06F17/00, G06Q10/00, опубликовано 2008-02-14.
28. Патент US 2003197054 (A1) «Intellectual property identification and recording system». МПК G03G21/02, G06F17/16, опубликовано 2003-10-23.
29. Патент US 2007078886 (A1) «Intellectual property assets manager (IPAM) for context processing of data objects». МПК G06F17/00, G06F17/30, опубликовано 2007-04-05.
30. Патент US 6330547 (B1) «Method and apparatus for establishing and enhancing the creditworthiness of intellectual property». МПК G06Q40/00, G06Q40/08, опубликовано 2001-12-11.
31. Патент US 2004122841 (A1) «Method and system for evaluating intellectual property». МПК G06F17/00, G06F7/00, опубликовано 2004-06-24.
32. Патент US 2002138297 (A1) «Apparatus for and method of analyzing intellectual property information». МПК G06Q10/10, G06Q50/18, опубликовано 2002-09-26.
33. Патент US 2008154682 (A1) «System and method for developing and implementing intellectual property marketing». МПК G06Q10/10, G06Q50/18, опубликовано 2008-06-26.
34. Патент WO 0239291 (A1) «Intellectual property commercialization method». МПК G06Q10/10, G06F17/00, G06F13/00, опубликовано 2002-05-16.
35. Патент WO 0193081 (A2) «Computer-implemented method for securing intellectual property». МПК G06Q10/10, G06Q50/18, G06F17/00, опубликовано 2001-12-06.
36. Патент WO 0152097 (A2) «Method of repeatedly securitizing intellectual property assets and facilitating investment therein». МПК G06Q10/10, G06Q40/00, опубликовано 2001-07-19.
37. Патент WO 0124035 (A2) «Fee transaction system and method for intellectual property acquisition and/or maintenance». МПК G06F17/00, G06Q50/18, опубликовано 2001-04-05.
38. Патент WO 0108031 (A2) «Electronic intellectual property management system». МПК G06F17/30, G06Q10/00, опубликовано 2001-02-01.
39. Патент WO 0102987 (A2) «Web-based intermediary for intellectual property transfer». МПК G06F17/30, G06Q30/00, опубликовано 2001-01-11.
40. Патент KR 20080033050 (A) «Server for utilizing intellectual property rights». МПК G06F17/00, опубликовано 2008-04-16.
41. Патент KR 20080033041 (A) «Method for utilizing intellectual property rights». МПК G06F17/00, опубликовано 2008-04-16.
42. Патент KR 20080033030 (A) «System and method for utilizing intellectual property rights and program recording medium». МПК G06F17/00, G06Q99/00, опубликовано 2008-04-16.
43. Патент KR 20070103885 (A) «Intellectual property management system». МПК G06F17/00, G06Q30/00, опубликовано 2007-10-25.
44. Патент KR 20030051376 (A) «System for managing digital intellectual property rights based on adaptive agent corresponding to digital contents and method thereof». МПК G06F17/00, опубликовано 2003-06-25.
45. Патент KR 20030092964 (A) «Method for displaying data related to intellectual property of multimedia contents». МПК G06F17/00, опубликовано 2003-12-06.
46. Патент WO 0237304 (A2) «Methods and systems for intellectual property management». МПК G06Q10/00, G06F17/00, опубликовано 2002-05-10.

ВАЖНАЯ ТЕМА

ПОВЫШЕНИЕ ОСВЕДОМЛЁННОСТИ КАК МЕТОД
ОБЕСПЕЧЕНИЯ ИБ НЕ ДОЛЖЕН БЫТЬ ВТОРОСТЕПЕННЫМ
В СРАВНЕНИИ С ТЕХНИЧЕСКИМИ МЕТОДАМИ

16 сентября Банк России опубликовал «Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов». Что говорить: документ концептуальный, комплексный, где-то спорный (например, насколько намерение Банка России стать «связующим звеном ... для создания условий подготовки специалистов в области ИБ нового типа» является профильным и посильным). Документ, по моему мнению, запоздавший лет на 5–7, но, тем не менее, очень нужный — систематизирующий и, как говорится, придающий новые стимулы.

ПРОБЕЛЫ, ПРОБЕЛЫ...

В данной заметке хотелось бы кратко прокомментировать «Основные направления» с точки зрения близкой мне проблематики повышения осведомлённости в области ИБ, её текущего состояния и возможного развития в свете вышедшего документа. Поскольку в том, что документ задал направления перспективного развития ИБ не только в финансовой сфере, но и в целом в РФ, сомневаться не приходится. При этом здесь я имею в виду повышение осведомлённости в самом широком прикладном смысле — применительно и к персоналу организаций, и к клиентам, и даже к населению страны (для чего чаще используются термины «повышение киберграмотности» и «повышение кибергигиены»).

Проблематика повышения осведомлённости сегодня в нашей стране, по большей части, характеризуется пробелами в её методологическом и методическом аспектах: необходимость повышения осведомлённости вопросов уже не вызывает, слово «геймификация»

знают почти все, некоторые даже научились рисовать правильные «весёлые картинки» для игр с курсами-тестами. А вот как это всё применять так, чтобы повышение не было формальностью или/и статьёй трудно обосновываемых затрат — тут пока каждый действует как понимает и как может. При том, что ощутимый на практике эффект от повышения осведомлённости можно ожидать только при правильном планировании мероприятий. Причём, с учётом специфики организации, с последующей ресурсообеспеченной реализацией непрерывного процесса работы с людьми и корректировками одного процесса на основе обратной связи. Можно и не усложнять, можно и «без этого» — конечно, если вас не интересует результат.

Однако, вернёмся к обсуждаемому документу...

НЕТ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ!

Во введении «Основных направлений» декларируются цели и задачи развития ИБ и киберустойчивости — обеспечение ИБ, киберустойчивости, операционной надёжности и непрерывности деятельности организаций финансового рынка, противодействие компьютерным атакам, защита прав потребителей финансовых услуг. Нет сомнений в том, что повышение осведомлённости как метод обеспечения ИБ способно внести весомый вклад в достижение каждой из этих целей, а потому считать его второстепенным в сравнении с техническими методами обеспечения ИБ — серьёзное упущение.

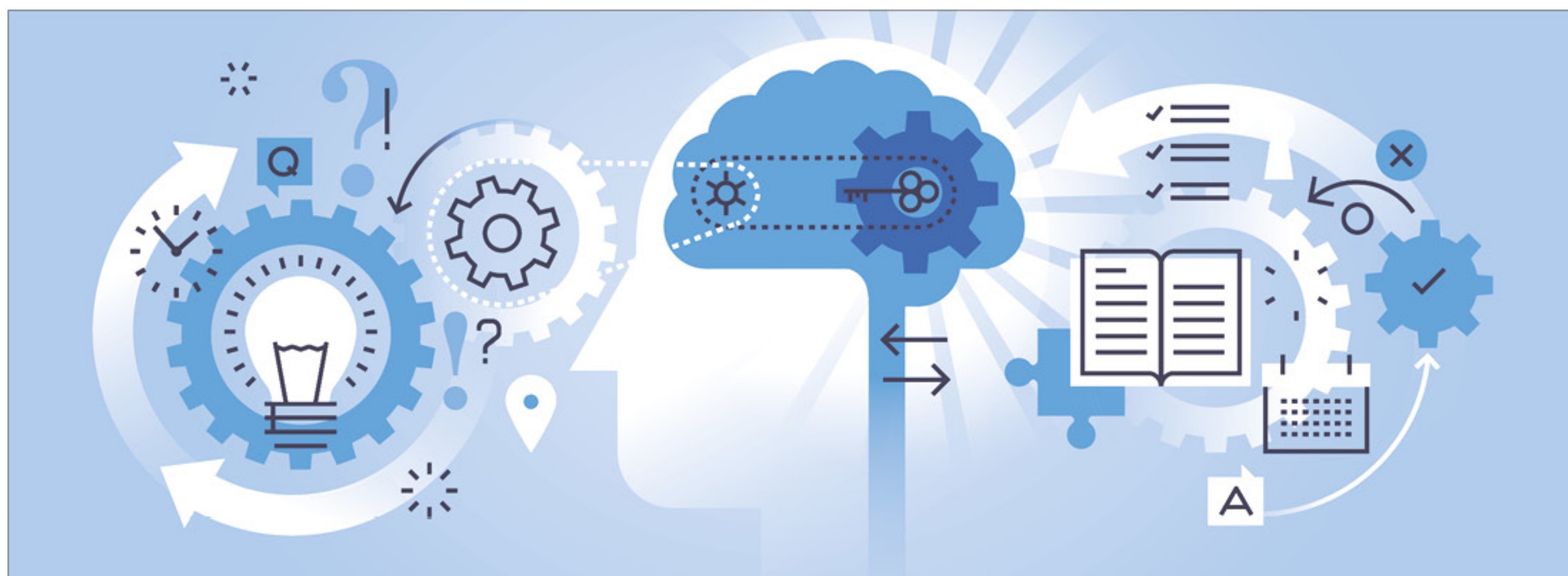
Далее, в «Основных направлениях» говорится о том, что Банк России «...разрабатывает методологию и обеспечивает развитие ИБ ... по следующим основным направлениям:

1) Стандартизация... разработка стандартов (включая разработку ГОСТ) в области ИБ и киберустойчивости <...>

6) Создание условий для развития культуры ИБ и кибергигиены в кредитно-финансовой сфере».

Необходимо отметить отсутствие в РФ в настоящее время какого-либо нормативного регулирования повышения осведомлённости —

Необходимо отметить отсутствие в РФ в настоящее время какого-либо нормативного регулирования повышения осведомлённости — ни стандарта, ни методических рекомендаций, ни «лучших практик» пока нет



ни стандарта, ни методических рекомендаций, ни «лучших практик» пока нет. А оно нужно — и в силу актуальности темы, и в силу прямой зависимости результатов повышения от того, как и кем оно выполняется. Потому видится уместной разработка стандарта либо методических рекомендаций по повышению осведомлённости в области ИБ (киберграмотности) с привлечением профильных государственных органов и экспертного сообщества. За основу можно, например, взять адаптированный перевод американского стандарта NIST SP 800–50, разработанного в далёком 2003 году и успешно используемого до сих пор как в мире, так и у нас.

УРОВЕНЬ ЧЕЛОВЕКА-ПОЛЬЗОВАТЕЛЯ, АУ!

Досадно видеть, что далее в «Основных направлениях» под общим принципом ИБ и киберустойчивости организаций кредитно-финансовой сферы понимается реализация ИБ на трёх уровнях — инфраструктурном, уровне приложений и уровне технологий обработки данных. И совершенно забыт уровень человека-пользователя! На каком уровне будут создаваться вышеупомянутые условия для развития культуры ИБ и кибергигиены — на инфраструктурном или на уровне технологий обработки данных?

Некоторое утешение вызывает приведённое в главе «Подготовка кадров и обеспечение доверия граждан к цифровой среде» намерение «...сформировать направления обучения и разработать соответствующие программы обучения:

- ♦ разработать профессиональный стандарт «Специалист в области ИБ организаций кредитно-финансовой сферы»;
- ♦ разработать примерную программу профессиональной переподготовки «Обеспечение ИБ в организациях кредитно-финансовой сферы».

ХОЧЕТСЯ НАДЕЯТЬСЯ

Хочется надеяться, что необходимость учёта «человеческого фактора» при обеспечении ИБ и основные принципы разработки эффективных программ повышения осведомлённости в данных разработках не будут забыты.

«Департамент ИБ является информационно-координационным хабом процессов и мероприятий по повышению финансовой киберграмотности населения и привлекает для решения этой задачи другие структурные подразделения Банка России, участников рынка, а также профильные федеральные органы исполнительной власти...» — потребность в определении курирующего тему повышения осведомлённости (пусть, для начала, хотя бы в части финансовой киберграмотности) органа, способного направлять и координировать развитие методолого-методического аспекта повышения на уровне отрасли, ощущается вполне явственно. Возможно, за этим последует и формирование соответствующей рабочей группы. Хочется надеяться, не только с привлечением «теоретиков», но и «практиков» — тех немногочисленных специалистов, кто имеет практический опыт разработки методологически обоснованных комплексных программ повышения осведомлённости для крупных корпоративных клиентов и государственных учреждений и организаций.

В заключение хотелось бы выразить надежду, что изложенные в «Основных направлениях» тезисы получают продолжение в виде конкретных своевременных тактических шагов, в том числе, и в части систематизации и формализации принципов создания эффективных программ повышения осведомлённости/киберграмотности.



**Марина
БРОДСКАЯ**
обозреватель
BIS Journal

«ЛУЧШЕ ПОЗДНО, ЧЕМ НИКОГДА»

ПАРАДОКСЫ НАШИХ СМИ

После Осенней сессии Уральского форума, прошедшей в сентябре, новостные полосы интернет- и печатных СМИ заполнили цитаты из выступления заместителя начальника Департамента ИБ Банка России Артема Сычева. Он всего лишь сообщил, что число случаев мошенничества, когда злоумышленники завладевают средствами пользователей социальных сетей через их аккаунты, заметно выросло. А какие события из сферы ИБ помимо кражи личных данных волнуют СМИ и их читателей?

СМИ СВОЮ РАБОТУ ДЕЛАЮТ

Для начала вернёмся к новости, распространённой по итогам Осенней сессии Уральского форума. Артем Сычев сообщил, что число случаев интернет-мошенничества, когда злоумышленники завладевают средствами пользователей социальных сетей с помощью захвата их аккаунтов, заметно выросло. Получив доступ к чужой странице, злоумышленник начинает публиковать посты и писать сообщения от имени жертвы с просьбой о помощи и переводе денег. Также преступники «разводят» своих жертв при помощи методов социальной инженерии, вводя их в заблуждение и вынуждая добровольно предоставить доступ к имеющимся средствам. Главная цель злоумышленников — создать стрессовую ситуацию, в которой человеку будет сложно мыслить рационально, — рассказал А. Сычев.

Разные массовые издания тут же отреагировали и стали распространять рекомендации. Например, чтобы максимально обезопасить себя от возможных взломов аккаунтов и хакерских атак, советуем придерживаться следующих правил:

- ♦ устанавливайте программы только из официальных источников;
- ♦ регулярно проверяйте устройства антивирусной программой;
- ♦ не пользуйтесь общественными Wi-Fi сетями или настройте на устройстве VPN, что минимизирует риск перехвата данных;
- ♦ регулярно меняйте пароли и используйте двухфакторную аутентификацию...

Советы, несомненно, правильные. Вот только, насколько кража личности актуальна для тех, кто эти правила соблюдает или вообще живёт вне соцсетей?

КЛЮЧ ОТ КВАРТИРЫ, ГДЕ ДЕНЬГИ ЛЕЖАТ

«Я не покажу вам свой паспорт, а то подпишусь, а вы квартиру украдёте, по телевизору рассказывали», — примерно такой отказ не раз слышали в Москве волонтеры, собиравшие подписи за выдвижение кандидатов в Мосгордуму. Пост в одной из социальных сетей о том, как квартиру сотрудника федеральной телекомпании «подарили» совершенно постороннему человеку с помощью электронной цифровой подписи (ЭЦП), быстро трансформировался в репортаж в вечерних новостях и слухи агентства ОБС.

Тот факт, что в квартиру любой потенциальной жертвы чуть ли не ежедневно звонят или пытаются попасть представители всевозможных поверочных и обслуживающих контор, большинство пенсионеров не волнует. Многие впускают посторонних в своё жильё и легко расстаются с крупными суммами денег за копеечную вещь. Базы данных с обновлёнными сведениями о проверке счётчиков регулярно поступают заинтересованным организациям, «врачи-кардиологи» и «вертебрологи» толпами стоят в подъездах в ожидании открытия двери после звонка из «регистратуры». Парадоксально, но утечка данных через сотрудников поликлиник, МФЦ, социальных служб или близких к ним структур, правоохранительные органы не беспокоит. Если следить за новостями, то поимки банды мошенников, сливших на сторону сведения о лицевых счётах или адресах горожан, не случилось ни разу. Значит, такой поимки и не было — СМИ не пропустили бы сенсацию.

Ещё парадокс, замеченный газетами. При официальном обращении в центр «Мои документы» получить сведения о проживавших некогда в квартире гражданах невозможно — действует Закон о персональных данных, он защищает от родственников даже покойников, скончавшихся за полвека до принятия норматива. Однако, всего за 2–2,5 тыс. руб. желающие могут купить любую выписку через интернет.

Скандал с «дарением» квартиры в Москве жителю дальнего региона и тот факт, что пострадавший работает на центральном телевидении, заставил законодателей в срочном порядке принять поправки к закону об электронной цифровой подписи и юридически закрыть найденную уязвимость. А в суде по возврату квартиры законному владельцу не всё так однозначно, — рассказывают источники, близкие к судебному процессу. Истец по-прежнему не является хозяином собственной квартиры. Возможно, бдительность москвича позволила оперативно прикрыть лазейку в операциях с недвижимостью с помощью ЭЦП. Возможно, по итогам суда, что-то изменится и в деятельности удостоверяющих центров.

ПРИВЕТ ИЗ НИГЕРИИ

Казалось бы, с момента массовой рассылки «нигерийских писем» по электронной почте, начавшейся в середине 1980-х гг. прошло больше тридцати лет. За это время выросло не одно поколение адресатов, которым обещали большой процент от прибыли в многомиллионных денежных операциях или помощь в получении наследства от внезапно скончавшегося где-то в Африке одинокого долларового миллионера с русской фамилией, так удачно совпавшей с фамилией адресата. Для того, чтобы стать наследником такого дядюшки, юрист/нотариус просит указать малость — номер банковского счёта или карты для перевода средств. Сколько людей повелось на этот трюк, распространённый ещё до появления электронной почты, доподлинно неизвестно. Однако на другую вариацию африканских (и теперь азиатских) проходимцев, почему-то попались многие соотечественники.

Недавно газета «Коммерсант» сообщила об отмене Верховного суда РФ пересматривать обвинительный приговор брачному аферисту, уроженцу Нигерии Олугбенгу Банколе. Он «сватал» состоятельных одиноких москвичек за «уходящего в отставку офицера армии США», роль которого играл гражданин Ганы. Желающих выйти замуж за «американского полковника» оказалось больше сотни, для «работы» с каждой «невестой» открывался персональный счёт, на который мошенники просили перевести деньги за помощь при доставке подарков от «жениха», «растаможку» или просто как подтверждение намерений вести совместное хозяйство. Тверской районный суд признал афророссиянина виновным в девяти эпизодах мошенничества в составе группы на общую сумму чуть более 3,5 млн руб. Сколько пострадавших не обратились в полицию, неизвестно.

Со временем «нигерийские» письма трансформировались, и сегодня папка «спам» в моей почте полна сообщений о перечислении мне пятизначных сумм от неизвестных лиц с единственной просьбой: перейти по ссылке в письме и указать номер карты для перевода...

У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН

Примерно треть россиян сталкивалась с телефонным мошенничеством лично или это случилось с их близкими, говорится в очередном исследовании «Лаборатории Касперского». Около 9% опрошенных потеряли таким образом значительную сумму. И только 4% обратились в правоохранительные органы.

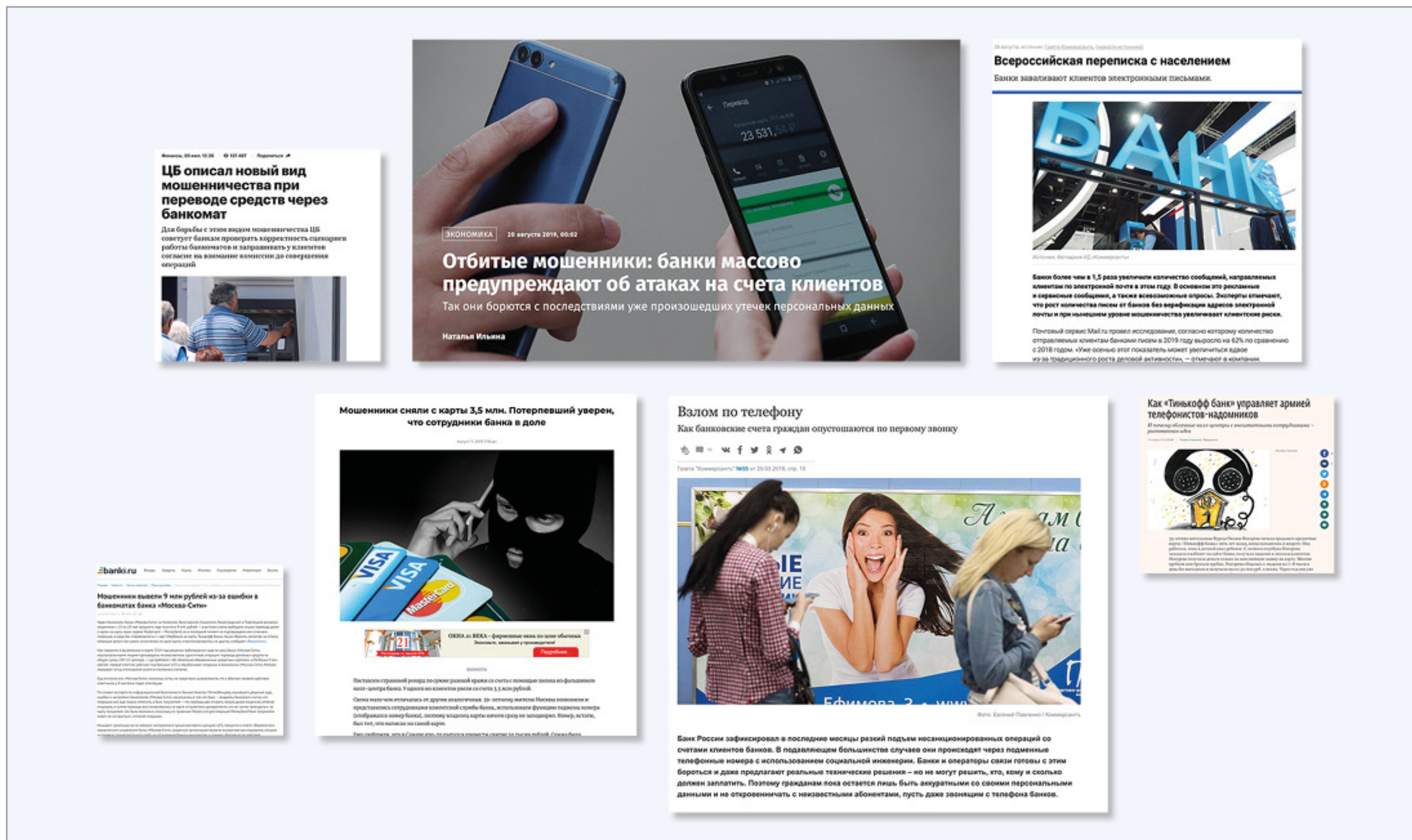
Как уже писалось выше, «горячие» и «холодные» телефонные звонки от менеджеров по продажам всего и вся, обзвон горожан операторами сервисных центров по краденным БД даёт мошенникам хорошую прибыль — иначе бизнес заглох бы сам по себе. Но апогеем стали звонки от имени служб безопасности крупных банков с использованием методов социальной инженерии.

Этот вид преступлений хорошо психологически просчитан. Эффект внезапности, служба безопасности, обращение по имени-отчеству, деньги, которые у вас хотят украсть... И телефонный номер, похожий на номер банка, где эти деньги лежат. Эпидемия такого мошенничества началась в конце 2018 г. Несмотря на усилия ЦБ и самих банков, которые регулярно сообщают о закрытии уязвимостей, заметки о мошеннических звонках от имени финансовых организаций в СМИ появляются регулярно.

Какие советы и разъяснения по этому поводу дают популярные в России СМИ, например, «Комсомольская правда»? Оставаться хладнокровными и не вестись на угрозы мошенников. Взять паузу, перезвонить в банк и заблокировать карту, сообщив о происшествии в службу безопасности.

Кстати, бдительность и подозрительность клиентов банков, а также работа сотрудников отделов ИБ привели к тому, что на чёрном рынке цены на выписки по счёту клиента выросли за 9 месяцев этого года с 2 тыс. до 15 тыс. руб. Эти данные привёл «Коммерсантъ» со ссылкой на исследование компании DeviceLock. На рынке появилась и новая услуга — продажа адресов банкоматов, которыми пользовался клиент банка в течение месяца. Перечень банкоматов, популярных у конкретного клиента, можно приобрести за 8–15 тыс. руб.

Как отмечает издание, «число банков, о чьих клиентах злоумышленники хотят узнать по-



больше, сократилось. Мошенникам интересны прежде всего крупные кредитные организации с большой базой, в идеале — с большим количеством премиальных клиентов с дебетовыми картами... В ЦБ признали проблему, но заявили, что рост цен на подобные услуги свидетельствует об эффективности мер по противодействию утечкам: злоумышленникам стало сложнее получать информацию».

По данным «Лаборатории Касперского», 21 % пользователей не защищают свой телефон от подозрительных звонков; 51 % не берут трубку, если видят неизвестный номер; 37 % используют «чёрный список», а 17 % — специализированное ПО.

ТЕЛЕГРАММА ОТ ЗАПРЕЩЁННОГО TELEGRAM

Больше всего информации о хакерах, мошенниках и методах их работы есть в запрещённом в России мессенджере Telegram. Телеграм-каналы часто пользуются той же информацией, что и официальные СМИ, но не связаны вопросами корпоративной этики.

Порой то в одном, то в другом телеграм-канале, среди прочего, мелькает информация о продаже некой БД «в одни руки, обращаться к админу», кто-то запускает учебный курс по методам взлома онлайн-казино или даёт актуальный алгоритм получения прибыли, работа-

ющий до того момента, пока администраторы ресурса не поймут, что у них нашли очередную уязвимость.

А кто-то остаётся на «белой» стороне и просто рассказывает о ситуации в мире ИБ. Например, один из популярных финансовых телеграм-каналов за 2,5 года опубликовал порядка 130 сообщений на тему мошенничества. В 2017–2018 гг. он писал о мошенниках и схемах обмана граждан в реальном мире, в 2019 г. уделяет внимание «проделкам» в интернете и банковской сфере. Главное достоинство таких каналов — оперативность и краткость в изложении информации.

О ЧЁМ СООБЩАЮТ...

Пролистывая новостную ленту, можно узнать (или вспомнить) как:

- ♦ На Новый год мошенники, найдя дыру в механизме модерации Google Ads, использовали e-mail рассылки с логотипами крупных банков. На каждом из этапов мошеннического опроса требовали выплат. Пострадали сотни наивных.

- ♦ Выявлен очередной победитель аферы. Житель Омска выложил за свою глупость 75 тыс. руб. Он осуществил 11 переводов, первый на 168 рублей, суммы остальных увеличивались с каждым разом.

- ♦ После разгрома тюремного колл-центра Сбербанка мошенники организовали новый тюремный колл-центр. На этот раз ВТБ. Во вре-

мя звонка включается фоновая музыка с шумом офиса.

♦ Мошенники при звонках потенциальным жертвам стали чаще использовать технологию подмены телефонного номера банка. Клиенту сообщают о попытке несанкционированного списания средств, называют его ФИО, номер паспорта, остаток по счёту и даже последнее транзакции. Сбитые с толку клиенты сообщают данные SMS злоумышленникам и теряют деньги. Для совершения подобных звонков злоумышленники используют IP-телефонию.

♦ У звонарей из тюремных колл-центров есть не только данные клиентов банков, но и информация о банкстерах... Схема обмана многоступенчатая. В итоге мошенникам удалось убедить жертву предоставить данные карт и похитить 800 тыс. руб.

♦ Мошенники вывели из банкоматов банка «Москва-сити» на вокзалах Москвы 9 млн руб. (\$ 134 122). Ошибка в настройках: банк — владелец банкомата считал, что операцию всё ещё можно отменить, а банк получателя — что перевод уже отозвать нельзя.

♦ Центробанк сообщил о новом виде мошенничества. Он основан на несовершенстве обработки переводов с карты на карту в банкоматах (эта новость вышла спустя некоторое время после предыдущей).

♦ Банкстеры годами учили клиентов никогда не называть сотрудникам банка коды из смс-сообщений, а теперь начали требовать данные для идентификации в колл-центрах. Формируется удобный для мошенников шаблон поведения: сотрудник банка может запросить код из СМС, и это нормально — это нужно для выполнения операции. Точно также поступают и мошенники.

♦ Поставлен рекорд страны по сумме разовой кражи со счёта с помощью звонка из фальшивого колл-центра. У одного из клиентов увели со счёта 3,5 млн рублей.

♦ Участились случаи использования мошенниками роботов для получения кода подтверждения операции по банковской карте из СМС в Сбербанке и ВТБ. В августе таким образом одна из жертв лишилась 3 млн руб.

ПРИЯТНЫЕ НОВОСТИ

Публикуются и отчёты компаний, работающих в сфере ИБ, и сообщения о достижениях. Так, технология Liveness компьютерного зрения VisionLabs, входящая в экосистему Сбербанка, признана экспертами лучшей в международном конкурсе ChaLearn Face Anti-spoofing Attack Detection Challenge на крупнейшей и главной международной конференции для разработчиков компьютерного зрения CVPR-2019...

СОЦИАЛЬНЫЕ СЕТИ И ДЕЛОВЫЕ ИЗДАНИЯ

В соцсетях, о краже аккаунтов в которых так обеспокоен ЦБ, чаще всего и обсуждаются случаи мошенничества и методы работы мошенников. Автор последнего поста на тему подменного звонка, который попался мне в Facebook, интересовалась, почему после ответа «оператору», что отделение банка рядом, и она сама сходит проверить счёт, её оставили в покое. А всё просто: разговор пошёл не по заданному сценарию, и «помощь в спасении средств со счёта» ей явно не требовалась. Другой пользователь делился эмоциями после реакции на том конце трубки, когда названные им номер карты и CVV не сработали.

Чаще всего в группах и местных сообществах обсуждают и просят предупредить пожилых родственников о подозрительных звонках с поверками счётчиков, поквартирных обходах неизвестных личностей с корочками липовых ООО, делятся информацией о квартирных и автомобильных кражах в районе — информирован, значит предупреждён. А призывы о помощи и сборе средств в пользу того или иного участника сообщества чаще всего проходят тщательную проверку: опыт сборов «на лечение» в сообществе из 30 тыс. человек или предложения скинуться «на корм и лечение» кошечкам заставил многих внимательно относиться к тем, кто собирает «пожертвования». Многие группы напрямую работают с благотворительными фондами и рекомендуют проводить все сборы через них.

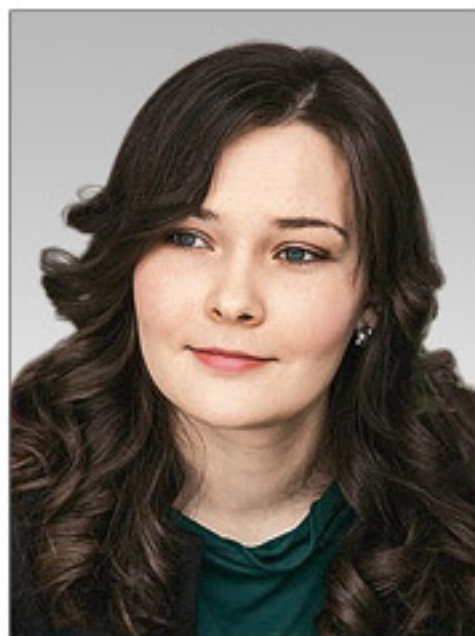
В деловых изданиях всё совсем по-другому. «Коммерсант», «Ведомости» и «РБК» чаще других пишут об ИБ. Здесь даются и аналитические статьи, и отчёты с профильных мероприятий с комментариями экспертов. Информация чаще носит сугубо прикладной характер и не интересна большинству читателей-обывателей.

* * *

«Конечно, рядовой россиянин может решить, что всякие хакерские хитрости ему знать не обязательно. Но это может дорого, в буквальном смысле, ему обойтись. Зачастую, гражданин даже не будет вникать в высокие технологии, действуя на эмоциях и перечисляя деньги мошенникам. Психология обывателя не сильно изменилась за последние годы, — пишут «Ведомости», и сложно с ними не согласиться. — Интересно, что вопрос безопасности не банков, а простых людей был поднят только сейчас, когда жулики действуют на данном поприще уже не первый год. Но лучше проявить бдительность поздно, чем никогда».



**Сергей
ВОЛДОХИН**
сооснователь и директор
ООО «Антифишинг»



**Ольга
ЛИМОНОВА**
психолог
ООО «Антифишинг»



**Андрей
ЖАРКЕВИЧ**
редактор
ООО «Антифишинг»

ПСИХОЛОГИЯ ЦИФРОВЫХ АТАК

ПОЧЕМУ КИБЕРАТАКИ ПРОТИВ ЛЮДЕЙ ТАК ЭФФЕКТИВНЫ

Как ни печально признавать, в борьбе людей и технических средств победили люди. Даже лучшие файерволы не всегда справляются с защитой корпоративных сетей, если атака направлена против сотрудника и активно эксплуатирует особенности человеческой психики. Защита беспомощно наблюдает за тем, как очередной пользователь передаёт свой логин и пароль злоумышленникам или вставляет заражённую флешку в USB-порт. Современные киберпреступники всё реже взламывают компьютеры, потому что гораздо эффективнее взламывать людей.

Объединение цифровых технологий и социальной инженерии породило новую разновидность кибератак — *цифровые атаки на людей*. Они отличаются от привычных хакерских нападений тем, что решающее значение в них имеет психологический аспект, а не уязвимости программ, операционных систем и оборудования.

Цифровые атаки на сотрудников относительно просты в реализации, но эффективны и приносят мошенникам серьёзный доход. Например, преступная группировка Silence атакует банки в 25 странах мира с помощью фишинга, используя электронные письма. По данным Group IB, только подтверждённый ущерб от деятельности Silence по состоянию на сентябрь 2018 года составил 52 млн рублей.

С 16 по 18 января 2019 года Silence запустила очередную кампанию против российских банков, в ходе которой только Сбербанк получил свыше полутора тысяч фишинговых писем. Особенностью этой атаки стала более качественная социальная инженерия. Осознав высокую результативность цифровых атак на людей, преступники сместили акцент с инструментальных средств на психологическую составляющую.

Существующая литература в области информационной безопасности не даёт полного понимания влияния личностных черт на поведение сотрудников при столкновении с цифровыми атаками, поэтому разработка и внедрение психологической модели, объясняющей манипулятивное воздействие киберпреступников на пользователей, является важнейшим направлением работы организационной кибербезопасности, дающим универсальный инструмент для обучения методам обнаружения цифровых атак.

Существующая литература в области информационной безопасности не даёт полного понимания влияния личностных черт на поведение сотрудников при столкновении с цифровыми атаками

ФАКТОРЫ КРИМИНАЛЬНОГО МАНИПУЛИРОВАНИЯ

Цифровые атаки на людей имеют множество форм. Это и классические электронные письма, которые предлагают открыть вложенный файл или перейти по ссылке, и мошеннические сайты, имитирующие интернет-ресурсы известных брендов, и даже точки доступа, внедряющие в трафик вредоносные скрипты.

В статье мы рассмотрим психологические манипуляции в цифровых атаках на примере фишинговых писем. Этот выбор не является случайным и имеет под собой весьма логичное обоснование.

Чтобы добраться до корпоративных систем с ценными данными — CRM, бухгалтерии или интернет-банка — мошенники могут найти и взломать внутреннюю сеть компании, которая хорошо защищена или вообще недоступна извне, либо взломать хотя бы одного пользователя, у которого уже есть нужные права.

Второй вариант проще и эффективнее: достаточно найти адреса электронной почты нескольких сотрудников и отправить им специально подготовленные письма. Во вложении к таким письмам будет вредоносная программа, которая заражает компьютер и даёт хакеру удалённый доступ, или шифрует все данные и требует выкуп. Такая же программа ждёт пользователя по ссылке в письме. Часто никаких дополнительных действий не требуется: компьютер будет заражён сразу после клика.

Таким образом, чтобы взломать компанию мошенникам приходится решить относительно простую задачу: сделать так, чтобы получатель письма захотел открыть вложение или перешёл по ссылке.

Для реализации этой манипуляции преступники используют рабочий инструментальный целый ряд дисциплин: психологии личности и социальной психологии, нейролингвистического программирования, маркетинга и других.

Основные «крючки» для проведения манипуляций — это эмоции, потребности людей, их личностные особенности и морально-этические установки. Важную роль играют демографические параметры потенциальных жертв, а также используемые в атаках атрибуция и усилители.

ЭМОЦИОНАЛЬНОЕ ВОЗДЕЙСТВИЕ

Среди всех способов манипулирования самым результативным являются эмоции.

Эмоции — это психофизиологические, субъективно переживаемые состояния, которые моделируют поведение человека и позволяют адаптироваться к окружающей среде.

Чтобы усыпить бдительность жертвы и создать эффект типовой ситуации и логичности требуемых действий, давление на базовые эмоции применяется в сочетании с методами лингвистического манипулирования

Все эмоции обладают специфическими мотивационными функциями и побуждают к определённому виду поведения.

В зависимости от происхождения эмоции разделяют на базовые и вторичные. Возникновение базовых эмоций обеспечивает самая древняя часть нашего мозга — лимбическая система, включающая миндалину, гипоталамус и таламус. Этот тип эмоций сыграл важную роль в процессе эволюции, обеспечивая быструю оценку ситуации и соответствующую реакцию, позволяя первобытным людям выживать в опасном диком мире.

К базовым эмоциям относятся **злость, отвращение, страх, счастье, печаль, удивление, любопытство**.

Вторичные или социальные эмоции — результат интерпретации опыта более сложных переживаний, имеющих когнитивный компонент. На физиологическом уровне вторичные эмоции задействуют лобные доли коры головного мозга.

Среди вторичных эмоций можно выделить **интерес-возбуждение, стыд-застенчивость, вину-раскаяние** и другие.

Базовые эмоции проходят более короткий путь обработки информации и задействуют меньше областей мозга, нежели вторичные. Формирование базовых эмоций происходит в таламусе и амигдале, в то время как вторичные эмоции проходят более длинный путь: таламус — лобная кора — амигдала.

Это и объясняет, почему воздействие мошенников через примитивнейшие из эмоций столь эффективно в получении быстрой обратной связи от жертвы.

Удар по базовым эмоциям — самый простой способ обеспечить быструю реакцию на предоставленный стимул. Чтобы усыпить бдительность жертвы и создать эффект типовой ситуации и логичности требуемых действий, давление на базовые эмоции применяется в сочетании с методами лингвистического манипулирования:

- ◆ предвзятыми категоричными формулировками,
- ◆ приписыванием или изменением акцентов,
- ◆ недосказанностью,
- ◆ умалчиванием.



Рисунок 1. Эффективность фишинг-атак с различными усилителями. Источник: статистика ООО «Антифишинг»



Рисунок 2. Эффективность фишинговых атак и средний уровень заработной платы. Источник: статистика ООО «Антифишинг»

Перечислим самые интенсивные по воздействию базовые эмоции.

Страх — требует быстрой защитной реакции и снижает порог критического мышления из-за погружения в активное предвосхищение негативного развития ситуации.

Пример: «Ваш компьютер заражён и заблокирован. Кликните здесь»

Злость — провоцирует на активные действия и «разбирательства».

Пример: «Что Вы написали в отчёте? Что за безграмотность? Немедленно исправьте!»

Любопытство — провоцирует поисковое и ориентировочное поведение.

Пример: «Смотри, как ты отжигаш на видео»

Счастье — стимулирует к расширению социальных контактов и притупляет критическое мышление, оценивание.

Пример: «Привет! Приглашаю тебя на нашу свадьбу свидетелем. Вся информация во вложении».

Жадность — стимулирует поисковое поведение, направленное на удовлетворение актуальной ситуативной потребности.

Пример: «Скидка 50% при оплате прямо сейчас».

Чтобы повысить мощность эмоционального воздействия на жертву, преступники могут использовать усилители — специальные элементы манипулирования, применяемые маркетологами и рекламщиками. Среди них наиболее часто встречаются

Срочность — когда требуется выполнить действие как можно быстрее.

Авторитет — когда отправитель письма — значимый для жертвы источник.

Уникальность — фиксация внимания на редкости и особой ценности предложения.

Собранные статистические данные по цифровым атакам на корпоративных пользователей демонстрируют, что наиболее мощным усилителем эмоционального воздействия можно считать авторитет (Рисунок 1).

ПОТРЕБНОСТИ

Следующим по значимости манипулятивным фактором являются актуальные потребности жертвы атаки. Именно они определяют, какую стратегию поведения выберет субъект в той или иной ситуации.

В соответствии с моделью Абрахама Маслоу потребности человека условно можно разделить на:

Физиологические — голод, жажда, сон, активность, секс.

Безопасность — защита от страданий, боли, разрушения, неустроенности

Социальные — потребность в общении, принадлежности к группе, любовь и доверие.

Уважение — одобрение, признание, принятие себя, положительная самооценка.

Самореализация — достижение своих целей и понимание смысла жизни.

Влияние потребностей на поведение сотрудников при цифровых атаках представлено на Рисунке 2, который демонстрирует взаимосвязь средней заработной платы по федеральным округам России и результативность атак с психологическим вектором воздействия на эмоцию Жадность.

Чем ниже уровень средней заработной платы сотрудников (внешние условия, формиру-

ющие актуальную потребность личности на уровне простейшей физиологической нужды — финансовой обеспеченности), тем эффективнее проявляют себя цифровые атаки с психологическим вектором воздействия на эмоцию Жадность.

ЛИЧНОСТНЫЕ ЧЕРТЫ И МОРАЛЬНО-ЭТИЧЕСКИЕ УСТАНОВКИ

Морально-этические установки отвечают за глубинную мотивацию поведения, обуславливая определённую реакцию на манипулятивные воздействия. Как показывают исследования, есть личностные черты, делающие людей более уязвимыми к цифровым атакам, и наоборот. Полное раскрытие значимости данного фактора требует дальнейшего дополнительного изучения, поскольку в общем случае тактику «взлома» можно найти к любому характерологическому портрету, если собрать необходимую информацию.

Примером могут служить рассогласующиеся результаты исследований об уязвимости экстравертов и интровертов, показывающие, что те и другие могут быть особо уязвимы.

Уязвимость экстравертов обусловлена тем, что они гораздо чаще и в большем объёме, чем интроверты, публикуют личную информацию в социальных сетях и прочих онлайн-ресурсах, а также легче откликаются на инициацию коммуникативной активности с незнакомыми людьми.

Интроверты чаще, чем экстраверты страдают от социальной изолированности, более подвержены интернет-зависимости и нейротизму, что также может делать их менее устойчивыми к цифровым атакам.

Тем не менее, это не мешает выделить ведущие характеристики, к которым следует проявлять особое внимание:

♦ **Экстраверсия — интроверсия.** Существует значимая положительная связь между экстраверсией и эффективностью цифровой атаки.

♦ **Эмоциональная неустойчивость (нейротизм) — эмоциональная устойчивость.** Эмоционально неустойчивые люди более уязвимы к цифровым атакам.

♦ **Доброжелательность (дружелюбие, способность прийти к согласию) — обособленность (недоверчивость, эгоизм, враждебность).** Доброжелательные люди более доверчивы.

♦ **Добросовестность (сознательность, организованность, ответственность, надёжность) — импульсивность (беззаботность, небрежность, ненадёжность).** Импульсивные личности чаще становятся жертвами кибермошенников.



Рисунок 3. Эффективность атак по атрибуции.

Источник: статистика ООО «Антифишинг»

♦ **Открытость опыту (креативность, любознательность, независимость) — практичность (конформность, консерватизм, узость интересов).** Консерваторы значительно реже поддаются на уловки организаторов цифровых атак.

АТРИБУЦИЯ

Важную роль в восприятии цифровой атаки играет атрибуция — источник, от имени которого производится манипулятивное воздействие.

По атрибуции можно выделить следующие варианты атак:

♦ **Внешняя** — от имени внешних партнёров или подрядчиков, сторонних известных организаций с узнаваемыми брендами.

♦ **Личная** — имитация личного обращения от знакомого или родственника, ссылка от друга в социальной сети.

♦ **Корпоративная** — от имени коллег из своей организации.

На рисунке 3 представлены результаты исследования эффективности цифровых атак в зависимости от атрибуции. Из полученных данных видно, что письма, написанные от имени коллег или руководства, подвергаются меньшему критическому осмыслению и вызывают больше доверия.

ДЕМОГРАФИЧЕСКИЕ ПОКАЗАТЕЛИ

Анализ цифровых атак выявил, что демографические показатели существенно влияют на их результативность:

Пол. Женщины чаще, чем мужчины, переходят по ссылкам фишинговых писем и предоставляют личные данные мошенническим сайтам даже со всплывающим предупреждением о существующей угрозе.

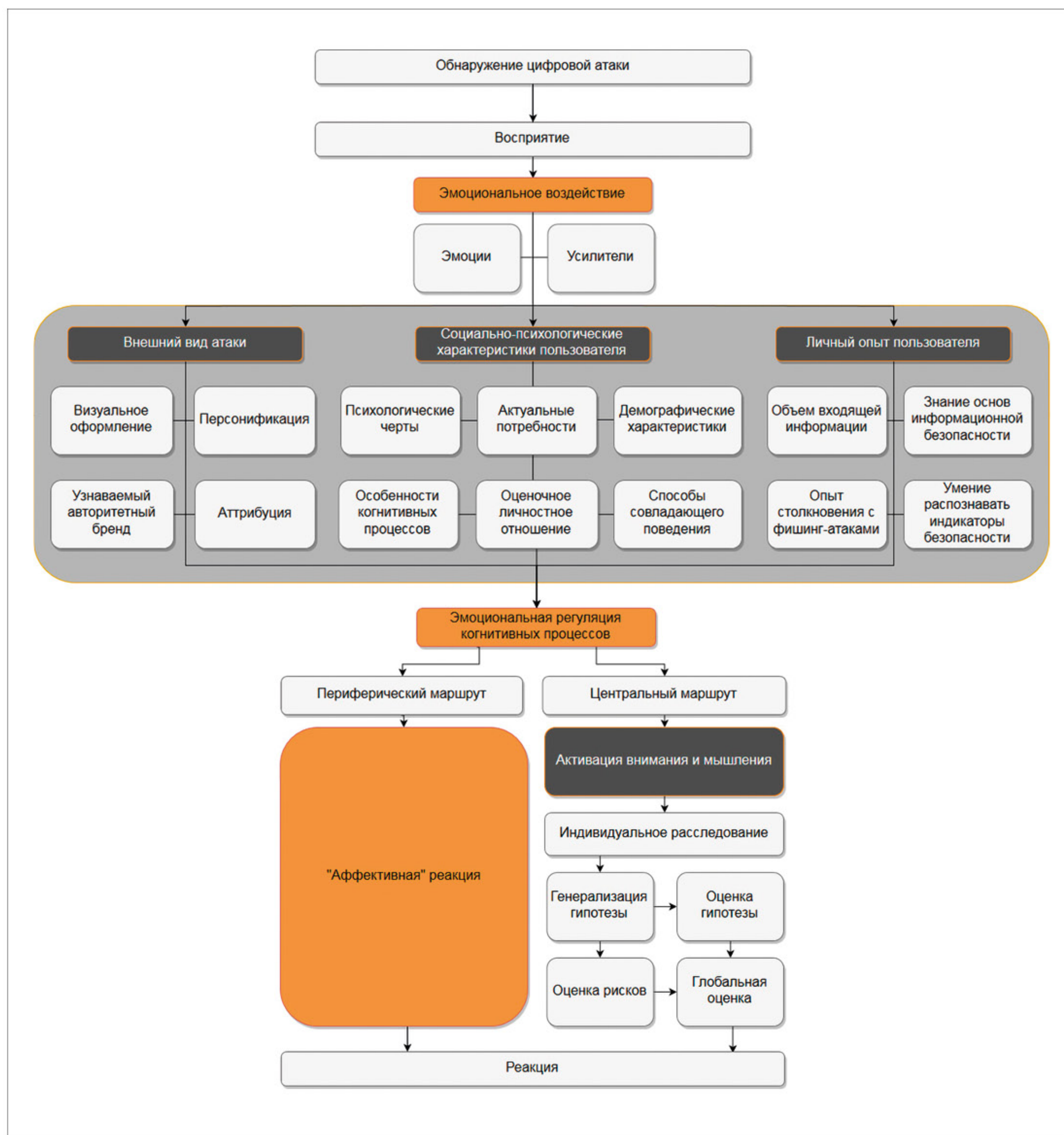


Рисунок 4. Модель психологического воздействия цифровых атак.
Авторы: Богданов А. В., Волдохин С. А., Лимонова О. И.

Возраст. Более уязвимы пользователи в возрасте 18–25 лет.

Культурная и территориальная принадлежность. По предварительным данным представители разных культур проявляют разную устойчивость к цифровым атакам. Атаки на жителей отдалённых районов более эффективны.

ПСИХОЛОГИЧЕСКАЯ МОДЕЛЬ ЦИФРОВЫХ АТАК

Обобщив собранные данные о поведении людей, специалисты Антифишинга разработали модель психологического воздействия цифровых атак, которая концентрирует в себе ключевые элементы когнитивного и эмоционального

воздействия, учитывает личностные особенности и актуальные потребности, предлагая деление атак на вектора (Рисунок 4).

Вектора в модели представлены по мере возрастания «себестоимости» реализации цифровой атаки для мошенников: учёт большего количества факторов воздействия требует индивидуализации подхода и сбора дополнительной информации о жертве.

В соответствии с моделью человек, столкнувшийся с цифровой атакой, проходит пять стадий: оценка внешнего вида, формирование эмоционального отношения, наложение личностных черт и опыта на восприятие письма, активация внимания с мышлением и реакция.

Рассмотрим эти стадии более подробно на примере фишинг-письма с имитацией рассылки от сервиса Яндекс.Еда. Письмо предлагает получить солидную скидку «здесь и сейчас».

Оценка внешнего вида. Получив письмо, человек оценивает его внешний вид и пытается классифицировать в соответствии с приобретённым опытом. Важную роль играет отправитель письма, в нашем примере — авторитетный бренд. Качественное оформление также повышает степень доверия, поскольку многие пользователи автоматически воспринимают такие письма как легитимные.

Формирование эмоций. Чаще всего авторы цифровых атак обращаются к базовым эмоциям, чтобы избежать «длинного» пути осмысления содержания. В примере используются две базовых эмоции: любопытство и жадность. Увеличить мощность воздействия помогают два усилителя — срочность и уникальность предложения. Сочетание эмоций и усилителей направляют пользователя как можно скорее совершить целевое действие, чтобы получить желанную скидку.

Наложение личностных особенностей. Эффективность воздействия сильно зависит от того, насколько мошенник учёл актуальные потребности, личностные черты и опыт пользователя, так как это сильно влияет на его восприятие атаки и последующие действия по отношению к ней. Кроме того, важное значение имеет регион проживания и предыдущий опыт цифровых атак.

Активация произвольного внимания. На этой стадии объект атаки понимает, что столкнулся с каким-то новым явлением и, если не поддавшись своим эмоциям, пытается выработать объяснение выявленной разнице между привычным и наблюдаемым. В его сознании рождается гипотеза, с достаточной степенью достоверности объясняющая происходящее. Выработав гипотезу, человек различными способами про-

веряет логичность этих объяснений. Оценив все гипотезы, человек принимает окончательное решение, которое глобально сводится к доверию или недоверию.

Реакция. Результатом принятого на предыдущей стадии решения становится действие, которое выполняет человек. Это может быть переход по ссылке, установка вредоносного обновления, ввод учётных данных в форму или наоборот, удаление фишингового письма или оповещение службы безопасности о факте атаки.

ЗАКЛЮЧЕНИЕ

Обеспечение информационной безопасности в организациях — комплексная задача. От специалистов ИБ требуются не только технические навыки, но и понимание логики действия мошенников, а также наиболее вероятной реакции коллег на цифровые нападения.

Использованные в статье статистические данные, собранные нами в процессе работы с многопрофильными организациями на территории РФ, позволяют уловить существующие тенденции в сфере цифровых атак, а также понять ключевые уязвимости сотрудников. Эта информация поможет компаниям сформировать группы риска для обучения и тренировки навыков сотрудников в сфере ИБ, а предложенная модель разбора цифровых атак позволит повысить эффективность обучения сотрудников распознаванию мошеннических нападений и правильным действиям при их обнаружении.

Также важно понимать ключевые идеи, которыми нужно руководствоваться при выстраивании грамотной системы обучения ИБ в своей компании:

1. Устойчивость компании к цифровым атакам определяется не только функциональностью технических средств защиты, но и уровнем подготовленности персонала.
2. Теоретические знания о цифровых атаках не всегда помогают противостоять реальным случаям кибернападений.
3. Обеспечить эффективную защиту от цифровых атак может только сочетание знаний принципов информационной безопасности и навыков их применения, отработанных на близких к настоящим атакам.
4. Проверить результативность тренировки сотрудников можно с помощью тестирования. Оно также выявит «слабые звенья», для которых необходимо повторное обучение.
5. Чтобы сохранять мотивацию, сотрудники должны понимать конечную цель обучения и тренировок, а также их личные бонусы.

ОТ РЕДАКЦИИ

Подборка рубрики «Биохакинг» в разделе Hi-Hume этого номера имеет две особенности. Первая — публикации посвящены темам, смежным с тематикой нашего журнала. Это высокотехнологические решения в сфере качества и продолжительности жизни. Однако их эффективность и безопасность, в том числе информационная, представляет не только «общечеловеческий» интерес, но напрямую касается каждого из нашей читательской аудитории, членов их семей и близких. С полными версиями статей

можно будет, как обычно, ознакомиться на сайте нашего журнала.

Вторая особенность — это уже не «протокол о намерениях», а публикации о прошедшем мероприятии, авторские статьи разработчиков.

Данная подборка, как говорится, ознакомительная. Медиа Группа «Авангард» анонсирует на конец текущего 2019 года выпуск нового специализированного издания «Hi-Hume Journal», куда впредь переместится разработка подобной тематики.



Павел
БЫЛЕВСКИЙ
шеф-редактор
BIS Journal

БИОХАКЕРОВ ГОСУДАРСТВО ПОКА В УПОР НЕ ВИДИТ

МОЖЕТ, ПРАВИЛЬНЕЕ ПЕРЕИМЕНОВАТЬСЯ В «СОЦИОБИОХАКЕРЫ»?

Новейшие впечатляющие достижения hi-tech не могли не соблазнить на попытки совершить столь же впечатляющие прорывы в гуманитарной сфере. Как за счёт внедрения технических новинок, так и её собственными «инструментами», наукоёмких гуманитарных разработок (hi-hume). Одним из направлений которых стал так называемый биохакинг. Слово это явно родилось в результате «скрещивания» компьютерного программирования и биологии.

НЕПОНЯТНОЕ ПОНЯТИЕ

Понятие биохакинга не является строгим. Буквальный смысл словосочетания «биологическое хакерство» — несанкционированное перепрограммирование биологического организма. В этом внутреннее противоречие, поскольку «программы» развития и функционирования живых организмов не пишутся людьми. В отличие от компьютерных, они развиваются и формируются, что называется, естественным образом. Но, конечно, «биохакер» звучит неизмеримо круче и более многообещающе, чем какой-нибудь «селекционер».

Тем более, что нынешние биохакеры ставят перед собой намного более амбициозные цели, чем выведение нового сорта яблок или породы

домашнего скота. Занимаются, главным образом, решением такой важной для каждого проблемы, как улучшение «человеческой природы». В том плане, что ищут наукоёмкие решения для радикального оздоровления и увеличения полноценного долголетия.

То, чем реально занимаются биохакеры, носит межотраслевой характер, относится к сферам медицины и здравоохранения в целом, биологии, биотехнологий, физкультуры, психологии и, конечно, вездесущих нынче компьютерно-коммуникационных технологий.

ХАРАКТЕРНОЕ МЕРОПРИЯТИЕ

Характерным и показательным примером происходящего «в отрасли» стало деловое мероприятие — Biohacking Conference Moscow, проведённая 19 сентября 2019 года в Технополисе «Москва». Собравшиеся обсуждали вопросы улучшения человека путём различных способов его «перепрограммирования».

Со своими решениями выступали разработчики, чаще всего по совместительству владельцы или ведущие специалисты коммерческих организаций, оказывающих услуги подобного рода. Среди человеческих параметров, подлежащих улучшению, рассматривались здоровье, красота, долголетие, физические и умственные способности.

Презентовался широкий спектр средств:

- ◆ медицинских (фармацевтических и физиотерапевтических),
- ◆ диетологических,
- ◆ лечебная физкультура и фитнес,
- ◆ биотехнологии (стволовые клетки и генная инженерия),
- ◆ нейростимуляция,
- ◆ компьютерно-телекоммуникационных (использование специальных гаджетов, в том числе имплантов — «киборгизация», BigData и «оцифровка личности»),
- ◆ а также различные комплексные решения.

В фойе спонсоры и партнёры конференции на стендах демонстрировали свои продукты и услуги. Кроме профессионалов, в зале на платной основе присутствовала аудитория — энтузиасты биохакинга. По информации организаторов конференции, в мероприятии анонимно участвовали и инвесторы, которые ищут, куда лучше вложить свои деньги.

К сожалению, на конференции отсутствовали как класс представители профильных государственных органов законодательной и исполнительной власти, отвечающих за здравоохранение, медицину, образование. Не было специалистов ни из министерств и прочих ведомств, ни из Государственной Думы и Совета Федерации РФ.

ПРИБАВИТЬ ГУМАНИТАРНОГО

Между тем участие государства могло бы послужить прологом к интеграции перспективных решений биохакеров в государственную политику в сфере «человекостроения». Тогда повышение пенсионного возраста стало бы естественным следствием продления трудоспособного возраста, и не было бы чревато снижением рейтинга политического руководства страны. Напротив, дополненное гарантированным трудоустройством таких граждан было бы на ура и с воодушевлением воспринято гражданским обществом.

В этом плане особый интерес представило выступление Елены Миловой (члена Совета директоров Life Extension Advocacy Foundation) о гуманитарных и социальных аспектах значительного увеличения трудоспособного возраста и долголетия. Другие участники этих сторон биохакинга, а также нравственных и культурных, не затрагивали. А напрасно: в отношении человека понятие «биологического хакерства» более уместно, чем применительно к прочим живым организмам. Поскольку роль сознательного программирования в обществе, в целом и в жизни каждого его члена, необычайно велика.



Главный вопрос в том, каким именно образом биологические механизмы человека соотносятся с этим социальным программированием. Те же условные рефлексы и важнейшая «автоматика» человека, включая привычки, формируются как результат его поведения, обучения. Так что точнее был бы термин «социобиохакинг». Звучит не так угрожающе, как «социальный хакер», сразу вспоминается «социальная инженерия». И, тем более, лучше, чем «политический хакер» со всякими «вмешательствами в выборы».

Тем не менее, самообозначение «биохакинг» уже прижилось, а в истории не раз бывало, что значение термина менялось порой до противоположного. Более важны не сами слова, а реальное содержание того, что делается под их вывеской. Ещё более важны стоящие проблемы и предлагаемые пути решения. Решающей оказывается динамика положительных результатов.



Елена МИЛОВА
член совета
директоров Life
Extension Advocacy
Foundation

НАШЕ БУДУЩЕЕ, КОТОРОЕ НЕ ЗА ГОРАМИ

СОЦИАЛЬНЫЕ АСПЕКТЫ И ПЕРСПЕКТИВЫ «ПЕРЕПРОГРАММИРОВАНИЯ» СРОКА ЧЕЛОВЕЧЕСКОЙ ЖИЗНИ

Современные наукоёмкие, высокотехнологичные исследования и разработки в области оздоровления и продления сроков полноценной жизни имеют длительную предысторию. Исследованиями старения, возрастных болезней, возможностями омоложения и продления жизни человечество занималось с доисторических времён.

ОТ МИФА К ТЕХНОЛОГИЯМ

Древнейшие мифы, дошедшие до нас литературные источники (сага о Гильгамеше и другие) повествуют о том, как люди утратили вечную молодость и как пытались вернуть её разными способами. В настоящее время вопрос о том, как продлить здоровую жизнь человека решается с помощью научных исследований и разработок.

Наш соотечественник И. И. Мечников (1845–1916), биолог, иммунолог и геронтолог, одним из первых заявил: старение подобно болезни, его можно и нужно лечить, как и прочие. Его исследования в области иммунологии позволили предположить, что хроническое снижение иммунитета играет большую роль в старении, и что правильное питание и поддержание здоровой микробиоты — факторы, влияющие на долголетие. Позднее многие из идей Мечникова были доказаны. Его фактически считают отцом научной геронтологии.

Развитие науки в XX веке расширило и углубило возможности исследовать организм человека, в том числе до молекулярного уровня. 1970–80-х годах был достигнут ряд научных прорывов. В частности, А. М. Оловников, специалист в теоретической молекулярной и клеточной биологии, выдвинул в 1971 году теорию старения из-за укорочения теломер — концевых участков хромосом — в результате деления клеток. За экспериментальное подтверждение этой теории Кэрл Грейдер, Эли-

забет Блэкберн и Джек Шостак в 2009 году получили Нобелевскую премию по физиологии и медицине.

На рубеже тысячелетий на сцену выходит Обри ди Грей, британско-американский биолог-геронтолог, информатик и математик, который разработал концепцию SENS — стратегию достижения пренебрежимого старения инженерными методами. В 2007 году в книге «Отменить старение» он сформулировал семь ключевых механизмов старения на клеточном уровне. По его мнению, воздействуя на эти механизмы теоретически можно замедлить или обратить вспять возрастные изменения и тем самым значительно продлить здоровый период жизни человека.

Задачей Обри было привлечение внимания научного сообщества к возможности превратить механизмы старения в новую терапевтическую мишень, и подтолкнуть медицинскую науку к поиску путей контроля над старением. Чтобы продвигать свою концепцию, Обри ди Грей стал соучредителем и главой Фонда SENS и Фонда Мафусаила, а также главным редактором академического журнала Rejuvenation Research.

Сегодня уже никто не может отрицать: старением принципиально можно управлять в широких пределах и даже обращать его вспять. Вопрос лишь в том, как скоро технологии для управления старением у людей пройдут клинические испытания и станут доступны.

СТАРЕНИЕ КАК ОБЩЕСТВЕННАЯ ПРОБЛЕМА

В мире наблюдается старение населения, то есть увеличение доли пожилых людей в структуре населения. Это связано, с одной стороны, со снижением рождаемости, а с другой, с повышением продолжительности жизни людей. Пожилые люди это самая быстро растущая возрастная группа, в развитых странах доля пожилых уже сейчас 25–30%.

С полной версией
статьи можно
ознакомиться
в интернет-версии
BIS Journal:
[www.ib-bank.ru/
bisjournal](http://www.ib-bank.ru/bisjournal)

Старение населения ставит перед обществом специфические проблемы. У тех, кто доживает до 60–70 лет, есть как минимум одно возрастное хроническое заболевание, чаще 2–3, а то и целый «букет». Лечить каждое из таких заболеваний по отдельности, считают эксперты в области здравоохранения, неэффективно, а в условиях роста доли пожилых людей нагрузка на систему здравоохранения увеличивается.

До сих пор речь шла зачастую лишь о симптоматическом лечении, из-за невозможности устранить причину возрастных заболеваний. Определение ключевых механизмов старения и развитие биотехнологий в сфере долголетия («антиэйджинга») открывает перспективы полноценной превентивной медицины. И поскольку эти технологии объективно необходимы обществу в условиях старения населения, неудивительно, что они привлекают все большее внимание инвесторов.

Одним из драйверов этого интереса выступил британский предприниматель и филантроп Джим Меллон. В своей книге *Juvenescence*, которая предварила основание одноименного фонда, он написал, что потенциально технологии долголетия представляют собой новый денежный фонтан, и серьезным инвесторам надо как можно скорее входить в эту индустрию. Выгода двойная — возможность продлить продуктивную жизнь себе и близким, а также помочь другим людям и заработать на новых медицинских технологиях.

Конечно, у новой индустрии есть свои специфические сложности. Главная — это то, что для подтверждения эффективности нового лекарства для продления жизни нужно проводить клинические испытания в течение долгого времени, так как люди — долгоживущий вид. Большинство инвесторов не захотят ждать 20 лет, пока пройдет эксперимент.

Чтобы быстрее получить объективные показатели эффективности новых лекарств, за последнее десятилетие были разработаны биомаркеры старения — такие показатели здоровья, которые самым тесным образом связаны с динамикой развития возрастных заболеваний и могут служить косвенным доказательством потенциала терапии к продлению жизни.

Стоит помнить, что любая страна, которая первой разработает и внедрит терапии против старения на массовом уровне, получит целый спектр преимуществ, связанных с высоким уровнем здоровья и продолжительности жизни населения, первыми из которых являются высокая производительность труда и повышение общего интеллектуального потенциала.

РОЛЬ СМЫСЛА ДЛЯ ЗДОРОВОГО ДОЛГОЛЕТИЯ

Мы довольно много знаем о том, какие обстоятельства лежат за долголетием. На срок жизни, помимо образа жизни, влияют такие разнообразные факторы как экономический статус, уровень образования, место рождения, месяц рождения, прочность социальных связей, уровень осознанности (организованности) и наличие целей и планов. Последние два фактора мне кажутся наиболее важными, так как именно понимание своих потребности и целей, а также уровень самодисциплины, определяют то, как именно мы живем. Эти факторы находятся под влиянием доминирующей идеологии.

Коммунистическая идеология в СССР, при некоторых ее недостатках, все же мотивировала людей на прогресс, на бесконечное развитие, в том числе развитие человеческих качеств — здоровья, физической силы, интеллекта, доброты. В постсоветский период, когда идеологическая машина замолчала, этот компас был утрачен. Будущим сверхдолгожителям как никогда прежде нужна новая, современная система жизнеутверждающих приоритетов, которые сделают сверхдолгую жизнь наполненной высокими смыслами.

Люди, у которых появляется возможность жить несколько столетий и больше, должны знать, куда и зачем им идти. Необходим высокий смысл, сильнейшая мотивация, «новый героизм». И эти смыслообразующие элементы не получится создать путём копирования прошлого опыта, включая религиозный. В основу мировоззрения долгожителя должна лечь наука.

Современный мир очень быстро меняется, усложняется. Долгая жизнь — это не просто абстракция. Глядя в будущее мы уже сегодня видим ожидающие нас вызовы, такие как старение населения, изменение климата, проблемы с экологией. Для того, чтобы их решить, нам придется перейти на новый уровень развития, усилить свои способности к анализу информации и принятию решений. Нам придется научиться общаться друг с другом и выстраивать

Мы уже сегодня видим ожидающие нас вызовы, такие как старение населения, изменение климата, проблемы с экологией. Для того, чтобы их решить, нам придется перейти на новый уровень развития

коллаборации глобального уровня. Наше время требует от нас принять принцип обучения в течение всей жизни как объективную необходимость.

Мы часто слышим опасение, что «таблетки от старения» будут доступны только элитам. Меня гораздо больше беспокоит то, что масса людей не захочет использовать эти технологии даже при их доступности просто потому, что долгая жизнь представляется слишком сложной, они к ней морально не готовы, не мотивированы к саморазвитию в достаточной степени, чтобы найти свою нишу в мире будущего.

Применять технологии или нет всегда будет делом свободного выбора. Все, что мы со своей стороны можем сделать, это информировать людей о потенциале и достижениях геронтологии, чтобы они могли принять осознанное решение, а также содействовать формированию жизнеутверждающего мировоззрения.

СМЕЖНЫЕ ПРОБЛЕМЫ

Перспектива серьезного продления полноценной жизни человека, скажем, до 150 лет, не может не вызывать вопроса о последствиях: какие изменения произойдут в мире по этой причине. Нам предстоит справиться с несколькими глобальными вызовами, например, ухудшением экологии, пищевым кризисом, изменениями климата, и конечно, если практически все взрослые будут полностью здоровы и способны участвовать в решении этих проблем, это огромный плюс. Дополнительный плюс в том, что у людей старшего возраста, как правило, большой социальный опыт.

Однако, в данный момент практически отсутствуют социальные институты, которые могли бы обеспечить для людей старшего возраста возможности «профессиональной реабилитации и реадaptации». Чтобы здоровые пожилые люди (а к середине века в развитых странах эта возрастная группа составит до 25 % населения) могли продуктивно работать, им необходимо обучение по востребованным специальностям.

Пока же международное движение «Университет третьего возраста» (сокращенное название U3A, от англ. university of third age) фактически состоит из центров досуга, где пожилым людям предлагают осваивать новые хобби или просто приятно проводить время с другими людьми той же возрастной группы. Сейчас имеет место дискриминация по возрасту, для пожилых людей не гарантировано «право на труд». Даже если люди старшего возраста получают новое образование, вопрос дальнейшего трудоустройства стоит крайне остро.

Поэтому для того, чтобы общество выиграло от радикального продления жизни, необходимо создавать программы переобучения для пожилых, противодействовать дискриминации по возрасту, формировать отношение к пожилым людям как перспективным сотрудникам, которых стоит нанимать и в развитие которых стоит вкладываться.

Еще один вызов, с которым нам предстоит столкнуться (причем независимо от результатов разработки технологий долголетия), это увеличение численности населения. Согласно последнему отчету ООН по народонаселению, к концу века на планете будет проживать около 10,9 миллиарда людей (сейчас население составляет 7,6 миллиарда). Рост населения на треть со-размерно повышает потребность в продуктах питания, увеличивает нагрузку на экологию.

Кроме того, в условиях изменений климата будет наблюдаться высокий уровень миграции из жарких стран в страны с умеренным климатом, обострение социальных конфликтов и изменение структуры заболеваемости в целом ряде стран.

Помимо этих глобальных кризисов предвидятся и другие, например, проблема быстрого нарастания лекарственной устойчивости со стороны возбудителей различных инфекционных заболеваний. Разработка новых антибиотиков и фунгицидов идет медленнее, чем накапливаются резистентные штаммы. Рост численности населения означает повышение плотности населения, что повышает вероятность и скорость распространения эпидемий.

Все эти аспекты нашего общего будущего следует рассматривать в комплексе и учитывать при формировании глобальной и национальной политики. На данный момент ясно одно: если вы планируете жить долго, вам следует направить свою профессиональную деятельность на решение глобальных проблем.

Контроль над старением может дать нам возможность, которой никогда еще не было в нашей истории, — возможность наращивать свой интеллектуальный потенциал в течение дополнительных десятилетий, а то и больше.

* * *

Без сомнения, долголетие в совокупности с практически неограниченным доступом к информации и созданием систем поддержки принятия решений на основе искусственного интеллекта может повысить нашу способность управлять развитием цивилизации. От начинающих долгожителей требуется только одно: искреннее стремление сделать этот мир лучше для всех.

БОЛЬШЕ ЗДОРОВЬЯ — МЕНЬШЕ БОЛЕЗНЕЙ

ПРЕВЕНТИВНАЯ МЕДИЦИНА КАК СТРАТЕГИЯ УЛУЧШЕНИЯ ЗДОРОВЬЯ И КАЧЕСТВА ЖИЗНИ

Главное отличие превентивной медицины от профилактики в решаемой задаче. Профилактика — стандартный базовый набор медицинских практик без учёта особенностей здоровья человека. Превентивная медицина нацелена на улучшение и расширение резервов организма ради prolongation полноценной жизни. Путь к решению этой задачи — персонализированное управление здоровьем.

ВОССТАНОВИТЬ И УЛУЧШИТЬ

Превентивная медицина существенно отличается от медицинской профилактики. Обычная медицинская профилактика работает по ограниченному стандартному направлению: диспансеризация, вакцинация, информирование граждан о факторах риска некоторых заболеваний. Даются общие рекомендации, чего не нужно делать и что нужно, чтобы не заболеть. Эти меры позволяют уменьшить риски заболеваний, отслеживать их начало на ранних этапах, чтобы легче было вылечить. Медицинская профилактика носит консервативный характер, она не направлена на индивидуальный подход к улучшению здоровья человека, усиление его иммунитета и коррекцию имеющихся нарушений.

Превентивная медицина по своему инструментарию близка к так называемой комплементарной, объединяющей разные методы и направления нелекарственных и нехирургических методов лечения. Таким образом сотни лет формировалась и развивалась народная медицина, истоки которой восходят к травникам и траволечению.

В нашей стране в государственном здравоохранении представлена только обычная официальная медицина. Превентивная медицина «отделена от государства», является частным делом разработчиков оздоровительной продукции и тех граждан, кто неудовлетворён эффективностью «обычного» государственного здравоохранения.

Для сравнения, в Китае работает созданное в 1988 году Государственное управление по делам традиционной китайской медицины и фармакологии, которое разрабатывает стратегию раз-

вития, курс, политику и законопроекты в этой области. Пациент имеет право выбрать, как он лечится в государственной системе: средствами официальной или традиционной китайской медицины (нелекарственной).

Аналогичный выбор нелекарственных средств лечения предлагается и в США. В Финляндии с помощью государственной нелекарственной программы поддержки здоровья граждан за два десятилетия удалось решить проблему депопуляции страны. По показателям здоровья населения и качества жизни они вышли на второе место в мире после Японии. К сожалению, в России пока нет аналогичного государственного органа.

У превентивной медицины в сравнении с «официальной», государственной, есть ряд преимуществ и ряд недостатков. У каждой своё место, своя сфера. Есть травматология, «скорая помощь», реаниматология, опасные обострения хронических заболеваний, включая инфекционные. В чрезвычайных ситуациях, угрожающих жизни и здоровью, у «официальной» медицины безусловный приоритет.

Она быстрыми жёсткими мерами спасает человека, сохраняет здоровье, не даёт погибнуть или остаться инвалидом. Но сильнодействующие средства, давая быстрый прямой эффект, сопровождаются и негативными побочными эффектами, часто довольно серьёзными. Фармацевты прямо и честно предупреждают об этом в инструкциях к препаратам.

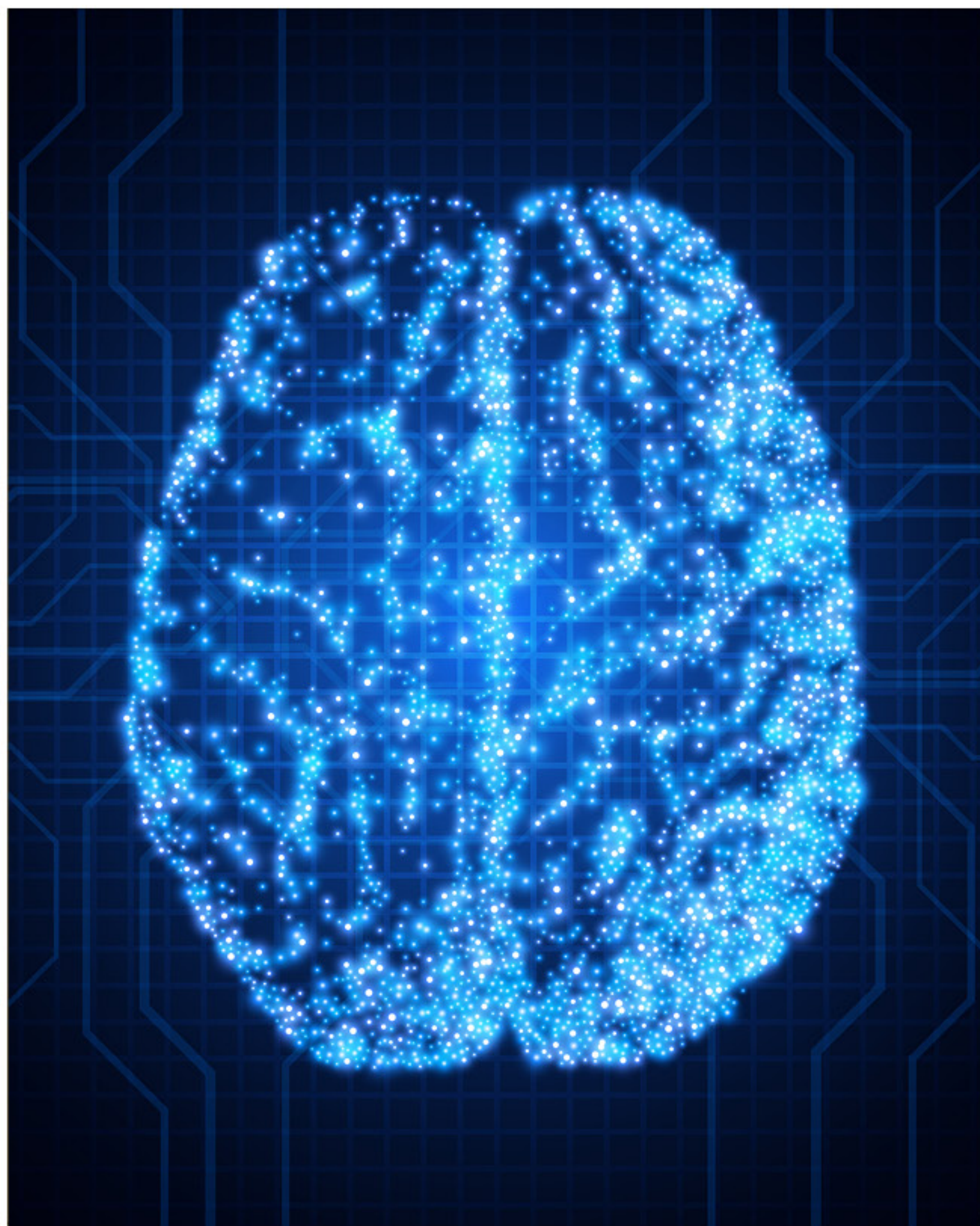
Превентивная медицина восстанавливает здоровье без негативных побочных эффектов. В том числе и после издержек, связанных со снятием острых состояний средствами официальной медицины.

КВАЛИФИЦИРОВАННАЯ СТРАТЕГИЯ

Применение природных препаратов, в сравнении с официальной терапией, не даёт быстрого сиюминутного эффекта. Это не краткосрочный курс, после которого можно вернуться к образу жизни, который послужил причиной заболевания. Нет, это стратегия, постоянная забота об улучшении своего здоровья, позитивном изменении образа жизни. Положительные измене-



Валентина БУРКОВА
доктор химических наук, академик РАЕН, президент компании «Биолит»



ния аккумулируются и начинают проявляться спустя недели, месяцы и годы. Накопительный эффект, улучшение здоровья, достигается медленно, зато верно и без негативных побочных эффектов.

В превентивной медицине грань между профессиональным лечением и самолечением более тонкая, чем в официальной. Это не страшно, во-первых, потому что средства природного происхождения, в большинстве своём, безвредны и не несут негативных побочных эффектов, разве что может быть индивидуальная непереносимость.

Во-вторых, человек, их практикующий, постоянно обучается, узнаёт новое, и повышает свою квалификацию. В-третьих, такой человек примеряет новые знания к своим индивидуальным особенностям, поэтому превентивная медицина является персонализированной при решающем участии самого пациента.

Тут принципиально важно сильное стремление человека к улучшению своего здоровья. Необходимо готовность регулярно уделять этому

внимание, анализировать и учиться новому. Не все это, к сожалению, понимают. Есть многочисленные примеры, в том числе из опыта богатых, успешных людей. В сорокалетнем возрасте у них за плечами и инфаркты, и инсульты. Причины — отсутствие стратегического внимания, «спортивного интереса» к своему здоровью. Надежды, «в случае чего», на «скорую помощь» и реанимацию.

К сожалению, в российском здравоохранении нет полноценного регулирования традиционной, народной, превентивной медицины. Соответственно, нет и системы обучения этому как граждан, так и самих врачей.

НАША НАУЧНО-ПРОИЗВОДСТВЕННАЯ БАЗА

В Институте химии нефти СО РАН мы изучали происхождение нефти и как практическую реализацию фундаментальной науки — перспективы использования лечебной грязи в курортном лечении. Исследовали потенциал литогенеза осадочных пород биологического происхождения, процесс концентрации и консервации биологически активных элементов. Отсюда, от сочетания слов «жизнь» и «камень» происходит название нашей компании «Биолит». Наше преимущество — использование высокого научного потенциала.

Начав четверть века назад заниматься, по своей сути, производством натуральных средств для превентивной медицины, мы пришли к тому, что создание качественного продукта требует полного производственного цикла, включая производство собственного растительного сырья. В нашей стране при СССР была создана обширная производственная база: 34 сельскохозяйственных производства с опытными станциями ВИЛР — Всесоюзного НИИ лекарственных и ароматических растений. На этой базе разрабатывались, а потом применялись технологии выращивания, заготовки, хранения и переработки лекарственных растений.

Развал Советского Союза привёл к полному уничтожению собственной сырьевой базы лекарственных растений. В итоге, на сегодняшний день, подавляющее большинство сырья стало закупаться в Китае.

Наша производственная сырьевая база была создана в предгорьях Алтая в начале 2000-х годов. Склоны гор нельзя распахать, поэтому там не выращивают однолетние злаковые культуры, рожь или пшеницу. Зато там растут разнообразные многолетние лекарственные травы. Около 20 бригад под нашим контролем начали в нужное время заготавливать это сырьё, правильно сушить и хранить.

Увидев, что объёмов растительного сырья из дикой природы не хватает для растущего сбыта, приняли решение начать их специально выращивать. Приобрели земельные участки, разрабатывали технологии, покупали оборудование, расширялись. Заинтересовали окрестных фермеров, излечив одного из них с помощью наших средств от тяжёлой аллергии.

Они помогли нам правильно выстроить производственный процесс выращивания сырья, подобрать оборудование. Мы научились выращивать корень лопуха, как у китайцев — длинный, «морковкой», без множества боковых отростков, которые являются только «проводящим органом» и многие другие многолетние растения, и даже легендарный женьшень.

Наши вложения в производство оправдали себя, а первоначальный капитал был получен в период первоначального бурного роста структур РПО «Арго». Вложения в развитие производства на Алтае продолжаем и сейчас. Быстро растут объёмы производства лопуха, осины и солянки холмовой. Для них требуются отдельные технологии и линии переработки.

В настоящее время мы производим более 500 наименований продукции не только на основе растительного сырья, но и органо-минерального. Это лечебные грязи, торф, панты алтайских маралов. Наша продукция предназначена для очищения организма, поддержания иммунитета, коррекции опорно-двигательного аппарата, а также гормональной системы, в том числе для противодействия стрессам. Есть комплексные схемы применения продукции, последовательно охватывающие все основные показатели здоровья организма.

ФАРМАЦЕВТИЧЕСКОЕ ЛОББИ

После запрета в России рекламы БАД компании, которые делали ставку на этот способ продвижения продукции, закрылись. Этот рынок сократился примерно вдвое. Тем не менее, сейчас в сфере превентивной медицины работают 500–600 таких компаний. Процветают экспортёры дикоросов — ягод, грибов, кедровых орехов, а также те, кто уделяет повышенное внимание качеству сырья и продукции. И, конечно, хорошему маркетингу, в том числе через сетевые структуры и через врачей.

В настоящее время в нашей стране зарегистрировано около 6 тыс. наименований БАД к пище. К слову сказать, только в Европе таких препаратов зарегистрировано полтора миллиона.

В инструкциях по их применению чётко прописана фраза «перед употреблением проконсультируйтесь с врачом». Но вот здесь любой производитель нелекарственной продукции и

сталкивается с тем, что мы называем «фармацевтическим лобби».

Большинство наших врачей, особенно в российской глубинке, категорически не желают разговаривать с пациентами на эту тему. Боятся увольнения, т.к. главные врачи поголовно стоят на страже интересов «производителей лекарств».

В то же время мы активно работаем в Евросоюзе (торговая марка «Биолит» зарегистрирована во всём мире), и там врачи с большим интересом используют БАДы, особенно если имеется серьёзная доказательная база. Для них это подспорье, расширение профессионального инструментария.

ОБЩЕСТВЕННОЕ ДВИЖЕНИЕ И ЗДОРОВЬЕ ЧЕЛОВЕКА

Важная роль в формировании осознанного отношения к своему здоровью принадлежит общественным организациям. Например, Общероссийское общественное движение «За сбережение народа», организатором и якорным партнёром которого является РПО «Арго». Это движение поддерживается депутатами Госдумы и представлено действующими филиалами в 63 регионах РФ. Важная роль участников Движения заключается в их взаимодействии с органами медицинской профилактики здоровья человека с использованием средств комплементарной медицины, имеющих современную доказательную базу.

Другой пример — «Родительский форум» в Калининградской области, где успешно налаживаются отношения с администрацией региона, структурами, отвечающими за здравоохранение.

Филиалы движения «За сбережение народа» уже два года активно участвуют в обучающих школах для врачей-инфекционистов, которые ежегодно проводятся профессорско-преподавательским составом, возглавляемым академиком В. И. Покровским. Школы инфекционистов охватывают в год около 30 регионов России, а привлечение к ним участников общественного движения «За сбережение народа» обогащает врачей новыми инструментами превентивной медицины.

* * *

Почему инфекционисты? Потому что, ОРЗ и гриппом болеют в 100 раз чаще и больше, чем всеми остальными заболеваниями. Врачи-инфекционисты, в арсенале которых главное оружие — антибиотики, давно убедились в огромном количестве их побочных эффектов, особенно в детской практике. И в этом комплементарная медицина с дополнительным применением природных препаратов является новым решающим шагом в здоровую и полноценную жизнь.



ИСКАТЬ ТАЛАНТЫ ИНТЕРЕСНО!

В СОЧИ ЗАВЕРШИЛАСЬ ПЕРВАЯ
В РОССИИ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ СТУДЕНТОВ

В разгар веселья на популярном аттракционе в курортном парке гаснет свет. Необходимо как можно быстрее расследовать атаку на сеть управления автоматикой одного из крупнейших аттракционов страны и восстановить работу системы иллюминации.

Это не сценарий очередного блокбастера — такими грандиозными совместными киберучениями, организованными компаниями «Ростелеком», «Ростелеком-Солар», Образовательным центром «Сириус» и Сочи Парком, завершилась в конце сентября новая студенческая учебная программа по кибербезопасности.

Образовательную программу по кибербезопасности для талантливых ребят со всей России создал образовательный фонд «Талант и успех» при поддерж-

ке «Ростелекома» и компании «Ростелеком-Солар». К участию были приглашены 40 студентов 1–4 курсов, которые победили во всероссийском соревновании по информационной безопасности «Кибервызов: Новый уровень». Кураторами программы со стороны индустриального партнера фонда стали старший вице-президент «Ростелекома» по организационному развитию и управлению персоналом Галина Рысакова и вице-президент «Ростелекома» по информационной безопасности Игорь Ляпунов.

Отбор участников программы прошел летом 2019 года. Принять участие в первом этапе могли все желающие студенты российских вузов, зарегистрировавшиеся на сайте организаторов.

Первый этап представлял собой онлайн-соревнование по ИБ. Он включал задачи по компьютерной криминали-

стике, криптографии, реверс-инжинирингу и веб-безопасности. Оценку работы участников вела автоматизированная система динамического скоринга: чем больше людей решили задачу, тем меньше была ее «стоимость». Рейтинг участников обновлялся в реальном времени на сайте организаторов.

На второй отборочный этап перешли 60 студентов, набравших максимальное число баллов. С ними специалисты «Ростелеком-Солар» провели скайп-интервью, по итогам которого 40 участников были приглашены на очное двухнедельное обучение на базе образовательного центра «Сириус» в Сочи. Победителями отборочных этапов стали студенты профильных вузов из Самары, Хабаровска, Нижнего Новгорода, Ростова-на-Дону и Москвы.



На фото слева: М. Сигаева, заместитель генерального директора, HR-директор компании «Ростелеком-Солар», на награждении участников программы по кибербезопасности в образовательном центре «Сириус»

Программа в центре «Сириус» на берегу Черного моря включала теоретические и практические занятия по обеспечению кибербезопасности АСУ ТП, защите веб-приложений, исследованию современных векторов атак, реверс-инжинирингу и компьютерной криминалистике. Отдельные модули программы были посвящены вопросам профессиональной этики и развитию требований к специалисту по ИБ, которые могут появиться в ближайшем будущем.

Практические занятия со студентами вели преподаватели в области ИБ и специалисты «Ростелеком-Солар». Технологические решения, необходимые для подготовки обучающего модуля «Кибербезопасность АСУ ТП», предоставили партнеры «Ростелеком-Солар» — компании «ИнСАТ», UserGate и Positive

Technologies. Это позволило максимально приблизить лабораторную базу, на которой происходит обучение студентов, к инфраструктуре реального промышленного предприятия.

— Программа основана на включении самых сильных студентов российских университетов в выполнение наиболее актуальных разработок российских компаний — лидеров технологического развития в Российской Федерации, — считает руководитель фонда «Талант и успех» Елена Шмелева.

— Как лидеры рынка мы должны приложить все усилия к созданию эффективной общенациональной программы, нацеленной на развитие талантов и формирование кадрового резерва в области информационной безопасности. Образовательные проекты «Ростелекома» выполняют эту задачу через це-

почку взаимодействия «школа — вуз — работодатель». Следуя этой концепции, в прошлом году мы провели смену по кибербезопасности для одаренных школьников старших классов, в этом году она ориентирована на студентов, лучшие из которых в дальнейшем попадут на стажировку в центр мониторинга и реагирования на кибератаки Solar JSOC, — отметил вице-президент ПАО «Ростелеком» по информационной безопасности, генеральный директор компании «Ростелеком-Солар» Игорь Ляпунов.

Заключительным этапом образовательной программы стало тестовое задание, в ходе которого студенты должны были изменить иллюминационную подсветку «Колеса Времени» в Сочи Парке. «Колесо Времени» — один из самых высоких аттракционов в России,



его высота — 57 м, в его иллюминации задействовано 10 тыс. диодных модулей подсветки.

Для киберучений ИТ-специалисты Сочи Парка создали отдельную инфраструктуру, имитирующую сеть управления автоматикой аттракциона. По легенде, во время замены части оборудования системы автоматизации подсветки колеса обозрения наладчики установили временный ненадежный пароль в настройках Wi-Fi. Атакующий, время от времени проверявший защищенность сетей Wi-Fi парка, обнаружил этот факт, проник в инфраструктуру и добрался до сети устройств подсветки колеса обозрения. После этого злоумышленник сменил все возможные пароли: к точке доступа и интерфейсу настройки коммуникационных устройств, компьютеру с системой управления. После первых перенастроек оборудования и ПО атакующий просканировал устройства внутри другой сети и нашел контроллеры системы управления, отключил подсветку колеса обозрения, испортив текущий сценарий на сервере подсветки, а также отключил питание элементов подсветки через протокол Modbus TCP на двух устройствах. Далее атакующий смог перехватить трафик от системы управления подсветкой колеса обозрения, авторизоваться с привилегированным

доступом на сервере и сменить пароль даже там.

И в этом месте к работе приступили команды победителей олимпиады «Кибервызов: Новый уровень». На восстановление доступа к инфраструктуре после атаки отводилось около двух часов, на попытки включить иллюминацию и расследовать инцидент — по одному часу.

Киберучения прошли в форме соревнования CTF (Capture The Flag): команды одновременно пытались выполнить поставленные задачи и как можно раньше сообщить об их выполнении организаторам соревнований. Победила сборная команда «Speedrun Кибервызова», которая справилась с задачей за 3 часа 27 минут.

— Для прохождения испытания участникам потребовался широкий спектр знаний сетевых технологий, информационной безопасности и решений в области автоматизированных систем управления технологическими процессами. Задание финала нельзя назвать простым, и Сочи Парк организовал площадку для испытаний, безусловно поддерживая образовательные проекты и предоставляя талантливым ребятам возможность проявить себя. Максимальная открытость технологического процесса на испытании «Кибервызов: Новый уровень» обуслов-

лена еще и тем, что мы гордимся инновациями Сочи Парка и заинтересованы принять участие в воспитании квалифицированных специалистов, привлечь интерес к нашей компании, как к потенциальному работодателю в области АСУ ТП и ИТ-технологий. Мы готовы реализовывать совместные проекты и в дальнейшем, — отметил начальник управления информационных технологий и программного обеспечения АО «Сочи-Парк» Константин Кареев.

Студенты, успешно освоившие программу, приглашены на стажировку в крупнейший российский центр мониторинга и реагирования на кибератаки Solar JSOC. А для следующих участников программы, школьников старших классов, планируется новый отборочный тур — олимпиада Кружкового движения Национальной технологической инициативы (КД НТИ) по профилю «Информационная безопасность». Победители этой олимпиады также смогут получить 100 баллов за ЕГЭ по одному из профильных предметов (математика или информатика по выбору вуза) при поступлении в ведущие инженерные вузы России.



Артем ЗУБКОВ
директор Фонда содействия
развитию безопасных
информационных технологий
(ФСРБИТ)

ТАКОМУ В ШКОЛЕ НЕ НАУЧАТ

ОТРАЖЕНИЕ АТАКИ КАК СПОСОБ ПРОФОРИЕНТАЦИИ

На отраслевых форумах из года в год констатируется нехватка специалистов. С той или иной эффективностью многие компании пытаются наладить взаимодействие с вузами, вовлекая старшекурсников в рамках практик, стажировок и других, ставших привычными, форм поиска будущих сотрудников. При этом технологии кадрового укрепления отрасли ИБ в целом на уровне системы высшего образования реализуются преимущественно через обновление образовательных стандартов и распределение бюджетных мест в вузах по соответствующим специальностям. Но можно ли улучшить ситуацию простым увеличением числа мест? Даже если пропустить мгновенно возникающий в сознании аргумент «денег нет», то всё равно останется «а где взять столько желающих, да ещё и адекватных абитуриентов?».

Наш Фонд поддерживает разнообразные мероприятия по профессиональной ориентации в направлении отрасли ИБ. Прежде всего, это профильные олимпиады и другие интеллектуальные соревнования. Старшеклассники, участвующие в них, образуют удачную, перспективную целевую аудиторию для такой деятельности.

В частности, по сложившейся традиции, Фонд организует в московском регионе торжественное закрытие Межрегиональной олимпиады школьников

им. И. Я. Верченко, проводимой по профилям «математика и криптография» и «компьютерная безопасность». Сценарий подобных мероприятий давно сложился и на протяжении многих лет считался единственно возможным: разбор решений сложных задач, представленных на олимпиаде, вручение дипломов призёрам и несколько ярких выступлений представителей профильных вузов, науки и промышленности.

И всё же такая программа казалась нам не вполне завершённой — она не давала школьникам живого представления о профессии. Поэтому в этом году мы дополнили программу закрытия олимпиады принципиально новым, на наш взгляд, форматом. Для участников была проведена виртуальная экскурсия по киберполигону кафедры № 252 МИРЭА.

Экскурсия состояла из двух частей. В ходе первой школьникам рассказали о компьютерных атаках, ГосСОПКА и устройстве учебного киберполигона.

Вторая часть, практическая, проходила после вручения дипломов победителям и больше напоминала деловую игру. Ребята разбились на группы по 2–3 человека. Каждой группе был выделен наставник из числа студентов 5 курса, обучающихся на кафедре. Задача юных олимпийцев состояла в том, чтобы вникнуть в актуальные проблемы ИБ и содержание обучения по специальности «Компьютерная безопасность», но главное — студенты должны были сами провести увлекатель-

ную демонстрацию будней ИБ-шника, отражая на киберполигоне приближённые к реальным компьютерные атаки на предприятие ТЭК. Понятно, что происходило это в рамках одного из заложенных в киберполигон сценариев.

Как это выглядело на практике, учитывая явный выход тематики за рамки школьной программы? Наставники давали подопечным подробные подсказки, как выявить ключевые события в потоке сетевого трафика, а затем устранить выявленную уязвимость. Малые группы и относительно небольшая разница в возрасте со студентами, безусловно, способствовали неформальному общению, позволяли задавать вопросы и получать ответы по всему ходу демонстрации-игры.

Интерес школьников к этому действу был неподдельным, и результаты вполне оправдали наши ожидания. Всего виртуальную экскурсию посетили около 50 участников торжественного закрытия олимпиады.

* * *

Таким образом, предложенный новый формат успешно прошёл апробацию и пополнил арсенал профориентационных методик, направленных на повышение осознанности выбора школьниками отрасли «информационная безопасность» как будущей сферы профессиональной деятельности.



Валентин ЗЯЗИН
профессор кафедры
№ 252 РТУ МИРЭА

КИБЕРПОЛИГОН В МИРЭА

«ГОТОВИМ СПЕЦИАЛИСТОВ ДЛЯ ГОССОПКА»

Об уникальной методике практического обучения в сфере ИБ рассказывает один из её авторов — профессор кафедры № 252 РТУ МИРЭА¹ Валентин Зязин.

— В чём особенности обучения студентов на вашей кафедре?

— В период образования нашей кафедры, а это было более 20 лет назад, в МИРЭА уже существовала многолетняя практика работы базовых кафедр. Все они были ориентированы на подготовку молодых специалистов для промышленных и научно-исследовательских организаций. В советские годы это реализовывалось через распределение выпускников, сейчас действует аналогичный правовой механизм — приём

на целевое обучение. На нашу кафедру абитуриенты поступают и на «обычные» бюджетные места.

Особенности образовательной программы определяются двумя факторами. Во-первых, это требования Федерального государственного образовательного стандарта «Компьютерная безопасность», предполагающего значительно больший объём дисциплин математического цикла по сравнению с другими специальностями и бакалавриатом по ИБ. Во-вторых, с 2014 года кафедрой проводится работа по профилизации обучения в интересах кадрового обеспечения ГосСОПКА. Была проведена корректировка учебного плана. При этом учитывались требования профессионального стандарта «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», принятого в 2015 г, а также целевые установки регуляторов. Изменения внесены в программы таких дисциплин и их блоков, как организационное и правовое

обеспечение ИБ, программирование, администрирование и обеспечение безопасности сетей, ОС и СУБД. Также введены новые дисциплины «Системы обнаружения компьютерных атак и вторжений», «Предупреждение, выявление и установление причин и условий компьютерных инцидентов» и др.

Значительное внимание было уделено совершенствованию практической части обучения. На кафедре развёрнут специализированный комплекс учебно-тренировочных средств, позволяющий проводить на старших курсах лабораторные практикумы и учения в условиях, приближённых к реальным. Для краткости его называют киберполигоном.

Таким образом, созданы необходимые условия для обучения специалистов в интересах ведомственных и корпоративных центров ГосСОПКА.

— Термин «киберполигон» используется довольно часто, но может подразумевать совершенно разные по

¹ В состав института кибернетики РТУ МИРЭА входит базовая кафедра № 252. С 1997 года ведётся обучение по специальности 10.05.01 «Компьютерная безопасность», специализация «Анализ безопасности компьютерных систем». Срок обучения 5,5 лет. Ежегодный набор на обучение за счёт бюджета — около 70 человек.

составу и назначению технические средства. Расскажите, пожалуйста, подробнее, что такое киберполигон кафедры, как строится его работа, какова материально-техническая база.

— С технической точки зрения киберполигон — это достаточно мощная вычислительная система, способная поддерживать одновременную работу более 100 виртуальных машин, осуществлять хранение данных (виртуальных образов, резервных копий, документации) объёмом более 10 Тб.

Созданное специально для киберполигона программное обеспечение поддерживает виртуальную модель предприятия ТЭК. Эмулируется информационная инфраструктура и процессы предприятия (включая реалистичный фоновый информационный обмен между пользователями и сервисами), атакующие воздействия. Также реализуются функции управления учебным процессом (визуализация сценариев атак, оценка результатов обучения, восстановление виртуальной модели предприятия перед началом учений).

Разработка этого ПО проводилась специалистами ЗАО «Перспективный мониторинг». Преподаватели кафедры активно участвовали на всех этапах разработки, начиная с подготовки раздела технического задания, описывающего планируемую методику обучения. Для этого были проанализированы и учтены преимущества и недостатки известных подходов. Особенности методики являются: реалистичность, оборонительная направленность заданий, состыкованность с содержанием учебных дисциплин и сроками их прохождения, высокая степень вовлечённости обучаемых и соревновательная атмосфера.

Промежуточные версии разрабатываемого ПО апробировались непосредственно на киберполигоне кафедры, что позволило в 2018 году получить качественное и готовое к применению в учебном процессе изделие.

Создание киберполигона кафедры ведётся с 2014 года. С учётом опыта обучения совершенствуются методические материалы, обновляются учебные сценарии атак. Разумеется, постоянного внимания и обслуживания требуют и технические средства.



Сергей НЕЙГЕР

менеджер по развитию
бизнеса компании
«Перспективный мониторинг»

ПЛАТФОРМА ПОДГОТОВКИ ПЕРСОНАЛА AMPIRE

Площадок, где могут тренироваться хакеры, много. Площадок для тренировок «безопасников» почти нет. В компании «Перспективный мониторинг» решили исправить эту ситуацию.

ЛЮДЕЙ НЕТ, НО МЫ ДЕРЖИМСЯ

В марте 2019 года были опубликованы результаты исследования¹, проведённого в социальных сетях накануне крупной конференции Infosecurity Europe 2019. Более половины опрошенных посчитали, что основной угрозой безопасности информации является дефицит профессиональных навыков ИБ-департаментов. С этой же «проблемой наличия навыков» сталкиваются и HR-департаменты при наборе сотрудников в отделы информационной безопасности.

Аналогичное наблюдение есть и по России. За четыре года проведения цикла конференций «Будни информационной безопасности», организатором которого является АО «ИнфоТекС», специалисты «Перспективного мониторинга» объездили почти четыре десятка городов в различных регионах. И очень часто слышали: «Мы хотим построить службу мониторинга событий и реагирования на инциденты, но лю-

дей нет». И нет центров компетенций, где таких сотрудников можно было бы готовить.

HARD? SOFT? WARE? SKILLS?

Очевидно, что без технического и методического обеспечения центр мониторинга не может работать. И сотрудники также должны обладать необходимыми навыками. «Жёсткие» навыки (те, которым можно научить и которые можно измерить) для сотрудников службы мониторинга — это знание технологий атаки и защиты, знание и умение применять средства защиты информации и другие инструменты. Личные качества (т.н. soft skills) — навыки командной работы, умение взаимодействовать с другими членами группы мониторинга и реагирования на инциденты, навыки тайм-менеджмента.

Подтянуть матчасть можно на курсах производителей оборудования или ПО, можно самостоятельно изучить доступные материалы, вебинары, live-demo. Но это будут сильно теоретизированные знания, зачастую оторванные от реальной ситуации, от того, с чем ежедневно работают центры мониторинга ИБ. И проблему развития soft skills такой подход не решает никак.

Проблему получения навыков командной работы и продуктивного взаимодействия между ИТ- и ИБ-направлениями успешно решают киберучения: со сценарием, с вводными,

¹ https://safe.cnews.ru/news/top/2019-04-29_kiberbezopasnost_evropejskih_predpriyatij_pod

Мы не пропагандируем культ хакерства, а даём возможность обучающимся действовать с позиций сотрудников SOC-центра компании

— В чём отличия применяемой методики обучения от популярных в студенческой среде соревнований CTF?

— Процесс обучения начинается с отработки навыков оценки защищённости информационной инфраструктуры. Обучаемым предоставляется доступ к внутренним сервисам и рабочим станциям виртуальной модели предприятия, а также комплект учебной технической документации (логическая и физическая схемы сети, паспорта ключевых рабочих станций и серверов, матрица доступа, политика безопасности и т.д.). На этом этапе проводятся стандартные мероприятия по оценке защищённости: проверка полноты и актуальности предоставленных документов, выявление «нелегально» установленного программного обеспечения, поиск уязвимостей, проверка корректности настроек оборудования, общесистемного и прикладного ПО. Одновременно решается ещё одна важная задача — знакомство обучающихся с защищаемой инфраструктурой. Тем самым происходит «погружение» в контекст учений.

Последующие этапы предполагают решение задач по мониторингу компьютерных атак и по реагированию на компьютерные инциденты. Для этого обучаемые делятся на группы и отрабатывают совместные действия при атакующих воздействиях, развивающихся по разработанным сценариям.

Группа мониторинга, по сути, представляет собой первую линию SOC, их задача — выявление и фиксация компьютерных инцидентов. Оценка деятельности данной группы осуществляется на основе количества заполненных карточек инцидентов, а также качества их заполнения (полнота описания, точность рекомендаций). Группа реагирования соответствует подразделению ИТ/ИБ компании, их задача: получая сообщения от группы мониторинга,

принимать меры по реагированию и устранению причин инцидентов.

Немаловажным фактором успешного прохождения сценариев является организация эффективного взаимодействия между группами мониторинга и реагирования.

В основном обучаемые работают самостоятельно, опираясь на подробные методические рекомендации, разработанные для каждого учебного сценария.

Реализуемая методика обучения на киберполигоне в чём-то действительно напоминает CTF, но имеет ряд принципиальных отличий. Во-первых, она ориентирована на «защитников», а не на «белых» хакеров. То есть акцент делается на отработке оборонительных навыков. Во-вторых, группы действуют внутри периметра предприятия, а не только снаружи. Им предоставлен полный доступ к элементам внутренней сети, включая коммутационное оборудование. Наконец, методика призвана воспитывать точность, внимательность, системность в применении средств защиты. Мы не пропагандируем культ хакерства (*атакующие воздействия полностью автоматизированы и запускаются преподавателем — Ред.*), а даём возможность обучающимся действовать с позиций сотрудников SOC-центра компании.

— Сколько человек одновременно может заниматься на этом полигоне, сколько по времени длится прохождение одного сценария?

— Полигон рассчитан на одновременную работу четырёх групп по 3–4 человека. Сложность сценариев подобрана из расчёта возможности их прохождения за 4 часа. При этом, несмотря на высокую производительность оборудования, требуется довольно большое время на перезагрузку виртуальной модели предприятия — около 40 минут. Поэтому за один день группа может пройти не более двух сценариев, с перерывом на обед.

— Какие возможности, помимо обучения студентов, имеет киберполигон?

— В первую очередь рассматриваемая методика ориентирована на студентов старших курсов специальности «Компьютерная безопасность». Изучаемые ими дисциплины дают необходимые теоретические сведения и практические навыки, которые комплексно используются и закрепляются в ходе учений на киберполигоне.

В позапрошлом году нами были разработаны две программы повышения квалификации по противодействию компьютерным атакам. Разумеется, что курсы рассчитаны на подготовленную аудиторию, имеющую профильное образование и опыт работы: администраторов безопасности, системных администраторов и т.п. В связи с выходом за прошедшее время большого числа новых правовых и методических документов создана ещё одна программа — по организационно-правовым основам ГосСОПКА.

Таким образом имеются наработки по обучению на киберполигоне как студенческой, так и «взрослой» аудитории.

— Можно ли масштабировать и тиражировать этот опыт или он прикреплён исключительно к киберполигону кафедры?

— С учётом успешного опыта разработки нашего киберполигона «Перспективный мониторинг» продолжает развиваться это направление деятельности. Поэтому при наличии достаточного финансирования можно строить аналогичные комплексы, приобретая необходимое оборудование и программное обеспечение. Думаю, что по этому пути пойдут только крупные отраслевые образовательные организации. Им потребуется разработать специализированные виртуальные модели и сценарии отражаемых атак, а также встроить в свой киберполигон средства защиты, используемые в соответствующих ведомственных центрах ГосСОПКА.

Но в любом случае необходимо наличие подготовленного преподавательского состава и инженерного сопровождения учебного процесса на киберполигоне.

с измеряемыми результатами. Но и в этом случае можно столкнуться с двумя важными ограничениями. Первое ограничение связано с невозможностью провести киберучения на «боевой» инфраструктуре. Если что-то пойдёт не так, есть риск нарушить бизнес-процессы. Второе ограничение — необходимость привлекать атакующую сторону. Если стоит задача повысить практические навыки защитников, то в киберучениях должен быть элемент противостояния компьютерным атакам. Да, на рынке есть услуга Red Teaming'a, но она дорого стоит, и её заказывают организации с высоким уровнем зрелости в области обеспечения информационной безопасности. Такие ограничения вызывают к созданию киберполигонов: с максимальным уровнем автоматизации и максимально повторяющих реальные инфраструктуры.

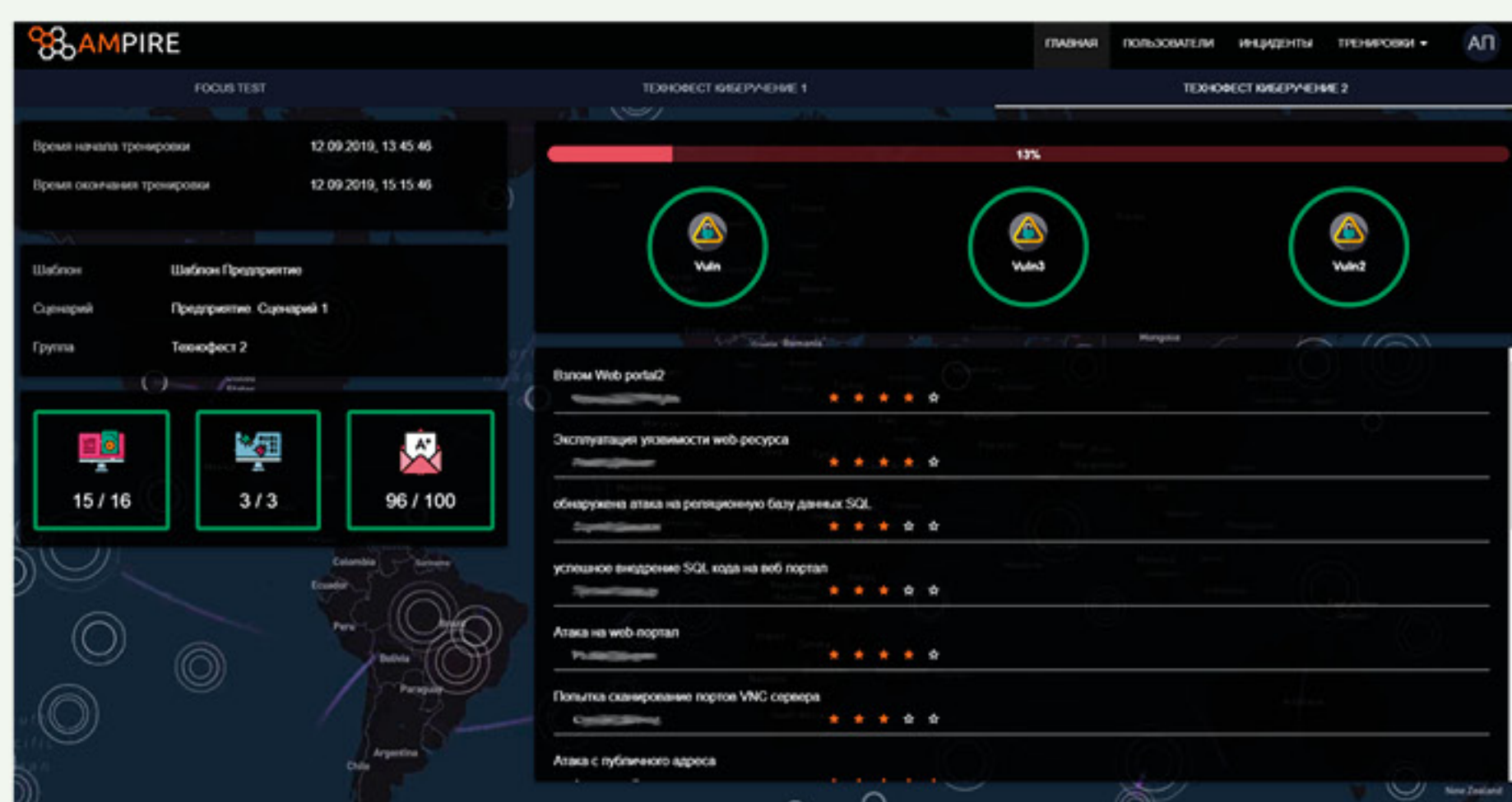
УЧЕБНО-ТРЕНИРОВОЧНАЯ ПЛАТФОРМА

AMPIRE — это программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак. Участники киберучений на AMPIRE примеряют на себя две роли — сотрудников групп мониторинга и реагирования.

Платформа AMPIRE — это смоделированная виртуальная инфраструктура организации, состоящая из нескольких сегментов: сетевая инфраструктура, ЦОД, ДМЗ, АСУ ТП, сегмент пользователей и разработчиков. В инфраструктуре могут быть развёрнуты средства защиты информации производства различных вендоров.

Группа мониторинга следит за событиями информационной безопасности, заводит карточки инцидентов, подтверждает инциденты, заведённые автоматическими средствами.

Группа реагирования выполняет рекомендации группы мониторинга, устраняет последствия инцидентов и «закрывает» обнаруженные уязвимости.



Пример дашборда, описывающего ход тренировки на AMPIRE

За проведение киберучений отвечает команда сотрудников «Перспективного мониторинга» — AMPIRE TEAM. Они помогают командам скоординировать действия и разобраться с особо сложными инцидентами и отвечают за работоспособность учебно-тренировочной платформы.

Основной сущностью киберучений на AMPIRE является так называемый «шаблон» — это смоделированная инфраструктура организации. Это могут быть предприятия ТЭК, телекома, банковской сферы.

Команда AMPIRE разрабатывает сценарии атак на эту инфраструктуру и полностью автоматизирует их. Таким образом в киберучениях не нужна дорогая команда нападения. Её роль играет автоматический атакующий.

Получив данные со средств защиты информации, группа мониторинга заводит карточки инцидентов, с которыми уже работает группа реагирования, и описывает вектора атак. Участники группы реагирования подключаются к узлам виртуальной инфраструктуры и предпринимают определённые шаги по устранению уязвимостей и последствий действий автоматического атакующего, включая изучение логов атакованных машин.

Задача команд в рамках отработки одного сценария — устранить все заложенные уязвимости и правильно описать действия атакующего в рамках kill chain.

В отличие от CTF-мероприятий (Capture The Flag) или деловых игр, при киберучениях на AMPIRE команды не соревнуются между собой. Да, можно выделять отдельных сотрудников «За лучшее описание инцидента» или «За первую заведённую карточку инцидента», но глобально команды преследуют другие цели:

1. получить навыки обращения со средствами защиты информации;
2. научиться выявлять атаки;
3. наладить взаимодействие между подразделениями.

* * *

В 2019 году AMPIRE TEAM «Перспективного мониторинга» провела две серии публичных киберучений. Первые из них состоялись в начале апреля в Салехарде, где Управление ФСТЭК России по Уральскому федеральному округу совместно с Департаментом специальных мероприятий и Департаментом информационных технологий и связи Ямало-Ненецкого автономного округа провели методический сбор по технической защите информации в органах власти Урала. Вторые киберучения состоялись в середине сентября в рамках однодневной технической конференции для специалистов по информационной безопасности ИнфоТеКС ТехноФест.

НАСТУПЛЕНИЕ ТРОЕЧНИКОВ?

ОБЗОР ВСТУПИТЕЛЬНОЙ КАМПАНИИ 2019/2020

АТТЕСТАТЫ «ПОДОРОЖАЛИ»

Ещё в августе ректоры многих университетов, подводя первые итоги вступительной кампании, отметили повышение баллов ЕГЭ в среднем по России. Выпускники школ 2019 г. сдали математику и физику лучше, чем выпускники предыдущего года. После успеха на ЕГЭ многие абитуриенты решили поступать в ведущие университеты Москвы и Санкт-Петербурга. С этим связывают и высокий конкурс — до тридцати и более человек на одно бюджетное место по направлениям «Информационная безопасность». Впрочем, отчёты о высоком конкурсе и рвущихся вверх проходных баллах традиционны для вступительной кампании, как и сообщения о популярности у абитуриентов специальностей юристов, экономистов и всех направлений IT.

В Высшей школе экономики по направлению специалитета 10.05.01 «Компьютерная безопасность» на 30 бюджетных мест были поданы 618 заявлений (в прошлом году — «всего» 412). На платные 45 мест претендовали 307 человек против 253 в 2018 г. В МФТИ на 10 бюджетных мест по той же специальности было подано 52 заявления (31 в прошлом году), на 5 платных — всего 19 желающих (9 в прошлом году). Но если в ВШЭ проходной балл за год вырос на 12 единиц (292 против 280), то в МФТИ он остался на прежнем уровне — 284 (283), значительно увеличившись для поступающих на платной основе. Тут проходной минимум баллов составил 251 против прошлогодних 221. И ещё одно различие. Оплата первого года обучения в ВШЭ выросла на 75 тыс.руб. (до 400 тыс. руб. в год), когда как в МФТИ она увеличилась незначительно, с 250 до 270 тыс. руб. в год.

Казалось бы, при таких высоких конкурсах на специальности по направлениям информационной безопасности, с учётом потребностей рынка число как

бюджетных, так и платных, мест должно расти. Но нет. Например, в МИФИ открыли дополнительно 10 бюджетных мест и 25 с компенсацией стоимости обучения по направлению 10.03.01 «Информационная безопасность» (бакалавриат), сократив при этом 15 бюджетных мест на специальности 10.05.04 (специалитет). Правда, по направлению 10.05.05 добавили ещё 5 мест на платной основе.

В МАИ сокращён приём абитуриентов на платные места по направлениям 10.03.01 (–20 бакалавров) и 10.05.02 (–5 специалистов). О фактическом отсутствии конкурса на платные места по большинству специальностей по ИБ можно говорить и в МИРЭА. Университет традиционно ведёт обучение почти по всем специальностям информационной безопасности. Судя по приказам о зачислении на первый курс, поступить в МИРЭА можно просто сдав ЕГЭ на минимальные баллы (в сумме от 120 баллов по математике, информатике и русскому языку) и заплатив чуть больше 220 тыс. руб. в год. Принятые на бюджетные места по конкурсу по разным направлениям ИБ набрали по ЕГЭ в два раза больше — от 240 баллов. Вопрос, как на одном потоке смогут учиться люди с таким разным уровнем базовой подготовки, в очередной раз остаётся открытым.

ХОРОШО ЗАБЫТОЕ СТАРОЕ

В этом году ВШЭ впервые провела набор на бакалавриат по направлению «Информационная безопасность» (10.03.01). «Программа направлена на подготовку специалистов, имеющих знания и навыки в области разработки, исследования и применения современных комплексных методов и средств защиты информации. Программа обеспечит выпускника соответствующими знаниями в математической, профессиональной, правовой области, професси-

ональной этике, а также практическими навыками проектной работы, позволяющими эффективно применять полученные знания в профессиональной деятельности. Выпускники программы смогут работать руководителями и сотрудниками фирм по разработке и выпуску средств защиты информации, оказывающих услуги по защите информации и выполняющих заказы по обеспечению информационной безопасности в различных сферах. Наиболее успешные студенты отбираются в качестве сотрудников ведущими кредитно-финансовыми организациями (Сбербанк, Газпромбанк, ВнешЭкономБанк), а также крупными государственными корпорациями (Ростелеком, Россети, Газпром)», — говорится на сайте ВШЭ. Как и на специалитете по ИБ, конкурс в бакалавриат превысил 20 человек на место, а проходной балл составил 288.

Новую форму обучения — очно-заочную для бакалавров (10.03.01) в дополнение к традиционной очной — предложил Лингвистический университет. Он традиционно пользуется популярностью у абитуриентов, несмотря на, казалось бы, гуманитарную направленность обучения. На 15 бюджетных мест очной формы обучения претендовали 414 человек (проходной балл 265, +8 к прошлому году), на 36 платных были поданы 287 заявлений. На 10 мест с компенсацией стоимости обучения в очно-заочной форме нашлось 55 желающих. Стоимость обучения в МГЛУ — 330 тыс. руб. в год (+90 тыс. руб. к цене 2018 г.).

Если удалиться от столицы, то наблюдается спрос на направления ИБ. Региональные университеты возобновляют приём на специальности по направлению 10.00.00, остановленный несколько лет назад. Так, в Северном Арктическом федеральном университете возобновился приём на «Информационную безопасность». На 17 бюджетных и 13 платных мест можно было

Вуз	Спец. по ИБ	Мест (бюд./пл.)	Заявлений (бюд./пл.)	Квоты на бюджет	Экзамены по ЕГЭ	Проходной балл 2019 г.	Проходной балл 2018 г.	Стоимость уч.года, тыс. руб (для сравн. 2018 г.)
ВШЭ	10.05.01 10.03.01**	30/45/1 ино 30/20	618/307 542/161	11 6	МИР МФР	292 288	280 нов. спец	400 (315) 400
НИЯУ МИФИ	10.03.01 10.05.04 10.05.05	30/30 15/15 -/10	420/72 194/37 -/2	3 2	МФР	287/212 270/222 -/217	272 275 278 (2017 г.)	258 (250,2)
МФТИ	10.05.01	10/5	52/19 (31/9)	1+3	МФР	284/251	283/221	270 (250)
МВТУ	10.05.01 10.05.03 10.05.07	15/14 30/26 нд	431 567 нд	6 13 нд	ФМР	288/192 288/166 нд	295 298 нд	302,533 (284,341)
МАИ	10.03.01 10.05.02	40/20 -/20	1065/116 /37	26	МИР	254/нд -/нд	245/153 -/171	208,550 (193,56)
РГГУ	10.03.01	30/10	468/94	3+3	МИР	224/164	216/138	249 (217)
МИИТ	10.05.01.65 10.03.01	17/13 17/43	337/49 (280/38) 462/82 (437/77)	2+4 2+2	МФР	225/156 230/162	215/167 217/160	215,2 (206,9)
МИРЭА	10.03.01 10.05.03 10.05.04 10.05.05 10.05.01 10.05.02	40/230 70/140 30/120 25/125 70/140 70/140	нд/540** нд/196** нд/124** нд/164** нд/205** нд/138**	4+4 7+17 3+3 3+3 7+29 7+29	МИР МФР МИР	259/120 248/124 244/185 249/143 241/150 245/181	247 233 232 227 226 229	221,250 (177 и 190 тр со скидками для недобравших баллы)
МГЛУ	10.03.01 10.03.01 оч-заоч.	19/36 -/10	414/287 -/55	2+2	М Иняз Р	265/нд -/нд	257/178 нов. напр.	330 (240)
СПбПУ	10.03.01 10.05.01 10.05.03 10.05.04	24/25 41/25 41/25 24/25	556/90 439/54 620/125 349/66	4 6 3 2	МФР МФР МИР МИР	268/168 257/179 261/179 260/182	247/нд 245/нд 248/нд 247/нд	191 (180)
ЛЭТИ	10.05.01	60/15	нд	1+1	МФР	262/нд	238/нд	166 (157)
СПбГУТ	10.03.01	17/60	нд/82**		МИР	нд	242/138	158
ПГУПС	10.05.03	15/35	363/15	3	МФР	198/нд	203/нд	203,8 (163,7)
РГГМУ	10.05.02	-/15	нд	-	МИР	-/нд**	-/131	202 (130)
СФУ	10.03.01 10.05.01 10.05.03	25/20 20/10 20/10	нд нд нд	3+3 2+5 2+4	МИР	235/нд 230/нд 219/нд	211 210 193	170,622 (154,306)
АлпГТУ	10.03.01	30/7	272/нд	4+4	МФР	198/148	198/157	109,5 (96,950)
АГУ	10.03.01	35/8	374/21	нд	МФР	200/нд	178/116	114,160 (99,5)
ДВФУ	10.03.01 10.05.01	25/5 23/5	нд/33 нд/13	2 1	МФР	195/147 178/169	189 189	210 (200)
ВГТУ	10.05.01 10.05.02 10.05.03	19/10 18/10 19/3	238/нд 134/нд 204/нд	2+5 2+5 2+4	МФР	205/нд 193/нд 203/нд	207 208 195	115,8 (103,8)
КБГУ	10.03.01	25/3	нд	2	МФР	нд	164	103,1
САФУ	10.03.01	17/13	нд	2	МИР	188/159	154 (2017 г)	117,420
КалГУ	10.03.01	17/3	96/7	2+2	МФР	188/133	-	От 77,910

* предусмотрена скидка для абитуриентов, не добравших баллы по конкурсу.
** по данным на конец августа

пройти, имея 188 и 159 баллов по ЕГЭ соответственно. Стоимость обучения в год — «всего» 117,42 тыс. руб.

Калмыцкий государственный университет им. Б. Б. Городовикова, спустя четыре года, возобновил набор на специальность «Информационная безопасность». Конкурс на 13 бюджетных мест составил почти 6 человек на место.

БЕГ НА МЕСТЕ

О дефиците кадров в области информационной безопасности не говорит только ленивый. Созданы государственные программы цифровизации, прогнозируются потребности экономики страны в IT-специалистах к 2020, 2025, 2035 годам... Однако какого бы то ни было увеличения числа мест в университетах по IT-направлениям не наблюдается. Более того, в большинстве вузов по различным специальностям в области информатики и программирования соотношение бюджетных и платных мест — 4:1 и групп по специализации как минимум две. В области ИБ комплектуется в лучшем случае одна группа, на 50–75% состоящая из бюджетных мест и 25–50% платных (как на IT направлениях). Такое соотношение характерно для многих региональных университетов. В Москве преобладают обратные пропорции: от 1:1 до 1:4 по числу бюджетников и платников.

С учётом ежегодного роста цен за обучение, ухудшения экономической ситуации в стране, конкурс на платное обучение высок только в столицах, чем и пользуются многие университеты. Стоимость обучения в ВШЭ и каком-нибудь периферийном вузе отличается в 3–4 раза. Часто в региональных университетах наблюдается недобор, а окончательные списки зачисленных на обучение с компенсацией его стоимости не сформированы до самого начала учебного года. Можно, конечно, сослаться на разницу в качестве обучения, но стандарт подготовки утверждён ФУМО по ИБ и, по идее, студенты получают одни и те же базовые знания

ИЗ МОСКВЫ

Принято считать, что за знаниями надо ехать в столицу. Однако тенденция обратная — абитуриенты из Москвы и Петербурга поступают в региональ-

О дефиците кадров в области ИБ не говорит только ленивый. Однако какого бы то ни было увеличения числа мест в университетах по IT-направлениям не наблюдается

ные вузы. Причин тут много — и конкурс меньше (4–7 человек на место против 20+ в столице), и проходной балл ниже (190–220, а не 280+), да и дешевле. И всё это при стандартной учебной программе. А с учётом некоторого падения престижности высшего образования (его необходимость всё чаще ставится под сомнение с высоких трибун) уже никто не смотрит на название университета, выдавшего диплом. Главное — знания. А как и где они получены, насколько хорошо усвоена программа, выяснится в процессе работы.

Например, большая часть поступивших в Владимирский госуниверситет — из Владимира и Владимирской области. Около 26% первокурсников — из Нижегородской, Московской, Ивановской и Рязанской областей. Схожая ситуация в Мурманском техническом университете. А в Новосибирском госуниверситете тенденция обратная. Около 40% абитуриентов — жители Новосибирска и Новосибирской области, 60% — жители других областей или стран.

Рост числа иностранных студентов с радостью отметили ректоры многих университетов, как по заказу подерживая мысль о престижности отечественного образования. О том, что в университете будут учиться представители Индонезии, Китая, Японии, Нигерии, Ирана, Ирака, Сирии, стран бывшего СССР и т.д. на итоговых пресс-конференциях отчитались представители вузов от Мурманска до Амура. Отчётами о таких мероприятиях была полна новостная лента конца июля.

Так ли это хорошо? Да, конкретный университет получает студента на платной основе, который (как полагают) будет гарантированно учиться. С другой стороны, этот студент часто занимает место российского абитуриента (если для иностранцев не выделены дополнительные места), который при успешной учёбе и защите диплома останется работать в стране.

ЦЕЛЬ ОПРАВДЫВАЕТ СРЕДСТВА?

В 2019 г. изменились нормативная база и регламент целевого набора в университеты. Перечень направлений, по которым может осуществляться целевой приём, утверждается Правительством РФ, а не соглашением между вузом и предприятием. Также повышается финансовая ответственность студента, которого отчислили за плохую учёбу или который отказался трудоустроиться после окончания вуза на предприятие заказчика. Впрочем, штраф грозит и предприятию в случае отказа трудоустроить выпускника.

Как показывает анализ приказов о зачислении абитуриентов по целевому приёму, лазейки поступить в вуз ищут выпускники с достаточно низкими баллами по ЕГЭ. И, как уже отмечалось, ни один университет не раскрывает статистику, сколько зачисленных на первый курс студентов с баллами ниже проходных, успешно завершили учёбу. И мало кто даёт статистику поступления. Например, в Университет ИТМО (Санкт-Петербург) на бюджетные места поступили абитуриенты со средним баллом по вузу 92,7, а средний балл поступивших по целевому приёму от предприятий — 82,9. Правда, на контрактной форме ситуация ещё хуже — средний балл всего 77,1.

Может быть, угроза финансовой ответственности и заставит кого-то учиться. Однако всё чаще опытные специалисты и педагоги старой школы сходятся во мнении: из почти хронического двоечника или тихого троечника, сдавшего ЕГЭ на 120–160 баллов, в результате учёбы в университете вряд ли получится квалифицированный специалист. Редкие исключения встречаются. На практике поступивший по целевому набору полудвоечник просто занимает чужое место, тем самым увеличивая общий конкурс на бюджет для тех, кто выбрал специальность самостоятельно, а не потому, что за него готово поручиться руководство какого-то предприятия.



Валерий КУЛИКОВ
обозреватель BIS Journal

БРИТВА ОККАМА¹ И ИБ

А НЕ ОТРЕЗАТЬ ЛИ ИБ-ОБРАЗОВАНИЕ КАК СЛУЧАЙНУЮ СУЩНОСТЬ?

Дежурный тезис ИБ-евангелистов в последние годы — утверждение о том, что отрасль ИБ должна черпать свои кадровые резервы из сферы ИТ. Удивительно, однако, что эта истина часто подаётся как откровение. Ведь подобный подход соответствует и здравому смыслу, и традициям инженерной культуры.

ИСТОРИЧЕСКИЙ ЭКСКУРС

Продукты ИТ — данные, информация, знания (далее *информация*) — появились намного раньше, чем ИТ в их нынешнем «цифровом» виде.

И уже работа с *информацией* в «аналоговом» виде (на бумаге и фото-, видео- и аудиоплёнках), потребовала для обеспечения ИБ помимо использования приёмов физической безопасности для поддержания должных уровней конфиденциальности и целостности (замки на дверях, сейфы и т.п.) создания целого пласта культуры соблюдения целостности и доступности («аналоговое» администрирование документооборота и архивирования); конфиденциальности (соблюдения режимов служебной и государственной тайны).

Но создание культуры «аналоговой» ИБ обошлось, выражаясь современным языком, без «хайпа» вокруг специализированных образовательных и проф. стандартов.

Носителями «аналоговой» культуры ИБ в нашей стране, например, были архивариусы и библиотекари, кадровики и сотрудники Первых отделов. В основе их работы лежали как технологии (административные и технические), так и черты характера — добросовестность, аккуратность, внимательность, честность и преданность Родине (особенно в случаях гостайны). Надлежащий уровень фундаментального образования и общей культуры вкупе с определённым психологическим складом позволял этим людям добросовестно выполнять инструкции, за строками которых фактически стояли метрики целостности-доступности-конфиденциальности.

И задолго до цифровой эпохи сформировались три эшелона защиты *информации*, существующие и поныне: оргмероприятия по классификации уровней доступа к информации; развитие у людей, работающих с информацией, чувства ответственности и понимания своей роли в системе ИБ; учёт юридических аспектов при работе с *информацией*.

Но в чём тогда причина появления «профстандартов» и специальных программ обучения для сферы ИБ эпохи цифровых ИТ? Похоже, что в появлении специфической сложной технической инфраструктуры для работы с *информацией*.

Да, инфраструктура новая. Но базовые принципы обеспечения ИБ не изменились! Их только необходимо адаптировать к новой ИКТ-реальности и контролировать надлежащее испол-

нение этих принципов в новой ИКТ-инфраструктуре. И кто, как не специалисты в сфере ИКТ, в первую очередь могут сделать это наилучшим образом! Если, конечно, не загонять их образование в узкие рамки «компетенций» бережливого болонского образования, а работу системы кибербезопасности не заменять «покером» риск-менеджмента, ломающего традиционные представления об инженерной культуре.

ИСТОЧНИКИ ЦИФРОВЫХ УГРОЗ ИБ

Пришедшие на смену «аналоговым» цифровые ИТ — это сложная техника, в которой манипуляции с *информацией* скрыты от человеческого взора, а работа техники описывается такими характеристиками, как вероятность отказа, среднее время наработки на отказ, требования к условиям окружающей среды, требования к электропитанию и т.п. Сложность «железа» сама по себе — это уже фактор негативного влияния на метрики ИБ.

Далее, цифровая техника ИТ — это, как правило, программируемое оборудование. Программное обеспечение ИТ — также источник негативного влияния на метрики ИБ. Причинами проблем может быть некорректный алгоритм работы с *информацией*, некорректная реализация корректного алгоритма, некорректная работа вполне корректной программы вследствие сбоя в питании «железа» и т.д. и т.п.

Сложная цифровая техника стала широко внедряться в специфических рыночных условиях, которые и поныне ха-

¹ Философский и методологический принцип, который гласит: «Не плоди сущности без нужды!»

рактируются глобализацией рынков и, как следствие, конфликтами технического мультикультурализма и общим падением культуры технических разработок в угоду таким требованиям бизнеса, как «бухгалтерская» эффективность и скорость выхода на рынок.

Внешние проявления этих конфликтов — снижение качества разработок (для «боевой» эксплуатации предлагаются продукты, фактически не прошедшие стадию опытной эксплуатации), снижение качества документации (в части полноты и актуальности) и техподдержки (языковые барьеры, перекладывание поддержки на региональные представительства, укомплектованные «ускоренно сертифицированными» специалистами). ПО до сих пор предлагается фактически на условиях согласия пользователя не предъявлять претензий к производителю в обмен на «своевременную» установку «заплаток».

При этом соблюдение «бухгалтерской» эффективности заставляет массу потребителей использовать в своей ИТ-инфраструктуре так называемые COTS-продукты и технологии. COTS — это англоязычная аббревиатура, обозначающая «коммерческие, с полки» предложения. Т.е. не разработанные под конкретные потребности заказчика, а отвечающие усреднённым требованиям. Среди проблем эксплуатации такого оборудования и ПО — повышенная вероятность ошибок, как следствие огрехов технической документации и низкой квалификации персонала, так и функциональных особенностей, выявленных лишь на этапе «боевой» эксплуатации.

Таким образом, в ходе начавшейся цифровизации ИТ возникли принципиально новые источники нарушения целостности и доступности информации вследствие:

- ♦ объективной технической сложности и новизны цифровых ИТ вкупе с субъективной природой недостатков большинства ИТ-разработок, прикрываемых флёром ссылок на технологии tick-tock, Copy Exactly!, Agile, Waterfall и подобные;

- ♦ необоснованной поспешности в проведении цифровой трансформации бизнеса в условиях объективного дефицита квалифицированных кадров, в том числе и ИТ-кадров.



«БУМАЖНАЯ» ИБ ЭПОХИ «БОЛЬШОГО ХАПКА»

Цифровая трансформация на этапе второго пришествия капитализма в Россию была и данью моде, и попыткой минимизировать влияние человеческого фактора на то, что теперь известно, как «бизнес по-русски». В контексте же нашей темы следует отметить, что особенностью очередного прихода капитализма в России стал кадровый состав бизнеса, его специфическая психология и квалификация «лиц, принимающих решения» и лиц, эти решения исполняющих. При этом изменились взгляды на ценность и структуру разного рода информации. Вспомним принципиально новые понятия «чёрной» и «белой» бухгалтерии, клиентские базы данных, получившие фактически гриф «Секретно» и т.п.

Бороться с новыми угрозами для информации в эпоху «приходящих сисадминов» и серверов с висящими «соплями» кабелей стали в первую очередь «бумажными» мерами — регламентами, инструкциями, политиками и проверками исполнения этой «нормативки».

Что было не лишено смысла, ибо иных способов воздействия на ситуацию на тот момент просто не было:

- ♦ отсутствовали инструменты для влияния на технологии ИТ и техническую политику формирования ИТ-инфраструктуры;

- ♦ «логистика» вороватой экономики предлагала и без того «сырое» ИТ-оборудование фактически без квалифицированной технической поддержки.

«Бумажные» технологии ИБ позволяли не только «латать дыры» угроз ИБ «по месту», но и сформировали, в конце концов, фундамент нынешней нормативной базы в сфере ИБ, а также элементы «общей гигиены» ИБ в виде технологий и регламентов резервного копирования, обеспечения бесперебойного питания, резервирования критических элементов ИТ-инфраструктуры и т.п.

ИТ В ИБ

Кроме угроз ИБ, связанных с качеством «волатильной» ИТ-инфраструктуры на основе COTS-технологий и качеством её «школярской» эксплуатации и

техподдержки в обособленных офисах, ситуация с ИБ стала раскачиваться в 21 веке из-за выхода цифровой трансформации на активный этап — формируются Интернет-экономика и соответственно возникают киберугрозы со стороны Всемирной Паутины.

Наиболее яркие моменты провалов в сфере ИБ по этой причине регулярно освещаются в деловых СМИ и инженерном «глянце». Поэтому имеет смысл обратить внимание лишь на то, что ныне инструментарий для кибератак всё чаще предлагается в «коробочном» варианте — сложились подходы к технической поддержке этого нового класса COTS-продуктов. Это, безусловно, огромная угроза для ИБ.

С началом активного внедрения Интернета в экономику совпало и появление «ИБ-специальностей» в программах вузов. Это было «в тренде» и потому стало одним из «плюсов» в конкурентной борьбе вузов.

Однако подобная отстройка ИБ от ИТ более чем сомнительна, ведь за каждой ИБ-угрозой стоит конкретный просчёт в ИТ-разработке и/или недостатки в эксплуатации ИТ-инфраструктуры. Даже негативное влияние на ИБ «человеческого фактора» можно демпфировать инженерно-административными методами «айтишной» природы.

«Светлой» стороной ситуации стало то обстоятельство, что становление хакерства способствовало приходу на рынок ИБ специализированных компаний, в штате которых значительную часть составляли «айтишники» — специалисты профессионально и системно знающие и исследующие ПО (операционные системы, инструментарий разработчиков приложений, популярные приложения классов COTS и Open Source, специализированный инструментарий хакеров) и (реже) аппаратные платформы ИТ.

COPY EXACTLY!

Тут уместно напомнить, что цифровые информационные технологии — это не единственная область техники, которая озабочена безопасностью своих продуктов и работы с ними, надёжностью своей инфраструктуры. И метрики безопасности вне ИТ до смешения

Подобная отстройка ИБ от ИТ более чем сомнительна, ведь за каждой ИБ-угрозой стоит конкретный просчёт в ИТ-разработке и/или недостатки в эксплуатации ИТ-инфраструктуры

похожи на те, которые стали привычными в ИБ.

Например, строительство или транспорт, имеющие гораздо более «древнюю» историю, нежели ИТ, также обладают опытом и технологиями для успешного управления процессами для поддержания всей своей «кухни» в надлежащем состоянии («целостность») для её бесперебойной работы («доступность» / с «точностью» до погодных условий и факторов непреодолимой силы), а также обеспечения квалифицированного допуска персонала к производству работ или управления объектами («конфиденциальность»).

Для этого в строительстве и на транспорте выстроены чёткие вертикали и горизонтالي управления безопасностью (в нынешней России — с некоторыми особенностями, которые следует отнести на счёт факторов пока ещё непреодолимой силы). Эти вертикали и горизонтали комплектуются специалистами с разными функциональными обязанностями (руководители, инспекторы-контролёры, аналитики, врачи, метрологи и прочие). Однако при этом в системе подготовки кадров нет специальных образовательных и «проф» стандартов для специалистов, занимающихся «Безопасностью».

Имеющийся и нарабатываемый опыт работы, знание и выполнение требований актуальных законов и нормативной документации вкупе с системной базовой образовательной подготовкой, профессиональные «лифты» и разумная ротация кадров — вот залог успешной работы людей в системе обеспечения безопасности в сфере техники и технологий. Безопасность в значительной степени не результат воплощения в жизнь специализированных теоретических исследований (хотя и этому есть место), а накапливаемый и осмысливаемый опыт, а также здравый смысл, базирующийся на образовании и снова на опыте.

И это справедливо не только для авиации с космонавтикой, но и для ИБ эры цифровых ИТ. Вполне логично формировать кадры ИБ эры цифровых ИТ (обозначим их «нестандартной» аббревиатурой ИБ&ИТ) из «культурных айтишников», сложный ИТ-образовательный фундамент которых дополнен представлениями об «общечеловеческих ИБ-ценностях», к которым относятся 1) классификация информации; 2) «социальная инженерия»; 3) «культура» НТД&НПД.

То, что «классический айтишник» вполне успешно способен впитать эти дополнительные культурные ценности, свидетельствует опыт «Лаборатории Касперского», Positive Technologies, InfoWatch, Qrator Labs и др. Созданные в массе своей «железными» и «софтверными» айтишниками, эти компании обладают и компетенциями в «бумажной» ИБ, часто выступая в качестве соавторов или экспертов при разработке нормативно-технической документации в сфере ИБ.

* * *

Совместная работа специализированных ИБ&ИТ-компаний и «бумажных ибэшников» из отраслевых и госрегуляторов, а также выросшая культура «чистых» ИТ-компаний, предлагающих рынку аппаратно-программные платформы и отдельные «хардверные» и «софтверные» ИТ-продукты со встроенными технологиями ИБ-защит (например, SELinux, сопроцессоры криптографической защиты информации и т.п.), позволяют сегодня говорить о возможности и необходимости создания ИТ с «врождённым ИБ-иммунитетом». При этом складывается понимание того, что ИТ — это та сфера, откуда службы ИБ должны черпать свои основные кадровые силы. Что весьма логично вытекает из предыдущего опыта развития техники.



Борис СТОЛПАКОВ
историк криптографии, кандидат
физико-математических наук

ГЕНЕРАЛЬНАЯ РЕПЕТИЦИЯ ШТУРМА БЕРЛИНА

75 ЛЕТ НАЗАД НАЧАЛАСЬ ПОДГОТОВКА К ВЗЯТИЮ КЁНИГСБЕРГА

Последней репетицией перед штурмом Берлина стало взятие советскими войсками в апреле 1945 г. «бастиона германского духа», каким считался Кёнигсберг (ныне Калининград). Там, а не в столичном Берлине, короновали последнего короля Пруссии Вильгельма I, впервые создавшего в 1871 г. единое германское государство — Германскую империю. В основном с той поры и утвердилось представление о Кёнигсберге, как о духовном бастионе. Видимо, укреплению духовной прочности служили и мощнейшие бастионы и форты, опоясавшие главный город Восточной Пруссии в конце XIX столетия.

ИСТОЧНИК КАДРОВ И ИДЕЙ

Вместе с тем, Кёнигсберг издавна был связан с культурной жизнью соседних стран, в том числе России. Когда в 1725 г. в Петербурге занялись организацией Академии наук, из Кёнигсберга туда потянулась профессура местного университета, претендуя на академические звания. Достаточно упомянуть хорошо известного всем интересующимся математикой и криптографией Христиана Гольдбаха. С его именем свя-

зан первый громкий успех российских дешифровальщиков дипломатической корреспонденции, заметно отразившийся во внешней государственной политике. Гольдбах, перешедший в 1742 г. на службу в МИД, до 1765 г. возглавлял Криптографическую службу России. Другой петербургский академик, великий Леонард Эйлер, прославил Кёнигсберг своей статьёй 1736 г. о его мостах, что стало началом новой математической дисциплины — теории графов. Как известно, поводом для исследования послужила задача о семи мостах Кёнигсберга через реку Преголь: можно ли пройти каждый мост по одному разу и вернуться в начальное место? Илл. 1 даёт представление о расположении всех семи городских мостов.

ССЫЛКИ В ИНТЕРНЕТЕ — ТОЖЕ МОСТЫ

Мы знаем, что Эйлер дал отрицательный ответ на поставленный вопрос, весьма остроумно формализовав задачу при поиске решения. С той поры математики и криптографы постоянно используют в своих рассуждениях термины вершин и рёбер графов. Сфера их применения, как и у многих абстрактных понятий, гораздо шире самой мате-

матики. Так, невольно создают личные графы все пользователи Интернета, эти графы имеют своими вершинами посещаемые сайты, а их рёбрами являются выбранные ссылки. Подобные графы надолго сохраняются в сетевой памяти. К сожалению, из семи исторических мостов Кёнигсберга до наших дней сохранился лишь Деревянный, точнее, Дровяной мост. Его можно видеть на илл. 2. Там же, на заднем плане, возвышается знаменитый Кёнигсбергский собор начала XIV столетия.

Он сгорел во время бомбардировки в августе 1944 г., но ныне восстановлен. У соборных стен в огне уцелела могила Иммануила Канта. По соседству прошла его жизнь, рядом находился и Кёнигсбергский университет.

ПЕРВЫЙ РАЗ В РОССИЙСКОМ ПОДДАНСТВЕ

В прошедшие столетия Кёнигсбергу довелось однажды оказаться на несколько лет в составе Российской империи. Тогда город открыл свои ворота перед русской армией и присягнул императрице Елизавете Петровне. Это случилось в середине XVIII века, во время Семилетней общеевропейской войны, в которой Россия и Пруссия стали против-



**ФОНД
ПРЕЗИДЕНТСКИХ
ГРАНТОВ**

Публикация подготовлена с использованием средств гранта Президента Российской Федерации на развитие гражданского общества №18-2-012576, представленного Фондом президентских грантов.

никами. В ту пору в королевском замке вполне мирного Кёнигсберга некоторое время залечивал свои раны молодой подполковник Александр Васильевич Суворов, а генерал-губернатором Восточной Пруссии был его отец, Василий Иванович. Тогда же мало кому известный И. Кант послал своё первое прошение на профессорскую должность императрице Елизавете Петровне. Спустя полвека, в январе 1813 г., жители Кёнигсберга приветствовали русские войска, освобождавшие их от французской оккупации. К сожалению, в XX столетии немецко-русские отношения часто складывались иначе.

КАК РАДИОРАЗВЕДЧИКИ ПОМОГАЛИ ДИПЛОМАТАМ

В конце января 1945 г. советские войска приблизились к Кёнигсбергу и прервали его сухопутное сообщение с остальной Германией. Пришло время «бастиону германского духа» почувствовать мощь удара Красной армии, совершенно изменившейся за четыре военных года. К тому моменту советская радиоразведка стала давать командованию полную картину фронтового и тылового положения противника, часто позволяя вскрывать заранее его намерения. Случалось, эти намерения были направлены против бывших союзников Германии. Так, в сентябре 1944 г. радиоразведкой ВМФ была отмечена интенсивная радиосвязь немецкого военно-морского флота в Финском заливе и сосредоточение кораблей в районе эстонского г. Кунда.

«14 сентября радиоразведка в донесении предупредила о предстоящей высадке немецкого морского десанта на занятый финнами остров Гогланд, за два с половиной часа до её начала. Тогда юридически Финляндия находилась еще в состоянии войны с СССР. Всё же командование Балтийского флота (БФ) приняло решение связаться по радио с финнами» (1). Заблаговременное извещение способствовало организации совместно с финскими войсками обороны острова и срыву планов немецкого командования. Действительно, в ночь на 15 сентября немцы начали высадку десанта и встретили ожесточённое сопротивление финнов, поддержанных бомбардировщиками БФ.

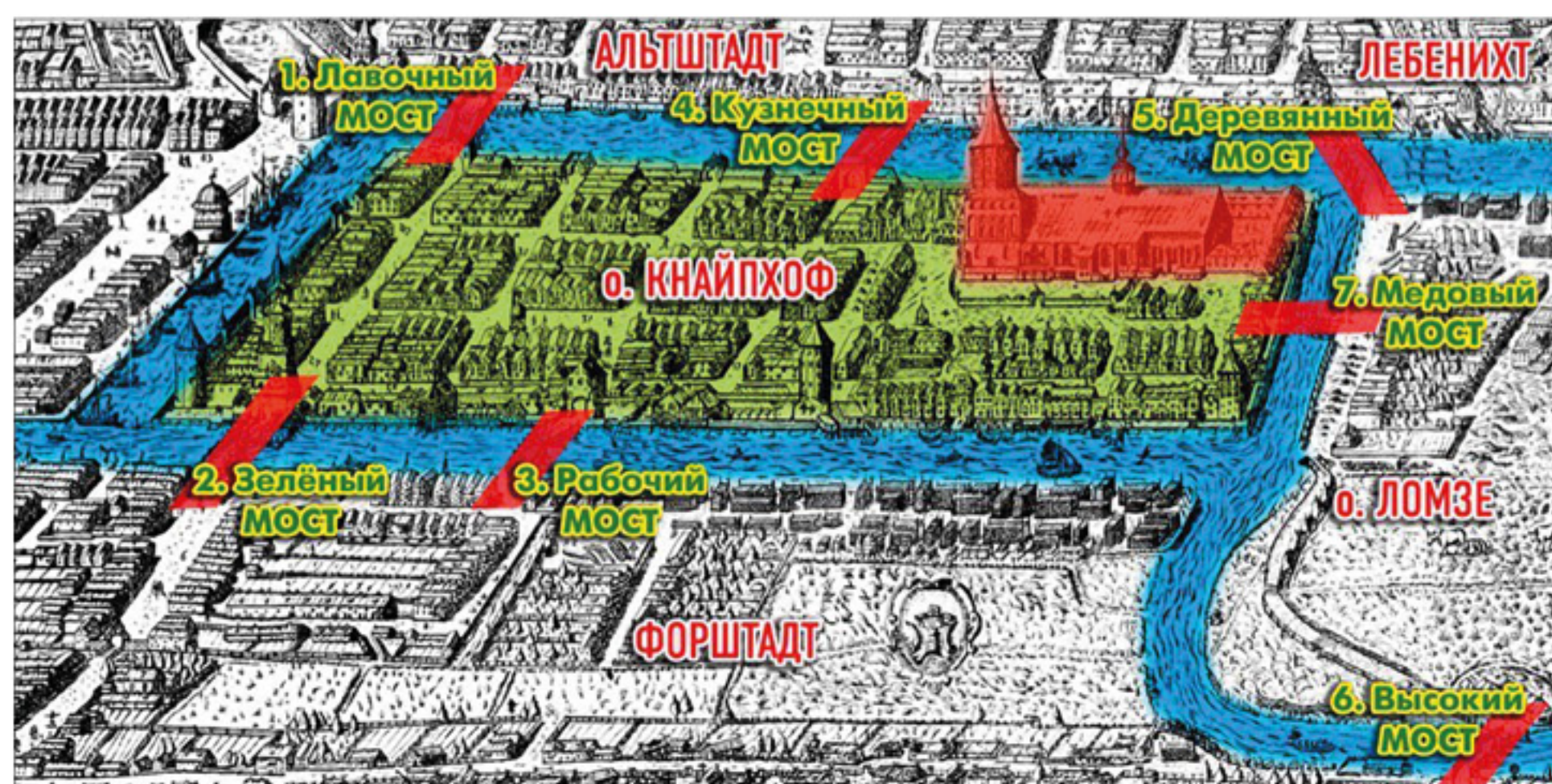


Иллюстрация 1. Семь мостов Кёнигсберга



Иллюстрация 2. Деревянный мост в начале XX века. На заднем плане виден о. Кнайпхоф, ныне о. Канта

16 сентября остатки полуторатысячного десанта сдались бывшим союзникам, а 24 сентября началась передача Гогланда советским войскам. Успех обеспечила своевременной обработкой данных перехвата флотская дешифровально-разведывательная служба (1). Заметим, что Гогланд играл весьма важную роль в системе немецкой морской обороны, занимая центральное положение в полосе минных полей и противолодочных заграждений, отсекавших Финский залив от остального Балтийского моря. Именно там советские лодки в подводном положении, сильно рискуя, пытались прорваться на просторы Балтики. И в дальнейшем радиоразведка способствовала успешному обмену сведениями с Финляндией. Ради-

оразведчики помогли предотвратить многие морские и сухопутные потери и обеспечили нанесение значительного ущерба противнику, наводя на врага авиацию и подводные лодки.

ЗАДАЧА — ПОДАВИТЬ РАДИОСВЯЗЬ ПРОТИВНИКА

Под Кёнигсбергом главной задачей радиодивизионов ОсНаз стало нарушение управления войсками окружённого противника путём подавления мощными помехами в эфире его радиосвязи. Поэтому в период подготовки штурма велось круглосуточное наблюдение за радиосетями противника с целью выявления основных и запасных частот вражеских радиостанций, их места расположения, войсковой принадлежности

и режимов работы. В результате, когда в течение первых суток штурма главная радиостанция окружённого гарнизона пыталась вести передачи последовательно на 43 частотах, то во всех случаях не достигла успеха, ибо каждая новая частота тут же забивалась советскими средствами радиоподавления (2).

«РАЗВЕДКА ДОЛОЖИЛА ТОЧНО»

Штурм готовили войска 3-го Белорусского фронта под командованием маршала А.М. Василевского. Все понимали моральное значение Кёнигсберга для немцев и важность быстрого успеха при штурме города. Поэтому к атаке готовились как никогда тщательно. Несколько десятков разведгрупп занимались разведкой Кёнигсберга и его пригородов на месте, каждая на своём участке территории. Разведчики действовали под видом власовских или немецких подразделений. Некоторые группы включали добровольцев из числа немецких военнопленных. Были и диверсионные группы, составленные из военнопленных, вошедших в организацию «Свободная Германия». Одним из её руководителей стал генерал В. Зайдлиц, пленённый в Сталинграде. Генерал О. Ляш, командовавший обороной Кёнигсберга, написал в своих

послевоенных воспоминаниях: «При господствовавшей в городе неразберихе, когда военные перемешались с гражданскими, русские, естественно, могли заслат в крепость многочисленных шпионов и составить себе точную картину нашего положения. Несомненно, противник не раз сбрасывал в Кёнигсберг на парашютах немецких военных и гражданских лиц. Кабель на улице Арндта прослушивался двумя представителями клики Зайдлица» (3). Надо сказать, что исторический центр города был сильно разрушен в результате бомбардировки английской авиации в августе 1944 г. Тогда в авианалёте, участвовали 189 бомбардировщиков в сопровождении сотен истребителей, город горел несколько дней.

К ШТУРМУ ГОТОВИЛИСЬ КАК НИКОГДА ТЩАТЕЛЬНО

Сведения, доставленные всеми видами разведки, после их анализа послужили основой для изготовления натурального макета. Его использовали при составлении плана штурмовой операции. Одновременно запланировали скользящий удар по Земландской группировке противника в направлении военно-морской крепости Пиллау (ныне Балтийск). На подступах и в самом Кёнигсберге предстояло преодолеть три мощных рубежа

обороны с водными преградами. При планировании уличных боёв упор был сделан на 26 штурмовых отрядов и 104 штурмовые группы из стрелковых частей и инженерных войск. По штурмовым подразделениям распределили большое количество огнемётчиков. В штурмовые отряды добавили по 1–2 танка и самоходному орудию, а также артиллерию, миномёты и пулемёты. Проводились тренировки штурмовых подразделений, приближённые к реальной обстановке предстоящих им операций.

Перед штурмом со 2 по 5 апреля (4 дня!) была проведена необычно мощная артиллерийская подготовка. Авиация при этом использовалась слабо из-за дождливой погоды. Вступили в бой постановщики радиопомех. Известно, что накануне штурма Кёнигсберга только 131-й и 226-й отдельные радиодивизионы ОсНаз эффективно заглушили 175 радиостанций противобойствующих частей врага, хотя те пытались вести работу в 30 радиосетях на 300 радиочастотах (2). Гражданское население до самого штурма имело возможность покинуть город в направлении балтийского побережья и Пиллау, чем большинство и воспользовалось.

«ВСЕ СРЕДСТВА СВЯЗИ БЫЛИ СРАЗУ ЖЕ УНИЧТОЖЕНЫ...»

Штурм Кёнигсберга начался утром 6 апреля. Генерал О. Ляш отметил в своих воспоминаниях: «6 апреля русские войска начали генеральное наступление такой мощи, какой мне не доводилось испытывать, несмотря на богатый опыт на востоке и на западе... В течение нескольких дней они беспрерывно засыпали крепость снарядами из орудий всех калибров и «сталинских органов» («катюш»). Волна за волной появлялись бомбардировщики противника...» (3). «Все средства связи были сразу же уничтожены и лишь пешие связные пробирались на ощупь сквозь груды развалин к своим командным пунктам или позициям» (3). Ход сражения показан на илл. 3.

Радиосвязь стала недоступна немцам из-за мощных помех в эфире. Всего по Кёнигсбергской группировке войск противника радиодивизионами ОсНаз был сорван приём около 1200, а по Земландской — 1000 радиogramм

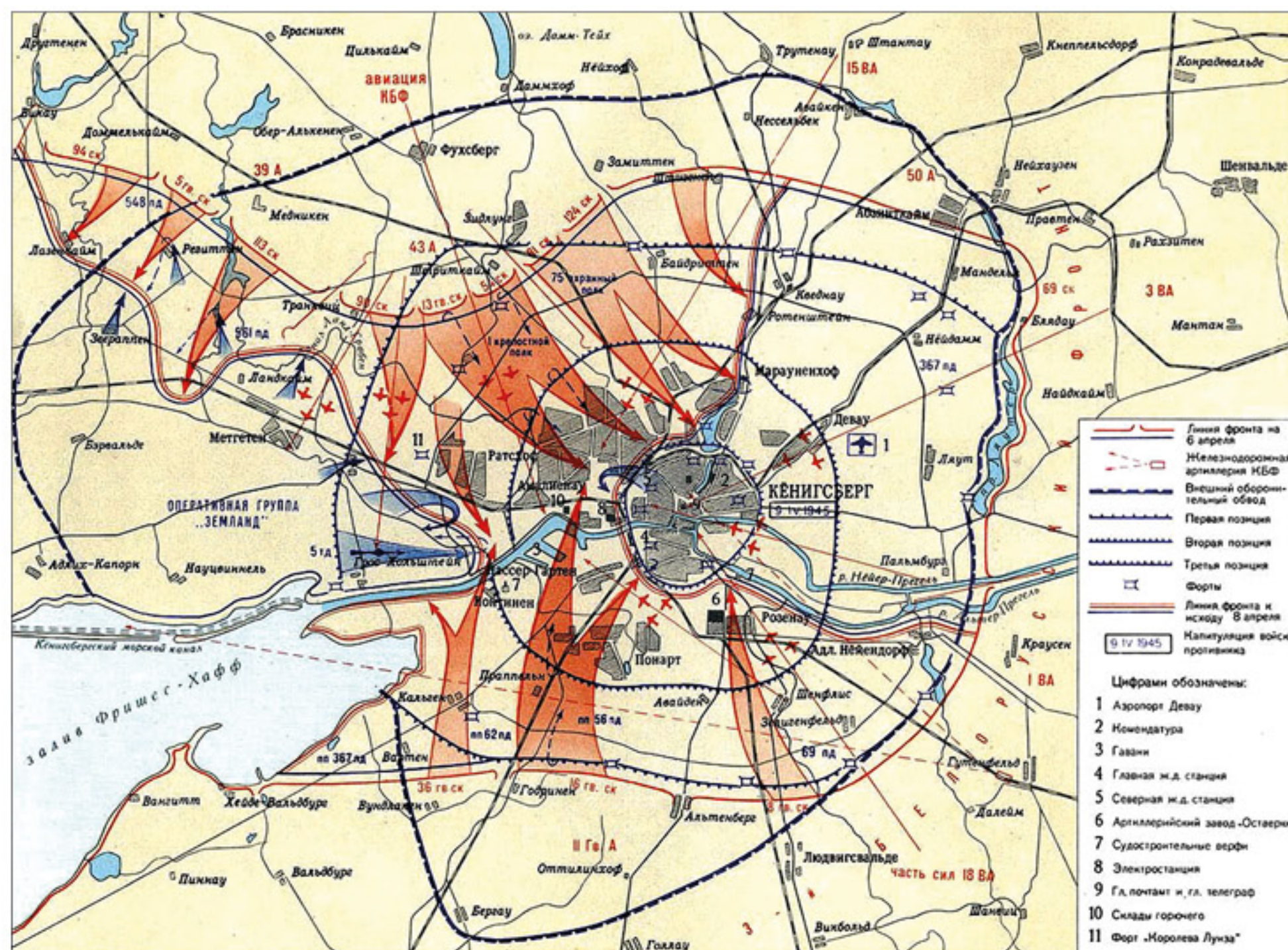


Иллюстрация 3. Рубежи обороны Кёнигсберга и их прорыв

(2). Характерно признание бывшего командующего войсками Кёнигсбергского гарнизона генерала О. Ляша, записанное с его слов на допросе сразу после пленения: «В результате ужасающей артиллерийской подготовки проводная связь в крепости была выведена из строя. Я надеялся на радиосвязь с Курляндией, с Земландской группировкой войск и с Центральной Германией. Но эффективные действия забивочных радиосредств русских не давали возможности использовать радиосредства для передачи радиogramм, и мои действия не могли координироваться ставкой верховного главнокомандования. Это послужило одной из причин моей капитуляции» (2). Это фактическое признание того, что было нарушено управление германскими войсками, ещё оборонявшимися на территории Восточной Пруссии.

БЕЗОГОВОРочная КАПИТУЛЯЦИЯ

Утром 9 апреля под контролем немецких войск остался лишь небольшой плацдарм в центре города, насквозь простреливаемый советской артиллерией. Стала улучшаться погода и авиация смогла совершить около 1500 вылетов на бомбардировку и штурмовку врага. По показаниям пленных штабных офицеров, подземный бункер штаба обороны уже едва выдерживал прямые попадания авиабомб и стал заливаться водой. Вот тогда генерал О. Ляш принял решение о прекращении сопротивления и отправил своих представителей для поиска контактов с советским командованием. А уже в 23:30 9 апреля 1945 г. Москва салютовала войскам 3-го Белорусского фронта, овладевшим крепостью Кёнигсберг.



Иллюстрация 4. Советская САУ ИСУ-152 «Зверобой» на улице взятого Кёнигсберга

Знаменательно, что приказ генерала О. Ляша о безоговорочной капитуляции был передан его войскам именно радиостанциями радиодивизионов ОсНаз. Они выдали приказ в эфир в ночь с 9 на 10 апреля открытым текстом на частотах немецких раций (2). Стремительное падение Кёнигсберга произвело на немцев удручающее впечатление. Генерала О. Ляша заочно приговорили к смертной казни, а его родственников репрессировали.

ПОБЕДИЛИ ПО-СУВОРОВСКИ

В Кёнигсберге настал весьма ответственный момент завершения военной операции. Теперь основная роль отводилась войскам НКВД. Надо сказать, что спецназ НКВД активно действовал уже в ходе штурмовых боёв. Он обеспечил своевременный захват здания государственного банка со всеми находившимися там ценностями и денежно-валютными запасами Восточ-

ной Пруссии, а также захват органов управления и разведки. Подразделения НКВД немедленно приступили к выявлению и захвату лиц, чьи показания потенциально могли представлять повышенный оперативный интерес. Незамедлительно была налажена охрана главных коммуникаций своих войск, поддержание порядка в тылу, а также работа пунктов приёма военнопленных, через них прошли 92000 человек, в том числе 8000 офицеров. С 11 по 19 апреля войска НКВД осуществили полную зачистку городской территории от остатков подразделений разбитого противника, ещё укрывавшихся в подвалах и руинах (2).

Теперь о потерях. Советские потери убитыми составили по современным данным 3700 человек. Для подобного сражения они невелики. Для сравнения: немецкие войска и фольксштурм потеряли убитыми 42000 человек; это больше, чем при штурме Берлина. Как пишут историки, при исходной приблизительно равной численности сторон победа была одержана по-суворовски: не числом, а умением.

* * *

ЛИТЕРАТУРА

1. Кикнадзе В. Г. Развитие сил и средств радиоразведки отечественного военно-морского флота в первой половине XX века: исторический опыт и уроки. Диссертация докт. ист. наук. Военная академия ГШ ВС РФ, 2014.
2. Лебедев А. Войска НКВД в боях за Кёнигсберг. Военное обозрение от 6 сентября 2012 г.
3. Ляш О. Так пал Кёнигсберг. М., 1991.

После нескольких дней передышки 3-й Белорусский фронт ликвидировал и Земландскую группировку противника, овладев 25 апреля 1945 г. городом Пиллау. В тот же день начался штурм Берлина.

ПОДВИГ РАДИОРАЗВЕДЧИКА

ПОД РУКОВОДСТВОМ ПЕТРА ШМЫРЕВА (1919–2009)
СОВЕТСКАЯ РАДИОРАЗВЕДКА ПРЕВРАТИЛАСЬ
ИЗ ФРОНТОВОЙ В СТРАТЕГИЧЕСКУЮ

3 октября 2019 года исполнилось бы 100 лет генерал-лейтенанту Петру Спиридоновичу Шмыреву, одному из создателей радиоэлектронной разведки СССР. Именно под его руководством радиоэлектронная разведка, начиная с 50-х годов, организационно и технически превратилась из фронтовой в стратегическую.

Пётр Спиридонович родился в Петрограде и после школы, в 1937 году, поступил в Военную электротехническую академию связи имени С. М. Буденного. Он попал в первую группу слушателей, которых готовили для работы в радиодивизионах особого назначения (ОСНАЗ).

Во время Великой Отечественной войны молодой радиоразведчик воевал в 623 отдельном радиодивизионе ОСНАЗ. Дивизион вёл радиоразведку на Карельском перешейке. К концу 1942 года его специалисты полностью

выявили сосредоточенную здесь группировку противника: места дислокации всех соединений Германии и Финляндии, аэродромы базирования финских ВВС и частей люфтваффе в Финляндии, Норвегии, а также в полосе действия войск Ленинградского фронта. Дивизион своевременно сообщал в штаб Ленинградского фронта о налётах вражеской авиации [Бурнусов, 2009].

Вот как заслуги Шмырева оцениваются в наградном листе от 16 апреля 1944 года: «При непосредственном участии П. С. Шмырева созданы ряд схем и конструкций, которые в значительной степени улучшили условия выполнения заданий командования фронта. Шмырев возглавил рационализаторскую работу в дивизионе, в результате чего многие образцы табельной аппаратуры модернизированы и в эксплуатации показали хорошие результаты... Достоин награждения орденом Красной Звезды» [Бурнусов, 2009].

Впоследствии дивизион работал на территории Румынии, Чехословакии, Венгрии, Югославии. «За этот период дивизионом была вскрыта дислокация более 100 аэродромов противника, на которых базировались свыше 40 частей ВВС Германии. Было зафиксировано более 30 тыс. самолёто-вылетов боевой и транспортной авиации противника. Вскрыта дислокация 30

крупных войсковых штабов сухопутных войск. Успешной боевой работе способствовала чёткая организация технического обеспечения, руководство которым осуществлял заместитель командира по технической части Пётр Шмырев».

А вот воспоминания самого Петра Шмырева: «Помню себя и своих товарищей — радиоразведчиков 1941 года, когда мы мало знали и ещё меньше умели. И вспоминаю их же и себя в 1943–1944 годах, когда радиооператоры знали по почерку чуть ли не всех немецких радистов, определяя по ним номера дивизий, корпусов, армий. Любая задача нашим радиоразведчикам была по плечу» [Бурнусов, 2009].

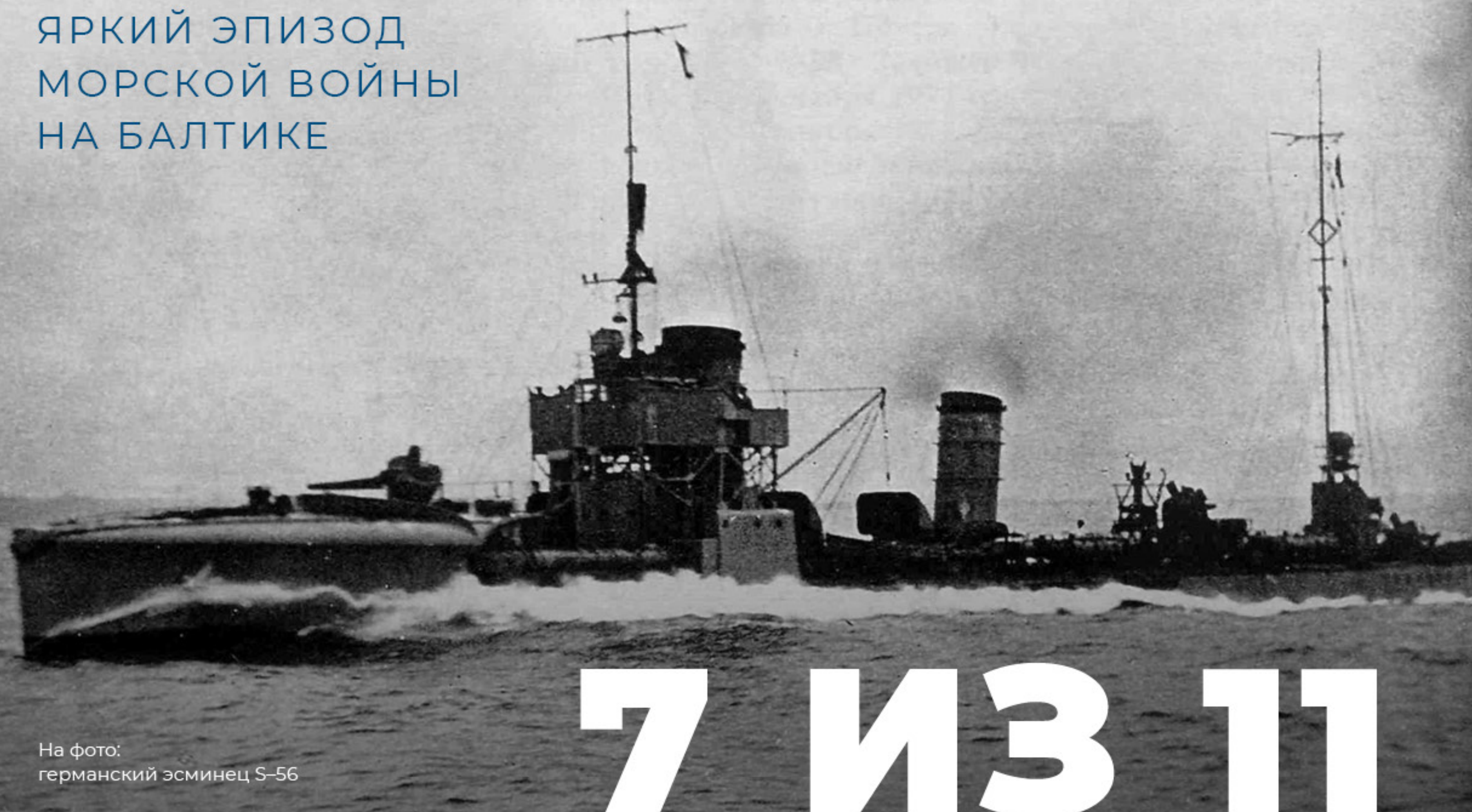
После Победы инженер-майор Шмырев продолжил военную службу в радиоразведке сначала в Болгарии, затем недалеко от Москвы и наконец в столице. В октябре 1954 года Пётр Спиридонович получил назначение в Главное разведывательное управление, в котором прослужил 32 года, пройдя путь от старшего офицера до начальника управления радиоразведки. С 1972 года в этой должности П. С. Шмырев прослужил 15 лет [Болтунов, 2011].



Петр Спиридонович Шмырев

ЛИТЕРАТУРА

1. [Анин, 1996] Анин Б. А., Петрович А. И. Радиошпионаж. М., «Международные отношения», 1996..
2. [Болтунов, 2011] Болтунов М. Е. «Золотое ухо» военной разведки. М.: Вече 2011. // <http://read24.ru/fb2/mihail-boltunov-zolotoe-uho-voennoy-razvedki>.
3. [Бурнусов, 2009] Бурнусов И. Мэтр радиоэлектронной разведки // Независимое военное обозрение № 35, 2009, с. 15.
4. [Ларин 2017] Ларин Д. А. Криптографическая служба России. Очерки истории. Монография. М.: Гелиос АРВ, 2017.
5. [Шмырев, 2004] Шмырев П. Часовые эфира (об истории радиоразведки). // Газета «Красная Звезда», 18 марта 2004 г. <http://offline.computerra.ru>.

ЯРКИЙ ЭПИЗОД
МОРСКОЙ ВОЙНЫ
НА БАЛТИКЕ

На фото:
германский эсминец S-56

7 ИЗ 11

Информационная безопасность, защита персональных данных... Эти слова мы слышим всё чаще. Вместе с тем, постепенно привыкаем к мысли, что все наши передвижения по поверхности земли можно автоматически проследить с помощью наших же, ставших такими привычными, мобильных телефонов.

ПЕЛЕНГОВАНИЕ И ПЕРВЫЕ РАДИОПЕЛЕНГАТОРЫ

Такую возможность создаёт использование явления, называемого радиопеленгованием. Ещё в 1906 году немецкий учёный Шейллер впервые применил изменение положения антенны для определения направления на источник пришедшей радиоволны. Антенная система Шейллера, сама не излучая, позволяла определить направление на источник излучения. Права изобретателя были защищены патентом.

Исторически раньше стали использовать явление радиолокации. Но первоначально радиолокаторы не привлекли к себе столько внимания, как чуть позже произошло с радиопеленгаторами. Ценное преимущество радиопеленга-

торов перед радиолокаторами заключается в отсутствии излучающей системы, а потому, в большей скрытности.

Конечно, идеи радиолокации и радиопеленгования обдумывались учёными и изобретателями одновременно во многих местах Старого и Нового Света. Конец XIX и начало XX столетий подарили человечеству много новшеств, связанных с радио. Как мы знаем, российские учёные, прежде всего А. С. Попов, были в числе первых, но предприимчивости во внедрении им явно не хватало.

В России в предвоенный период опытные работы по радиопеленгованию активизировались и, буквально в самом начале Первой мировой войны, командованием Балтийского флота было принято решение об установке в Кильконде на о. Эзель первого разведывательного радиопеленгатора (РРП). Идею этого РРП предложил И. И. Ренгартен, им же была разработана и сама конструкция.

Первый береговой РРП системы Ренгартена имел антенну зонтичного типа, состоящую из 16 лучей-радиусов, ориентированных на местности согласно ком-

пасным румбам, отсюда его наименование «радиостанцией компасного типа». С помощью радиопеленгатора в Кильконде моряки начали решать разведывательные задачи 8 сентября 1914 года. А уже 12 октября ввели в действие второй РРП — в Гангэ, на северном побережье Финского залива, затем 12 ноября — третий — на о. Даго (оба РРП — на 32 луча). В 1916 году действовали уже 10 РРП и 10 станций радиоперехвата в различных местах побережья Балтики. Линиями связи они были объединены в единую сеть.

Эта сеть, руководимая Службой связи Балтийского флота, не раз демонстрировала свою боевую эффективность.

ПОРАЗИТЕЛЬНЫЕ СВИДЕТЕЛЬСТВА ДЕЖУРНЫХ РАДИОРАЗВЕДЧИКОВ

Сейчас речь пойдёт о случае исключительном, не имеющем аналогов. Представьте себе волчью стаю, отправившуюся по известной и безопасной тропе в ночной набег на загон для овец. Но загон оказался пуст, зато на тропе неожиданно встретились капканы, куда угодили в большинстве волки.

А теперь укажем эту волчью стаю: германская 10-я флотилия эсминцев, состоявшая из 11 новейших кораблей постройки 1914–16 годов с усиленным вооружением, около 1100 моряков. В ночь с 10 на 11 ноября 1916 года флотилия преодолела минные поля, закрывавшие вход в Финский залив, по заранее разведанному и проверенному маршруту. После нападения на пустой порт Балтийский (ныне Палдиски), так и не встретив противника, флотилия ушла из Финского залива. При возвращении через минные поля на русских минах погибли 7 из 11 боевых кораблей. На рис. 1 показаны маршрут флотилии и места гибели эсминцев.

На рис. 1 мы видим о. Оденсхольм, место гибели крейсера «Магдебург», известного читателям по предыдущим публикациям. А напротив острова, на побережье выделяется мыс Шпитгамн, именно там располагалась Радиостанция особого назначения, место сосредоточения и обработки всех данных радиоразведки, добытых на Балтийском флоте. Стоит отметить, что именно в этом месте побережья были сосредоточены и береговые посты Службы связи, и РРП, и станции радиоперехвата. Работа всех этих служб позволила в дальнейшем восстановить подробности происшедшей катастрофы германского флота. Уже в первый момент береговые посты сообщили о многочисленных взрывах, напоминающих артиллерийскую канонаду. В море вышли 1-й и 5-й дивизионы русских эсминцев, всего 12 кораблей, однако, никого не обнаружили.

Уже после войны бывший командир германской 10-й флотилии корветтен-капитан фон Витинг сообщил много интересного о ночном набеге. Моряк так живо описал подробности события, что даже перевод его воспоминаний читается на одном дыхании («Морской сборник» №№ 8–9 за 1922 г.).

ТРАГИЧЕСКОЕ НАЧАЛО ПОХОДА

«Что может быть лучше! В моём распоряжении — храбрые, закалённые войной офицеры и команды. Их томит нетерпение столкнуться с врагом, сразиться во имя победы и славы Германии. Моя флотилия состоит из новейших, лучших миноносцев. Нам поставлена цель — унич-



Рисунок 1. Маршрут германских эсминцев

тожение неприятельских кораблей... Итак, вперёд! В бесконечно длинной колонне шли миноносцы за головным S-56. Такой строй был избран, чтобы по возможности предохранить себя от мин. Расстояние между каждым из миноносцев — 300 метров. Погода благоприятная: луна скрыта облаками, и море спокойно.

В 20.38 передают морзянкой, что задние миноносцы отстали. Пришлось повернуть, чтобы узнать, что случилось. Трёх задних миноносцев нет. Наконец по линии с заднего миноносца передают, что один из них подорвался на mine. Это было печальное начало. Но что делать! Долгие поиски в темноте этих миноносцев, которые теперь остались где-то далеко на западе, всё равно ни к чему не приведут. Кроме того, ведь при пострадавшем, согласно ранее отданному распоряжению, остались 2 миноносца.

Повернули опять и с остальными идём дальше на восток. Только позже удалось узнать подробности того, что случилось. Оказывается, на V-75 под командирским мостиком взорвалась мина, и кочегарки быстро наполнились водой. На помощь к нему подошёл S-57. Вдруг раздался новый страшный взрыв, которым V-75 был разорван на три части. Этим же взрывом на S-57 срывает главный паропровод, а вскоре он сам попадает на мину и гибнет. G-89 спасает с обоих миноносцев их экипажи.

МНИМЫЙ УСПЕХ

Между тем флотилия продолжает свой путь 21-узловым ходом. В 10 часов мы с большим трудом открыли остров Оден-

схольм и определились, чтобы точно знать своё место во время предстоящей операции.

Наконец, от G-89 приходит радио, что V-75 и S-57 погибли... Приходит второе радио, что G-89 повернул на запад и имеет ход 30 узлов. Тем лучше. Значит, я могу спокойно продолжать путь с 8 миноносцами. Пусть успех операции вознаградит нас за потерю 2 кораблей.

Но где же неприятель? Или он опять предательски предупреждён о нашем набеге? Ни одного корабля, ни одного дозорного судна, хотя мы уже давно в Финском заливе. Это обидно... Для того, чтобы сделать хоть что-нибудь, я решаю обстрелять укреплённый Балтийский порт. Возможно, что в его гавани стоят неприятельские корабли. 5 миноносцев я оставляю перед бухтой, а с G-90, S-59 и S-56 я вхожу в бухту Рогервик.

Осторожно мы подходим к молу на расстояние 600 метров. Ни одного корабля нет. Как это досадно! Что же, остаётся обстрелять только военные сооружения. Бедный Балтийский порт! Напрасно там чувствуют себя так спокойно за минными заграждениями. Какой переполох поднялся, вероятно, в нём, когда в 1.30 ночи 6 прожекторов вдруг неожиданно забежали своими лучами взад и вперёд и началась ужасная бомбардировка. Но «варвары» обстреливают только сооружения в гавани, склады, сараи и подобные постройки и щадят мирный город... Выпущены 162 разрывные гранаты; результат — солдаты и лошади убиты, а военные сооружения превращены в развалины...

После этого выходим из бухты и, дав 26 узлов, несемся на запад. Чтобы не попасть на то место, где взорвались S-57 и V-75, я немного меняю курс.

НЕУМОЛИМОЕ ВОЗМЕЗДИЕ

Вдруг за последним миноносцем нашей колонны блеснули вспышки, и послышался грохот орудий! Итак, неприятель всё-таки нас открыл и напал на задние миноносцы! Самый полный ход вперед! Скорее на помощь! В этот момент у второго миноносца поднимается огромный столб воды. Кругом больше ничего не слышно. На самом миноносце — образцовое спокойствие. Проходя мимо G-90, я узнаю подробности несчастья. Оказывается, мина взорвалась под турбинами. Это уже третий миноносец.

S-59, подойдя к борту G-90, принимает его команду, а тот тем временем тонет. Не успело ещё остыть впечатление от этой потери, как прожектор заднего миноносца, прорезая своими лучами темноту, ночи, начинает сигнализировать. С отчаянием читаем: «V-72 ММ». Это означает попадание миной. Нет, это не подводные лодки — это мины! Но ведь это ад, куда мы попали! Я подхожу к V-72. У его борта уже стоит V-77, который снимает команду. Довести подорванные миноносцы до порта нечего и думать: они настолько повреждены, что еле держатся на воде.

Итак, S-57 и V-75 погибли на пути вперед, а теперь погибли G-90 и V-72. От гордой флотилии остаётся всего 6 миноносцев. Что-то ещё готовит нам судьба! Продолжаем путь на запад. Но не успели ещё все миноносцы соединиться, как сзади меня снова вспыхивает ужасное «ММ». Это S-58. И этот миноносец так сильно повреждён, что больше не в состоянии держаться на воде. В его отсеки вливается огромное количество воды, и он вдруг опрокидывается. Слава Богу ещё, что большая часть команды уже на S-59.

Что за страшная ночь! Кругом темнота, погода всё портится, а за заграждениями, наверное, нас ждёт со своими флотилиями неприятель. Среди же этого чёртова котла — только мины, против которых нет защиты. Вдруг опять зажигается прожектор: «ММ». Значит, опять надо, рискуя собой, снимать лю-



Рисунок 2. Гибель 10-й флотилии эсминцев. Художник С. Г. Невельштейн

дей с подорвавшегося миноносца. Весь этот ужас скрашивается только благодаря мужеству, проявляемому офицерами и командами. Но не время для размышлений! Всем довольно работы: и миноносцам, которые тонут, и тем, которые спасают. Мне самому то и дело приходится отдавать приказание за приказанием и по возможности вести миноносцы так, чтобы и остальные не наткнулись на мины. Курс держим на юг, так как мне он кажется самым безопасным. Вероятно, заграждения расположены именно по этому направлению, а, следовательно, мы будем идти параллельно ему...

Спасение шлюпками тянется слишком долго. Уже более часа S-59 перевозит ими команду S-58. Он не может подойти к самому борту, ибо на поверхности рядом с ним видны мины. Все это время остальные миноносцы держатся тут же, на минном поле. Наконец S-59 готов и идёт за остальными миноносцами. Но не успевает он пройти и тысячи метров, как его постигает та же судьба. Сквозь темноту ночи опять сверкает зловещее «ММ».

Теперь уже я сам иду к борту S-59. Очень неприятное плавание. Вот я вижу 2 большие мины, плавающие на поверхности, почти рядом с S-59. Скорее к борту, взять команду, и прочь от тебя, доблестный корабль! Ты слишком тяжело повреждён, чтобы тебя можно было

довести домой. S-59 уже имел на себе два лишних состава, а поэтому, когда S-56 пришлось снять с него всех людей, на нём оказалось три лишних комплекта. Всего на нашем борту находилось теперь почти 400 человек. Но как хорошо держат себя люди! Ни страха, ни злобы, ни слова упрека. Даже нет торопливости при пересадке...

Я ещё имею 4 миноносца! Неужели ещё не конец этой дьявольской ночи? Нет! Мы все пока на минах. Довольно размышлений! Они не помогут. Скорее, как можно скорее прочь из этих злых вод. Дальше, дальше на запад с S-56, V-76, V-77 и V-78 со скоростью 27 узлов! Одно утешение: стало светать. Но бедам ещё не пришёл конец. Вдруг опять тихий звук взрыва под последним миноносцем, V-76. Высокий столб воды, и «ММ». V-77 спасает экипаж, а V-76 тонет.

Осталось только 3 миноносца. Одиноко и грустно мы ищем правильный путь домой и на этот раз находим... Удивительным стечением обстоятельств S-56 избежал всех мин, хотя как флагманский шёл в голове кильватерной колонны. Наконец и с ним произошло несчастье, но, правда, без тяжёлых последствий. Неожиданно лопнула одна из труб, и из котлов ушла почти вся вода. Миноносец принуждён остановиться. Исправление аварии длится почти час. Кругом все ещё мины.



Рисунок 3. Мины русского флота

Наконец мы на чистой воде... Неприятеля мы так и не видели. Как выяснилось позже, он даже не выходил в море. Проклятая, злая ночь была позади нас!

Война требует жертв. Правда, мы не потопили ни одного неприятельского корабля, но зато всё же разрушили важные сооружения Балтийского порта и проникли в те воды, где русские чувствовали себя в полной безопасности. Отныне они должны быть всегда готовы к таким же случаям, как этот...». Рис. 2 иллюстрирует обстановку, описанную фон Витингом.

РАССЛЕДОВАНИЕ ОБСТОЯТЕЛЬСТВ НОЧНОГО НАБЕГА

В качестве комментария к воспоминаниям заметим, что баланс взаимных потерь весьма неутешителен для германского моряка: обстрел пустого порта Балтийский и города продолжался около 20 минут, при этом было повреждено 24 здания, 10 человек убито, из них 8 — мирные жители. Контрразведкой установлено, что с берега германским кораблям подавали световые сигналы фонарём.

Члены комиссии Балтийского флота, расследовавшей обстоятельства германского ночного набега, посчитали эту вылазку форменным безумием. Ведь командование германского флота прекрасно знало о наличии сплошных

минных заграждений, составленных из тысяч разнотипных мин и закрывавших вход в Финский залив. Что касается минного оружия, то в его теории и практике Россия была «впереди планеты всей».

Чтобы понять логику действий германского командования, вероятно, надо обратиться к военной обстановке в тот момент времени. Ныне известно, что к концу 1916 года Германия и её союзники исчерпали свои материальные и людские ресурсы для продолжения войны, реально наступала катастрофа. Руководители Антанты знали положение противника. Уже на исходе ноября 1916 года Германия с союзниками предложила мир, но Антанта отклонила предложение, указав при этом, что мир невозможен «пока не обеспечено восстановление нарушенных прав и свобод, признание принципа национальностей и свободного существования малых государств». Пользуясь борцовской терминологией, можно сказать, что Германия попала в жёсткий захват и началось её дожимание. Главы государств Антанты ждали победоносного исхода военной борьбы в 1917 году.

Похоже, что, готовясь предложить мир, германское руководство решило «стимулировать» Россию к мирному соглашению демонстрацией уязвимости её военно-морских позиций. Германские радиопеленгаторы позволили вы-

явить безопасные проходы, которыми пользовались российские корабли для преодоления своих минных полей. По выявленным маршрутам прошли германские подводные лодки, подтвердив возможность и безопасность преодоления минных заграждений. Рассчитывая на успех, военно-морское командование хорошо представляло и риск операции, вероятно, заранее готовясь к потерям. А потери оказались велики: 7 из 11 эсминцев. Для сравнения: летом 1916 года в крупнейшем морском сражении Первой мировой войны, Ютландском, немцы потеряли 5 эсминцев из 61, участвовавших в сражении.

ТВОРЦЫ НОВОЙ ТАКТИКИ МОРСКИХ БОЁВ

Теперь укажем и виновников потерь германской стаи эсминцев. Прежде всего, следует отметить радиоразведчиков, постоянно отслеживавших перемещение неприятельских кораблей, включая и прохождение германских подводных лодок в Финский залив. Российские офицеры не страдали недооценкой возможностей германской разведки и прекрасно понимали, что противник также пеленгует перемещения кораблей Балтийского флота и следит за их связью. А потому старались предусмотреть шаги неприятеля, действовать на опережение. Был и непосредственный виновник трагедии германского флота — капитан первого ранга Михаил Борисович Черкасский, флаг-капитан по оперативной части штаба командующего Балтийским флотом. В обязанности флаг-капитана, т.е. помощника начальника штаба по оперативной части, входили и разработка планов минной обороны, и разведка. Ему непосредственно подчинялся И. И. Ренгартен, инициатор и организатор радиоразведывательной деятельности на флоте.

Весьма вероятно, что русское командование предполагало атаку германских кораблей именно там, где она произошла, и заранее готовилось к ней. Об этом свидетельствует рапорт, представленный командующему флотом А. И. Непенину, где М. Б. Черкасский указал: «Проход лодок через нашу позицию легко закрыть установлением ещё одного противолодочного заграждения... Преодоление минными крей-



Рисунок 4. Штаб Балтийского флота, штабной корабль «Кречет» (июль 1916 г.). М. Б. Черкасский во втором ряду, второй справа. В центре — командующий флотом вице-адмирал В. А. Канин и контр-адмирал А. В. Колчак. В верхнем ряду второй справа — И. И. Ренгартен

серами невозможно. Дополнительной разведки у позиции неприятель не ведёт, недооценивает эту опасность для судов». Рапорт датирован 4/17 октября. На следующий день Непенин поставил резолюцию: «Действуйте. Это важнее наступательных плаваний» (впервые опубликовано в 1952 году в журнале «Морские записки», Нью-Йорк). В конце октября моряки скрытно выставили добавочное заграждение: 705 мин на глубину 55–90 метров. Результат нам уже известен: 7 из 11 германских эсминцев не смогли их преодолеть.

За успешную операцию по установке минного поля М. Б. Черкасский был награждён орденом св. Владимира 3-й степени с мечами.

Весь недолгий жизненный путь Михаила Борисовича князя Черкасского был связан с флотом. Потомок кабардинского княжеского рода, он родился в

Новочеркасске в 1882 году. В 1901 году окончил Морской кадетский корпус с присуждением Премии адмирала Нахимова. С 1901 по 1912 год служил вахтенным начальником и артиллерийским офицером на больших кораблях, включая броненосцы «Слава» и «Андрей Первозванный». 1912–1914 годы — учёба в Николаевской морской академии. В 1914–1918 годах служил в Штабе командующего Балтийским флотом: с самого начала в оперативной части, с декабря 1915 — флаг-капитан по оперативной части, с марта 1917 — и.д. начальника штаба, с июля 1917 — контр-адмирал и начальник штаба. В январе 1918 года был уволен с флота, после чего уехал в своё имение близ Черкасс в Полтавской губернии. Дальнейшее неясно, существуют несколько версий его гибели в конце 1918 или начале 1919 годов.

Таков печальный итог жизни 36-летнего адмирала. Не прошло и двух лет с того момента, когда он принял активное участие в Февральской революции на Балтийском флоте. Есть предположение, что именно о М. Б. Черкасском упомянул писатель В. Г. Короленко в своих письмах из Полтавы: «В кровавом пекле сгорела и жизнь молодого адмирала, которого растерзали только за то, что он больше не хотел воевать...».

А тогда, в конце 1916 года, героям нашего повествования будущее представлялось, вероятно, совсем иным. И если не безопасным для себя, война есть война, то всё же надёжно обеспеченным для Отечества. Прежде всего для Отечества.

**Александр БОДРИК**

управляющий партнер бизнес-инкубатора по кибербезопасности Cyberlands B.V., вице-президент по ИБ ISACA Moscow Chapter

ДВЕНАДЦАТЬ БОГАТЫРЕЙ

ДЛЯ БИТВЫ ЗА ПРОИЗВОДИТЕЛЬНОСТЬ ИБ-ТРУДА

Слова о производительности труда всё активнее звучат с правительственных трибун и входят в повестку служб информационной безопасности. Уже нельзя, как раньше, просить деньги на все технологии и штатные позиции подряд — требуется подготовка бизнес-кейсов и простое человеческое объяснение, что тот или иной конкретный ход даст компании. Между тем, задача повышения производительности труда была актуальна для ИТ-сектора с самого его рождения, и мы (сектор ИБ) можем многое у него почерпнуть. Другой хороший источник — международные компании, которые прошли много циклов внутренней оценки эффективности и набили шишки на «лучших» практиках. И, как и любая задача, производительность труда может повышаться благодаря использованию управленческих методик и методик классических направлений: «Персонал», «Технологии» и «Процессы». 12 из них опишем ниже.

УПРАВЛЕНЧЕСКИЕ МЕТОДИКИ

Производительность, как и любая другая характеристика, требует измерения. Измерять нужно в понятных бизнесу метриках, например, затратах на обеспечение безопасности одного ПК.

Однако условные 100 000 рублей / ПК в год (пример реальной цифры крупной структуры) сами по себе ничего не значат: получается, как в истории про «42», ответ на все вопросы вселенной.

1. Тарификация услуг. Хочет того служба ИБ или нет, но большая часть ее деятельности заключается в оказании операционных сервисов безопасности. Фиксация определенного натурального и денежного объема стимулирует владельцев сервисов (например, начальников отделов службы ИБ) управлять их себестоимостью, а также позволяет в принципе понять, во сколько нам обходится та или иная активность, не проводя дни в аллокации новых проектов, затрат на продление лицензий и других затрат в конкретную услугу.

2. Нормализация затрат. Затраты могут расти и вне зависимости от службы ИБ, например, из-за инфляции. Структурирование изменения затрат на затраты из-за ввода новых сервисов и из-за внешних факторов — полезный инструмент при обсуждении с бизнесом.

3. Аллокация затрат на проекты ИТ. Основная функция службы ИБ в любой организации — формирование и согласование правил игры в корпорации в целом и в общих сервисах в частности («ИТ-коммуналка» при общении с русским менеджментом и «umbrella» при общении с западным менеджментом). Затраты на проектирование, реа-

лизацию и эксплуатацию систем ИБ отдельных крупных проектов, например, системы закупок, могут и должны быть аллоцированы в итоге на бюджет соответствующего ИТ-проекта и подразделения функционального заказчика.

Международные компании широко применяют вышеуказанные три практики.

МЕТОДИКИ НАПРАВЛЕНИЯ «ПЕРСОНАЛ»

4. Managed Security Services Provider (MSSP). Внутренний MSSP, как ультимативная форма повышения производительности труда через централизацию функций, позволяет наконец-то найти ответственных и определить рычаги влияния на сервис во всей корпорации — без разницы 2 тыс. сотрудников в ней работает или 200 тыс. Чтобы MSSP работал, важно добиться единообразия стандартов эксплуатации ИТ и базовых средств информационной безопасности во всей корпоративной сети или аутсорсить там, где это по тем или иным причинам невозможно, передавая сложные участки в работу квалифицированным компаниям.

5. Селективный аутсорсинг. Аутсорсинг, как средство передачи обеспечения безопасности сложных участков профильным компаниям, упрощает управление операционными сервисами и позволяет высвободить ресурсы

для управления безопасностью. Впрочем, аутсорсинг не зря 5-й в списке — особенно удобно и разумно использовать внешние сервисы безопасности уже после установления единых стандартов ИТ-инфраструктуры, тарификации внутренних услуг и других ранее описанных механизмов управления производительностью труда.

6. Обучение персонала. Однако самые эффективные методики могут быть сведены на нет слабыми сотрудниками. Причем, слабым звеном могут оказаться (и оказываются) не только сотрудники службы ИБ, но и ИТ-администраторы, разработчики, владельцы активов, директора бизнес-направлений и обычные пользователи. Обучение традиционно является недооцененной темой в ИБ, но в последнее время намечаются сдвиги. В частности, компании-лидеры проводят «Недели ИБ» с целым рядом лекций по релевантным тематикам информационной безопасности для различных целевых аудиторий.

Важно развивать не только знания, но и навыки, но это уже вопрос следующего блока — технологий.

МЕТОДИКИ НАПРАВЛЕНИЯ «ТЕХНОЛОГИИ»

7. Цифровые платформы кибербезопасности. Некоторые средства защиты начинают эволюционировать в новую сущность — цифровые платформы. Цифровые платформы определяются тремя принципиальными особенностями. Во-первых, они так или иначе автоматизируют деятельность службы ИБ, снижая требования к количеству и качеству необходимых талантов в рутинных процессах или операционных сервисах. Во-вторых, они содержат внутреннюю логику (например, trigger engine), позволяющую автоматически запускать те или иные действия в зависимости от тех или иных событий или статусов защищаемых объектов (ПК, IP-адресов, пользователей). В-третьих, цифровые платформы обладают горизонтальной масштабируемостью, позволяя безопасности расти соразмерно росту бизнеса, даже если он растет вдвое год к году.

8. API. Закрытая цифровая платформа обладает ограниченной ценностью. Для извлечения из нее максимально-

го толка нужен двусторонний RESTful API — в целях автоматизации рутинных задач по всему фронту задач службы ИБ.

9. Машинное обучение. Так как мы не можем знать, чего мы не знаем в конкретной ситуации, разумно привлечь независимого советника с более широким и детальным взглядом. В технологической плоскости, с учетом разнообразия и количества данных, в роли советника выступают технологии машинного обучения, которые подсвечивают рискованные области, даже если мы еще не поняли, в чем проблема, и еще не описали предметную область на языке сигнатур или корреляционных правил.

Все три вышеуказанные методики активно используются компаниями ИТ-сектора, стремительный рост которого в последние 20 лет не оставил иного выбора внутренним службам ИБ, кроме как автоматизироваться по максимуму.

МЕТОДИКА НАПРАВЛЕНИЯ «ПРОЦЕССЫ»

10. Передача СЗИ на поддержку в ИТ. Прежде чем наводить порядок в процессах, разумно избавиться от процессного хлама. В процессах ИБ к таковому относятся активности, которые не приносят заметной ценности и не очень понятны бизнесу. Например, поддержка классических средств защиты информации — межсетевых экранов, антивирусов и др. Нельзя службе ИБ с ограниченными ресурсами делать все хорошо, и в корпорации хорошо делает поддержку та служба ИТ, у которой есть выделенные специалисты или даже команды по Windows, UNIX, поддержке СУБД и сетевого оборудования. Особенно это касается тех средств защиты, что могут блокировать сетевое взаимодействие или другие операции — приостановив тем самым бизнес-процесс.

11. Интеграция процессов. Процессы — как прутья в венике: сильнее вместе, чем по отдельности. Сетевая безопасность может быть эффективна, если мы не нарезаем (или быстро отнимаем) расширенные доступы в Интернет пользователям — нарушителям политики ИБ, а реагирование на ин-

циденты ИБ не может быть эффективным без четкого понимания, кто за какой актив отвечает, и кто полномочен авторизовать ту или иную стратегию реагирования. Интеграция процессов ИБ между собой повышает эффективность каждого из них и в совокупности повышает возврат инвестиций в сами процессы и необходимые им технологии и навыки людей.

12. Обмен данными. Старая мудрость «один в поле не воин» применима и в ИБ, обмен данными тут позволяет выиграть время у злоумышленников. Обмен может быть как внутри индустрии (практически все коллеги из финансовой отрасли уже подключились к ФинЦЕРТ), так и внутри государства (ГосСОПКА), а в супербольших организациях нужно подумать и про обмен данными между подразделениями, ведь каждое из них представляет собой немалый холдинг со своими правилами и соображениями. Для обмена данными внутри большой организации полезен институт бизнес-партнеров, которые и выступают первичной точкой обмена данными и консолидации мнения бизнес-подразделений.

Особенно активны в применении практик повышения производительности направления Процессы международные компании с их бесчисленными подразделениями и корпоративными функциями, каждое из которых требует координации.

СКАЗКА ЛОЖЬ, ДА В НЕЙ НАМЕК

Как сказали как-то коллеге на собеседовании в крупнейшем швейцарском банке, «Цена не является ключевым фактором в проектах кибербезопасности». И правда, производительность труда частенько проигрывает в списке приоритетов руководителя службы ИБ показателю эффективности в противостоянии актуальным киберугрозам или своевременному приведению корпорации в соответствие очередному КИИ или GDPR. Однако экономические и внутрикорпоративные тренды неумолимы — производительность труда повышать рано или поздно придется, а значит, лучше готовиться летом, пока еще не наступила зима обрезающих бюджетов.



BIS-🔥: АНДРЕЙ, ЗАЖИГАЙ!

МАСТЕРА ПРОДВИЖЕНИЯ
СВОИХ КОМПАНИЙ
НА ИТ- И ИБ-РЫНКАХ ВНОВЬ
ВСТРЕТИЛИСЬ НА BIS-ОГОНЬКЕ
3 ОКТЯБРЯ

В очередной раз, на уже традиционный BIS Огонек собрались пиарщики и маркетологи в сфере ИБ — обворожительные девушки, создающие своим компаниям лёгкое дыхание на коммерческих рынках. Собрание этого закрытого клуба как всегда проходило в нескольких измерениях: маги ИТ- и ИБ-продаж делились тайными знаниями, оперативной информацией и, конечно, неподдельными эмоциями.

Директор по маркетингу Softline Елена Шедова — признанный лидер среди российских профессионалов — сразу подняла разговор на международную высоту. Она рассказала, как налаживала работу маркетинговой службы своей компании в Бразилии и других странах. Раскованно, порой смешно до слез и, безусловно, полезно и поучительно. Вопросов и споров было гораздо больше, чем запланировали.

После деловой части управление взял в свои руки директор по развитию BIS Journal Андрей Миных. Зажигательное караоке, танцы до упаду, ну, и между делом непринужденное общение, включая обмен полезной информацией. Было очаровательно.



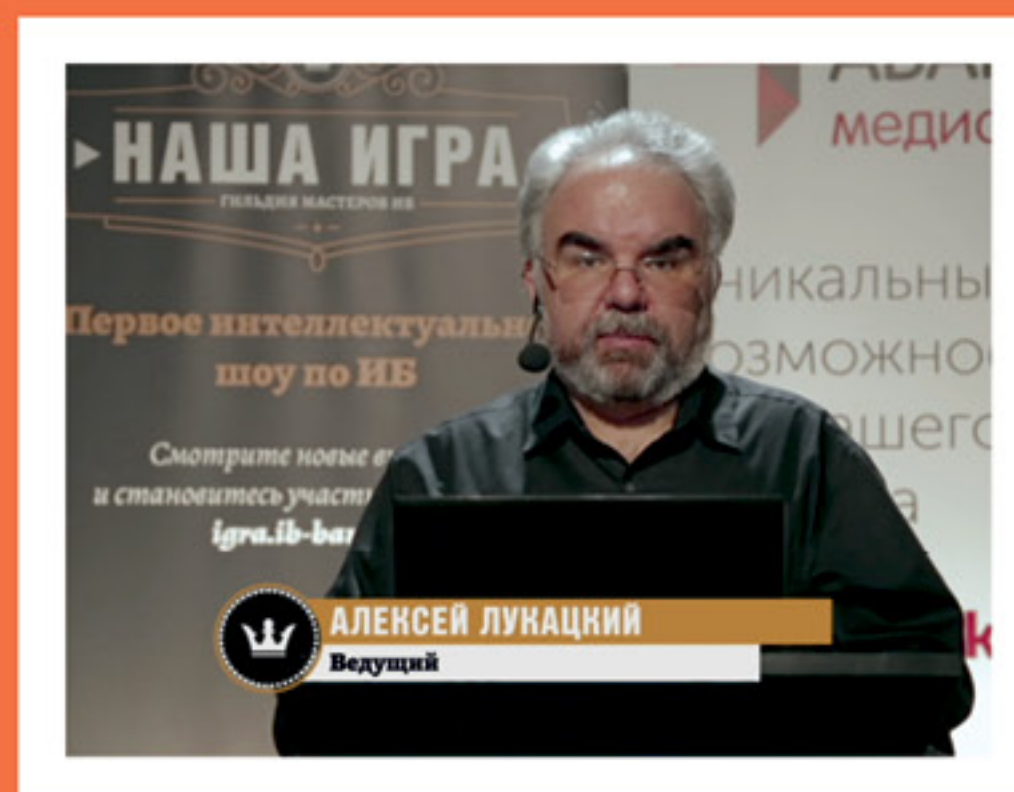


ОСВЕЩАЕТ ГЛАВНЫЕ МЕРОПРИЯТИЯ
ОТРАСЛИ И ПРОИЗВОДИТ
ВИДЕОКОНТЕНТ ДЛЯ ВАШИХ ЗАДАЧ:



На деловых мероприятиях:

- Яркие видеоотчёты
- Развёрнутые обзоры
- Интервью с участниками



Видео для ваших целей:

- Динамичные промовидео
- Серия тематических интервью
- Презентация продуктов
- Имиджевый ролик



В студии:

- Ток-шоу об ИТ и ИБ
- Телевикторина
- Специальные ТВ-проекты



BIS TV — фокус на безопасность



tv.ib-bank.ru



УРАЛЬСКИЙ ФОРУМ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ФИНАНСОВОЙ СФЕРЫ



IB-BANK.RU

17-21 ФЕВРАЛЯ 2020 ГОДА

Встречаемся на Урале!