



18 Ольга СКОРОБОГАТОВА
Банк России
Большие проекты ЦБ в 2019 году



10 Сергей ПАЗИЗИН
Банк ВТБ
Облачная платформа для RegTech и SupTech

30 Георгий ЛУНТОВСКИЙ
Ассоциация банков России
Рост цифровых технологий опережает регулирование

84 Павел БЫЛЕВСКИЙ
BIS Journal
Hi-hume – hi-tech: вызов принят!

100 Борис СТОЛПАКОВ
Историк криптографии
Крым наш! К 75-летию освобождения Севастополя

ПУТЬ РЕГУЛЯТОРА В ОБЛАКАХ



VIII симпозиум «Современные тенденции в криптографии»

Тематика симпозиума включает следующие вопросы (но не ограничивается ими):

- исследование криптографических алгоритмов и протоколов, в том числе являющихся международными стандартами;
- эффективная реализация методов анализа криптографических алгоритмов и протоколов;
- оценка криптографической стойкости российских криптографических алгоритмов и протоколов;
- эффективная реализация российских криптографических алгоритмов и протоколов;
- математические аспекты криптографии;
- криптография в «Интернете вещей»;
- квантовая криптография и квантовые вычисления;
- постквантовая криптография;
- криптография и технология блокчейн;
- криптографическая защита биометрических данных;
- другие актуальные и перспективные направления криптографии.

ОРГАНИЗАТОРЫ



Академия
криптографии РФ



Технический комитет
«Криптографическая защита информации»



Математический институт
им. В.А. Стеклова РАН

ГЕНЕРАЛЬНЫЙ ПАРТНЕР



ОФИЦИАЛЬНЫЙ ПАРТНЕР



ПАРТНЕР



ОРГПОДДЕРЖКА





Игорь НЕКРАСОВ
главный редактор
BIS Journal

Органное звучание Уральского форума плывет над Москвой, удерживая в гармонии настроения и поступки в сфере ИБ. Этот номер BIS Journal — почти нотная тетрадь, хранящая основные темы грандиозного концерта, вдохновившего отрасль и в этом году. Коснемся лишь некоторых фрагментов.

Органная импровизация — тот же форум, где различные по длине и толщине трубы-инструменты высказывают свои мнения. Вот, например, лабиальный регистр, флейта — звук нежнейший и, не будем забывать, главный в военных маршах. Первый зампред Банка России, очаровательная Ольга Скоробогатова выводит на сцену, словно пять легионов, пять Больших финтех-проектов ЦБ. Тут суть дела не в количестве, а именно в завершенности, плюс, безусловно, качестве, дисциплине, выучке и т.д. Так римляне наступали на варварство, строя цивилизацию на века — не быстро, но уверенно и неотвратимо. Завораживающая партия.

В ответ тромбон, тревожный и мощный, — серьезный наступательный инструмент в другом — язычковом регистре. Президент Ассоциации банков России Георгий Лунтовский буквально врывается со своей темой «Рост цифровых технологий опережает регулирование!» Трепещи, Банк России! Эту интригу на свой лад подхватывает дерзкий и чистый горн — вице-президент АБР Алексей Войлуков проанализировал проекты RegTech и SupTech на финансовом рынке и в гневе труббит: «Доколе? У российских банков есть и потребности!»

Что тут начинается! Полная трагизма и слез полемика представителей ИБ малых и средних банков — пронзительно диссонансирующие микстуры: «Мы — пасынки системы!», «Не плачь, не плачь!», «Проблема действительно существует!» Восхитительное трио!

Вдруг, будто вкрадчивый полубог, вступает бархатный гобой. Сергей Пазизин, Банк ВТБ, выводит на первый план свою группу инструментов и объединяет регистры в grand jeu (лабиальные и язычковые без микстур). Он сливает воедино темы финтеха и RegTech-SupTech. Ему пяти легионов Ольги Скоробогатовой мало. Нужен еще один — облачная платформа. Чтобы на всех парусах — как на обложке BIS Journal. Его поддерживают другие величавые полубоги, звуки обрушиваются каскадом, накрывая мир ИБ без остатка. И тут же, поддержанный басом, то бишь мануалом ниже контроктавы (зампред Банка России Василий Поздышев: «Аргументы такие... обсуждаемые»), хор разных по длине и толщине труб взмывает на божественную — очень полезную для отрасли — высоту.

И так на протяжении всего форума. То вверх, то вниз.

А в конце, после азартного эпилога, на сцену поднимается Артём Сычёв.

И красиво раскланивается.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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

Сычёв А.М. — Первый заместитель директора Департамента информационной безопасности Банка России, кандидат технических наук, доцент

Шипилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Былевский П.Г. — шеф-редактор, кандидат философских наук

Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПО», CISA, кандидат физико-математических наук

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

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

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

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

Курило А.П. — заместитель генерального директора компании «РНТ», кандидат технических наук

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

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

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

Некрасов И.В. — главный редактор журнала

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

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

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

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

ЭКСПЕРТНАЯ ГРУППА

Одувалов М.В. — эксперт BIS Journal

Филипчук А.А. — технический директор ГК ЦРТ

Калашникова Е.В. — Банк ВТБ (ПАО)

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**

Шеф-редактор: **Былевский П.Г.**

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

Арт-директор: **Мельников Н.С.**

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

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**

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

Цветокорректор: **Науменко М.Б.**

Корректор: **Бальтерманц Л.Ф.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группы „Авангард“»

Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д.21 (м. «Достоевская»)

Координаты: 55.779380, 37.61150

Тел./факс: +7 499 271-70-85

Интернет-версия: journal.lib-bank.ru

E-mail: bis@ib-bank.ru

Отдел рекламы: reklama@ib-bank.ru

Отдел распространения: tirazh@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство ПИ № ФС77-61378 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 12.04.2019. Тираж 7000 экз.

Заказ № 45/89. Цена договорная.

Отпечатан в «Типографии на Угрешской»

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

Тел.+7 495 720-62-28

© BIS Journal, 2019



НОВОСТИ

5 В России, в мире, технологии

ТЕМА НОМЕРА

- 10 **Облачные технологии**
Сергей Пазизин (Банк ВТБ)
Путь регулятора... в облаках?
- 13 **Облачные технологии**
Александр Никитин (ЛИНС-М)
Банк-как-сервис
- 14 **Облачные технологии**
Андрей Курило
Требуется консорциум
- 16 **Облачные технологии**
Алексей Забродин (РТК-ЦТ, Ростелеком)
Масштаб задачи очевиден



10

РЕГУЛЯТОРЫ

- 18 **Банк России**
Ольга Скоробогатова (Банк России)
Большие проекты
- 22 **Банк России**
Дмитрий Скобелкин (Банк России)
Широким фронтом
- 27 **Банк России**
Артём Сычёв (Банк России)
Распознать и обезвредить



22



18

БАНКИ

- 30 От первого лица**
Георгий Лунтовский
(Ассоциация банков России)
Рост цифровых технологий опережает регулирование
- 33 RegTech и SupTech**
Алексей Войлуков
(Ассоциация банков России)
У банков есть и потребности
- 36 Полемика**
Денис Антонов (КБ «Банк Союз»)
Пасынки системы
- 40 Обзор**
Татьяна Жаркова (Ассоциация ФинТех)
Банки на волне финтеха
- 42 Импортозамещение**
Карл Сумманен (независимый эксперт)
ИТ-импортозамещение в России
- 50 Биометрия**
Максим Федотенко (Сбербанк)
Технология защиты от угрозы подмены биометрического сканера



60



36

УГРОЗЫ И РЕШЕНИЯ

- 54 События**
Николай Мальковский, Дмитрий Попов,
Екатерина Крылова (ГК ЦРТ)
Что это там шумит?
- 58 Контроль действий**
Дмитрий Михеев (ООО «АйТи БАСТИОН»)
Кому на самом деле нужна СКДПУ ИТ в банке
- 60 Автоматизация**
Виктор Сердюк, Роман Ванерке
(АО «ДиалогНаука»)
Внимание, робот-пентестер!
- 63 Управление сетью**
Максим Ксенофонтов (АМТ-ГРУП)
Что? Где? Куда?
- 66 Файловый обмен**
Леонид Бондаренко
(ООО «Секрет Технолоджис»)
Корпоративная безопасность
- 68 Форензика**
Александра Бялькина
(АО «Кросс Технолоджис»)
Forensics forever!

ИНФРАСТРУКТУРА

- 72 **Деловые мероприятия**
Логика в масштабе
- 76 **Деловые мероприятия**
Марк Новодачный (BIS Journal)
ИНФОФОРУМ 2019
- 78 **Деловые мероприятия**
Николай Кольский (BIS Journal)
ТБ форум 2019
- 79 **Деловые мероприятия**
Корней Реут (BIS Journal)
BIT-2019
- 80 **Деловые мероприятия**
Корней Реут (BIS Journal)
«В теории нет разницы между теорией и практикой. А на практике есть»
- 82 **Деловые мероприятия**
Анна Воробьева (BIS Journal)
DLTReg 2019



HI-HUME

- 84 **Открываем новый раздел**
Павел Былевский (BIS Journal)
Hi-hume — hi-tech: вызов принят
- 88 **Социальные сети**
Наталья Касперская (ГК InfoWatch),
Игорь Ашманов (АО «Крибрум»)
Анатомия деструкции
- 90 **Воспитание**
Виталий Григорьев (РТУ МИРЭА)
Профессионализм: по ту сторону добра и зла?



ОБРАЗОВАНИЕ И КАРЬЕРА

- 96 **Обзор**
Марина Бродская (BIS Journal)
СТФ — источник кадров
- 98 **Олимпиады**
Код Верченко

СУБЪЕКТЫ

- 100 **История**
Борис Столпаков (историк криптографии)
«Мы вернулись домой в Севастополь родной...»
- 106 **История**
Борис Столпаков (историк криптографии)
На Волге широкой
- 112 **Мысли вслух**
Валерий Куликов (BIS Journal)
Ушёл ли поезд?
- 114 **Заметки безопасника**
Александр Бодрик (ISACA Moscow)
Sex questions

«ЦИФРОВАЯ ЭКОНОМИКА»: НОВЫЕ ЭКСПЕРТЫ ПО ИБ

Финансовый университет при Правительстве РФ в рамках поручения Минкомсвязи создаёт АНО «Центр экспертных исследований в цифровой экономике». Вместе с Центром компетенций по импортозамещению в сфере ИКТ он будет отслеживать исполнение работ в рамках нацпрограммы «Цифровая экономика» и контролировать затраты на них. Новый центр получит бюджетные субсидии, сумма которых пока не определена.

Новый Центр займётся экспертным сопровождением направления «Информационная безопасность» нацпрограммы «Цифровая экономика». Его задачей станет организация ряда мероприятий нацпрограммы и «анализ результатов выполненных работ на предмет соответствия первоначальным ТЭО и ТЗ». Кроме того, он будет соотносить затраты на реализацию нацпрограммы с текущими рыночными ценами.

Ранее сопровождением мероприятий «Информационной безопасности» занимался Центр компетенций по импортозамещению в сфере ИКТ, возглавляемый Ильёй Массухом, но по итогам 2018 года было решено, что его ресурсов для этого недостаточно. В связи с этим к выполнению задач и был привлечён Финансовый университет.



ФСТЭК УЖЕСТОЧИЛ ТРЕБОВАНИЯ

ФСТЭК утвердил новые требования к софту в области кибербезопасности. Они распространяются на антивирусы, межсетевые экраны, софт для борьбы со спамом и т.п. Документ вступит в силу 1 июня 2019 года, а до 1 января 2020 года разработчики защитного софта должны будут при участии лабораторий ФСТЭК оценить соответствие своих продуктов новым требованиям и провести испытания по выявлению уязвимостей и недекларированных возможностей.

Эксперты считают, что компаниям придётся нести дополнительные расходы. Непрерывное сопровождение продукта, анализ и устранение недостат-

ков — это серьёзная работа. Зато такое ужесточение позволит отсеять недобросовестных участников рынка. Но наибольшие трудности новые требования создадут иностранным компаниям. Дело в том, что документ ФСТЭК обязывает разработчиков передать на проверку исходный код решений с описанием каждой функции и механизма работы. По мнению экспертов, крупные разработчики никогда не предоставят код, составляющий коммерческую тайну. Это значит, что число иностранных средств защиты в российских госорганах скоро сократится.

Сегодня до половины рынка ИБ в России приходится на госорганы и госкорпорации, до недавнего времени две трети его занимали решения зарубежных компаний. Изменения в законодательстве уже привели к тому, что число сертификатов на зарубежные средства защиты сократилось и составляет теперь пятую часть от общего числа.



ПОЗНАКОМЬТЕСЬ С ЧЁРНЫМ СПИСКОМ!

В публичном доступе появилась информация о клиентах, которым банки отказали в обслуживании по закону о противодействии отмыванию доходов.

В базе содержатся сведения о 120 тыс. граждан и компаний. По физическим лицам доступны ФИО, дата рождения, серия и номер паспорта, по индивидуальным предпринимателям — ФИО и ИНН, по компаниям — наименование, ИНН и ОГРН.

В ЦБ заявили, что сведения передавались по зашифрованным каналам, и возложили ответственность за утечку на банки. Росфинмониторинг также исключил свою вину.

По словам экспертов, для клиентов утечка опасна самим фактом присутствия в базе — у лиц из списка могут возникнуть трудности при устройстве на работу и заключении договоров с контрагентами.

КИБЕРДИКТАНТ ПРОТИВ КИБЕРМОШЕННИКОВ

Кибермошенники в России переключились с пенсионеров на молодёжь, — такое заявление сделал глава Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России Артём Калашников.

— Сейчас фокус внимания мошенников сместился на людей 25–40 лет, — сказал он. Благодаря проведённой в СМИ кампании по повышению финансовой грамотности пенсионеры стали более бдительными, в то же время граждане 25–40 лет чаще всех пользуются финансовыми услугами.

Чтобы подготовить юных к встрече с мошенниками, Банк России проводит Кибердиктант для школьников. Пока только в 12 регионах. В дальнейшем регулятор выработает программу по повышению финансовой грамотности и запустит её по всей стране.

ВЕЛИКОБРИТАНИЯ ВВОДИТ ИНТЕРНЕТ- ОПРИЧНИНУ

Великобритания заявила о планах создать отдельный регулятор, который займётся социальными сетями, поисковыми системами, мессенджерами и т.п. Он будет пресекать контент, наносящий «онлайн-вред». Таким зонтичным термином обозначили контент, включающий в себя сексуальное насилие, риторику ненависти, экстремистские и террористические видео, призывы к самоубийству.

Новый регулятор получит особые полномочия штрафовать компании и их представителей за нарушение законодательства. Согласно законопроекту, социальные сети будут обязаны публиковать отчёты о вредоносном контенте на своих платформах и рассказывать, какие меры по борьбе с ним были предприняты.

КИБЕРАТАКА НА ВЕНЕСУЭЛУ

Кибератака США на энергетическую систему Венесуэлы шла тремя способами, — рассказали президент Венесуэлы Николас Мадуро и министр связи и информации страны Хорхе Родригес.

Сначала была атакована АСУ ГЭС им. Симона Боливара и система в Каракасе. Затем были поданы мощные электромагнитные импульсы, прервавшие процессы восстановления этих систем. Кроме того, были ещё и физические нападения на энергетические объекты в виде поджогов и подрывов электрических подстанций.

Руководители страны обвинили в атаке США. В качестве доказательства Хорхе Родригес также привёл сообщение из Твиттера американского сенатора Марко Рубио, которое появилось через несколько минут после отключения энергосистемы Венесуэлы 7 марта. В своём твите Марко Рубио заявил о полном

отключении энергии в 18 из 23 штатов Венесуэлы, а также о полном отключении главного аэропорта страны и отказе резервных генераторов в аэропорту. По мнению Родригеса, такая быстрая и точная подача информации также свидетельствует об американском следе в этом инциденте.

Сложная ситуация с энергоснабжением тут же была использована оппозицией. По предложению самозванца Хуана Гуайдо Национальная ассамблея объявила в стране чрезвычайное положение.



XVIII ВСЕРОССИЙСКИЙ ФОРУМ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.
РЕГУЛИРОВАНИЕ. ТЕХНОЛОГИИ. ПРАКТИКА.

ИнфобЕРЕГ

9 - 13 сентября 2019
Крым, г. Ялта

Организатор:
Академия Информационных Систем



ПО ВОПРОСАМ УЧАСТИЯ ОБРАЩАЙТЕСЬ В ОРГАНИЗАЦИОННЫЙ КОМИТЕТ



+7 (495) 120-04-02



conf@infosystem.ru



www.vipforum.ru



Kaspersky® Anti Targeted Attack Platform

Комплексное решение для защиты от целевых атак и сложных угроз

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

www.kaspersky.ru/enterprise

#ИстиннаяБезопасность

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

«ГРУППА ТИНЬКОФФ» СОЗДАЛА СУПЕРКОМПЬЮТЕР

«Группа Тинькофф» начнёт использовать в работе мощности собственного суперкомпьютера. Устройство позволит обучать нейронные сети быстрее и эффективнее.

Устройство назвали «Колмогоров» в честь российского математика. На 10 серверов и сопутствующее оборудование было потрачено около \$1 млн. Суперкомпьютер позволит обучать нейросетевые модели быстрее, используя массив всех данных, собранных группой компаний за 13 лет работы. В перспективе специалисты «Группы Тинькофф» смогут эффективнее развивать предиктивную аналитику (прогнозирование поведения клиентов), обучая модели на текстовых данных, а также на звуковых. Звуковые данные суперкомпьютер сможет ускоренно переводить в тексты.

ТЕХНОЛОГИЯ ОБМАНА... ИИ

Команда специалистов IBM, Amazon и Техасского университета разработала атаку на алгоритмы обработки естественного языка, с помощью которой им удалось изменить поведение модели искусственного интеллекта.

Атака, названная исследователями «атакой перефразирования», была представлена на конференции по вопросам ИИ в Стэнфордском университете 1 апреля. Её суть заключается

в изменении вводимого текста таким образом, чтобы при сохранении первоначального смысла ИИ воспринимал его по-другому.

К примеру, существует алгоритм ИИ, анализирующий содержимое электронных писем и обозначающий их как «спам» или «не спам». Злоумышленник может так модифицировать текст спам-сообщения, что ИИ будет классифицировать его как «не спам». В то же время для человека смысл сообщения останется без изменений.

Предыдущие варианты атак на текстовые модели предполагали изменение одного слова в предложениях. Такое модифицирование действительно позволяло «обмануть» алгоритм, однако сами предложения при этом звучали неестественно и резали ухо. Команда исследователей IBM, Amazon и Техасского университета решила не менять слова в предложениях, а перефразировать их полностью, сохраняя при этом читабельность.



ЛУЧШИЕ
В РОССИИ
best.ru

a
news
ВСЕ НОВОСТИ И БЛОГИ

BEST.RU 2018

КОМПАНИИ И ПЕРСОНЫ ГОДА

КУПИ БИЛЕТ

При поддержке

Официальный рейтинговый партнер

Аналитический партнер

Официальная площадка церемонии

Официальный кейтеринг

Официальная вода

Сладкий партнер

Официальный печатный партнер

Генеральный информационный партнер

Информационные партнеры

Реклама

PHD
Positive
Hack
Days

BREAKING THE CONSTANT*



Реклама



БИЛЕТЫ
УЖЕ В ПРОДАЖЕ

21–22 Мая/2019

Более 100 активностей
PHDays9 объединит идея взаимодействия социума и ИТ: доклады и дискуссии с участием признанных лидеров мнений, мастер-классы от ведущих экспертов в сфере исследования безопасности информационных систем, выставочная зона, конкурсы по анализу защищенности всевозможных систем и технологий, умных машин и устройств, музыкальный фестиваль и многое другое.

* Взлом константы

Действительно ли привычные цифровые константы на самом деле неизменны? А что, если их взломать?

На PHDays9 вы увидите в действии эффект «цифровой» бабочки в контексте:

- промышленного IoT, умного дома и видеонаблюдения;
- телекоммуникационных сетей;
- финансовых технологий и блокчейна;
- веб- и бизнес-приложений;
- машинного обучения;
- прикладной криптографии;
- безопасной разработки и автоматизации средств защиты;
- вредоносного ПО и разработки эксплойтов;
- целевых атак и аппаратных закладок.

#PHDays phdays.com

Практические соревнования

в уникальном реалистическом формате The Standoff — грандиозная битва экспертов по взлому и защите информации.

Более 5000 участников:

элита хакерского мира, первые лица, CIO и CISO российских и зарубежных компаний, представители интернет-сообщества и госструктур, регуляторы, политики, теоретики и практики в области медицины и нейротехнологий, деятели искусств и другие.

Открыта регистрация СМИ.
E-mail для заявок:
ysorokina@ptsecurity.com

 **КРОКУС ЭКСПО**
Международный выставочный центр



twitter.com/phdays_ru



facebook.com/PHDays

POSITIVE TECHNOLOGIES

ПУТЬ РЕГУЛЯТОРА... В ОБЛАКАХ?

ЗАДАЧИ РЕГУЛИРОВАНИЯ И ПЕРСПЕКТИВЫ
ИСПОЛЬЗОВАНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

На XI Уральском форуме во время дискуссии «Перспективы применения RegTech и SupTech» был поднят вопрос использования облачных технологий. Причем, в международном контексте. Модератор дискуссии — заместитель председателя Банка России Василий Поздышев — рассказал, что один из главных вызовов настоящего времени — это создание системы регулирования технологических рисков. Суть проблемы в том, что на протяжении последних двадцати лет банковское регулирование занималось рисками, имеющими финансовую природу — недостаточность капитала, недосоздание резервов, риски ликвидности, процентные риски и т.д. И сегодня регулирование таких рисков хорошо развито. Но в последние пять лет стало понятно, что регуляторы во всём мире упускают риски, имеющие технологическую природу, что приводит к колоссальным потерям от кибератак — до 90–100 млрд долларов в год. Очевидно, что с учётом взрывного развития новых технологий риск такого ущерба будет только возрастать.

С учётом этого были определены направления работы финансовых регуляторов во всём мире. Первое направление — разработка и принятие стандартов в области кибербезопасности. В разных странах подходы к формулированию таких стандартов различаются, но в недалёком будущем нам придётся работать над тем, чтобы сближать их друг с другом. Второе направление — составление и принятие дорожных карт по реализации технологических инноваций. Практически во всех дорожных картах присутствуют такие компоненты как идентификация и биометрия, мониторинг транзакций, централизованная система сбора и анализа отчётности, управление рисками и цифровизация регуляторных требований.

Принятие российской дорожной карты планируется в течение этого года.

Начальник Управления по обеспечению информационной безопасности Банка ВТБ Сергей Пазизин предложил использовать проект создания отечественной платформы для регуляторных и надзорных технологий как драйвер развития Российской банковской системы на основе использования облачных технологий.

На основе зарубежного опыта можно утверждать, что наиболее эффективными являются регуляторные и надзорные технологии, построенные с использованием облачных решений. Одним из таких примеров может служить система сбора и анализа отчётности Банка Австрии.

Преимущества облачных вычислений известны. Это рациональное использование оборудования в условиях неравномерной загрузки, быстрота получения услуги, экономия на капитальных вложениях, сокращение расходов на поддержку.

В ключевых докладах Уральского форума неоднократно подчёркивалась необходимость снижения издержек малых и средних банков, в том числе связанных с обеспечением информационной безопасности. Создание облачных сервисов для небольших банков позволило бы решить эту задачу в комплексе, обеспечив практически полный аутсорсинг ИТ и безопасности. Проконтролировать соблюдение требований крупными поставщиками услуг значительно проще, чем проверять сотни небольших банков.

Что касается крупных банков, то их масштабы позволяют создавать собственные корпоративные облака и вкладывать достаточно средств в обеспечение информационной безопасности. Тем не менее, ряд продуктов в настоящее время предлагается только в облачном варианте, например, системы автоматизации предприятия, решения по биометрической обработке данных, различные сервисы для организации совместной работы сотрудников. Кроме того, крупные банки заинтересованы в использовании облаков при проведении пилотных разработок, а также в развитии облачных сервисов для своих клиентов.

Недостатки облачных решений также известны. Это:

- ♦ отсутствие необходимого уровня гарантии непрерывности предоставления услуг;
- ♦ возникновение неконтролируемых данных;
- ♦ низкий уровень сервисов безопасности существующих облачных решений (о чём на данном форуме подробно говорилось в докладе компании Symantec).

Отсутствие явно выраженной позиции регулятора в отношении условий использования облаков в банковской сфере приводит к тому, что соответствующие услуги не развиваются в России, а банки все в большей мере используют иностранные публичные облака.

В качестве положительного примера можно привести вышедшие на прошлой неделе методические рекомендации по нейтрализации угроз,

в рамках которых компания ЦФТ разрабатывает облачное решение для работы с Единой биометрической системой.

Тем не менее, вопрос об условиях возможности передачи банковской тайны для обработки в облачной платформе остаётся открытым. Например, до сих пор непонятно, считается ли размещение информации в облаке, которое обслуживает сторонняя организация, передачей информации третьему лицу? Или это исключительно аренда вычислительных мощностей, а всё остальное зависит от того, как реализована система контроля и разделения доступа?

Есть и чисто технические проблемы. Например, задача физически раздельного хранения персональных данных уже неадекватна технологиям, применяемым на практике. В среде виртуализации это требование вообще невозможно реализовать.

Для решения указанных вопросов было бы целесообразным разработать рекомендации Банка России по использованию облачных технологий в серии «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» с учётом опыта разработки документа «Обеспечение информационной безопасности при использовании технологии виртуализации».

Если необходимо, можно также использовать возможности регулятивной «песочницы» Банка России, созданной специально для проведения пилотирования и быстрого внедрения новых финансовых сервисов и технологий, требующих изменения правового регулирования.

Инициировав создание отечественной платформы для регуляторных и надзорных технологий, можно было бы не только решить задачи Банка России как надзорного органа, но и создать точку роста широкого спектра облачных сервисов для Российской банковской системы.

В перспективе, создание комплекса облачных приложений для небольших банков позволило бы, значительно снизить их расходы на выполнение требований информационной безопасности и, в целом регуляторных требований. Крупные банки в обозримом будущем продолжат развитие своих автоматизированных информационных систем, но смогут использовать отдельные сервисы, там, где это им выгодно.

В целом расширение применения облачных решений банками будет способствовать повышению экономической эффективности, прозрачности и устойчивости банковской системы. А в части банковского надзора — позволит перейти от ретроспективного к превентивному выявлению нарушений.



Сергей ПАЗИЗИН

начальник
Управления
по обеспечению
информационной
безопасности
Банка ВТБ



Дискуссия
«Перспективы
применения RegTech
и SupTech» на
XI Уральском форуме
«Информационная
безопасность
финансовой сферы»

Модератор дискуссии Василий Поздышев поблагодарил за доклад и отметил, что при обсуждении с банками каждого из проектов дорожной карты рассматривается, в том числе, и вопрос, на базе каких технологических решений этот проект будет реализован. «Пока нет уверенности, что облачные технологии менее рискованные, чем другие. Аргумент сторонников облаков состоит в том, что в системы безопасности общественных облаков могут быть вложены настолько большие средства, какие ни один банк, даже Центробанк, в своё частное облако вкладывать не станет. Аргумент такой... обсуждаемый. На самом деле, будем смотреть каждый раз индивидуально», — подвёл итог Василий Поздышев.

Артём Сычёв, первый заместитель директора Департамента информационной безопасности Банка России, со своей стороны пригласил желающих поработать над стандартом безопасности облачных технологий на площадке ТК 122 в подкомитете по безопасности финансовых (банковских) операций. А также предложил более внимательно посмотреть на возможности использования текущих уже документов. Прежде всего, стандарта по аутсорсингу и рекомендаций по виртуализации.

Третью позицию со стороны регулятора представил и.о. директора Департамента финансовых технологий Банка России Иван Зимин. Он отметил, что в Банке России часто обсуждается вопрос применения облачных технологий. В конце 2018 года вышел обзор, в котором, в том числе, содержатся подходы регуляторов по аутсорсингу облачной инфраструктуры. «В этом году в рамках основных направлений развития финансовых технологий уже запланирована работа, связанная с выработкой предложений по использованию облачной инфраструктуры сторонних поставщиков, именно в кредитно-финансовой сфере. Поэтому мы в любом случае либо рекомендации, либо определённые требования в этой части предъявим», — сказал Иван Зимин.

* * *

Дальнейшая дискуссия по теме продолжалась с участием зала и в кулуарах форума. Учитывая большой интерес к теме применения облачных технологий в финансовом секторе, поднятой Сергеем Пазизиным, BIS Journal предоставил свои страницы для развития дискуссии.

BIS-КОММЕНТАРИЙ

БАНК-КАК-СЕРВИС

ЗАИНТЕРЕСОВАН ЛИ БАНК РОССИИ В ТАКОЙ УСЛУГЕ?

Кредитные организации РФ видят серьёзные преимущества переноса ИТ-инфраструктуры на облачную платформу и начинают делать шаги в этом направлении. Малые и средние банки ищут в переносе банковских сервисов в облака снижение своих операционных расходов. Крупные банки чаще идут по пути построения собственных корпоративных облаков, тем самым снижая свои риски за счёт более высоких издержек на поддержание инфраструктуры. Однако даже они ищут снижения расходов за счёт переноса части своих услуг на плечи внешних операторов.

Операторы, уже имеющие созданную инфраструктуру и развитую систему её поддержки и сопровождения, заинтересованы в более эффективном способе её использования и частичном возврате вложенных инвестиций. В том числе и за счёт предоставления инфраструктуры в виде сервиса.

Однако представляется, что «инфраструктура-как-сервис» мало интересна малым и средним банкам по причине того, что издержки на содержание собственной службы ИТ, вынужденной переносить в арендованное облако свои приложения, остаются относительно высокими. Им скорее была бы интересна услуга «Банк-как-сервис», по сути предоставляющая под ключ весь набор типизированных банковских приложений. Переложив на плечи оператора вопросы поддержания и развития инфраструктуры, а также техническую поддержку и сопровождение прикладных банковских систем, кредитные организации могут сосредоточить усилия на совершенствовании предоставляемых бизнес-услуг.

Бизнес развивается очень динамично. И не все банковские задачи можно типизировать. Однако, ориентируясь на мелкие и средние банки, оператор услуг «Банк-как-сервис» быстрее и дешевле реализует нестандартную финтех услугу, чем то же самое сделает небольшой банк, опираясь лишь на собственные ИТ-ресурсы.

Наметившийся мировой тренд по оказанию услуг «Банк-как-сервис» подтверждается появлением таких организаций, как: The Bancorp, Fidor, OCBC Bank и пр.

В российских условиях инфраструктурой, достаточной для размещения подобного сервиса, обладают операторы связи, имеющие помимо развитой аппаратной части ещё и каналы, что в случае с финансовыми технологиями может стать определяющим. Выступив в консорциуме с разработчиками прикладного банковского ПО, они могут предложить рынку законченную услугу «Банк-как-сервис», не уступающую по своим характеристикам прикладным банковским системам крупных банков.

Однако в этом вопросе ключевую роль будет играть мнение Банка России, как регулятора в данной области. Вынос в облако всей банковской инфраструктуры связан с обеспечением информационной безопасности, а также юридическими аспектами предоставления услуг ИБ в облаках.

Наличие явных преимуществ в виде централизованной банковской отчётности, сокращения издержек на аудит кредитных организаций, использующих облачную инфраструктуру для оказания банковских услуг, позволяют предполагать заинтересованность Банка России в нормативном регулировании данной деятельности.

Тренд на использование облачных инфраструктур в финансовой отрасли может видоизменяться с течением времени, однако необходимость регулирования предоставления безопасных услуг в облаках останется неизменной на ближайшие годы. Наличие нормативной базы, регулирующей использование облачных финансовых приложений, будет не только ограничивать кредитные организации в предоставлении финансовых сервисов небезопасным способом, но и стимулировать их к расширению спектра предоставляемых услуг, вынесенных в облако. Поскольку отсутствие регулируемости рынка создаёт для него риски, а наличие правил их снижает.

* * *

Исходя из этого, наличие нормативных документов, регулирующих обеспечение ИБ в облачной инфраструктуре при предоставлении банковских услуг, было бы серьёзным вкладом регулятора в развитие кредитно-финансовой сферы.



**Александр
НИКИТИН**
генеральный
директор «ЛИНС-М»



Андрей КУРИЛО

BIS-КОММЕНТАРИЙ

ТРЕБУЕТСЯ КОНСОРЦИУМ

ПО АНАЛОГИИ С НСПК И СИСТЕМОЙ SWIFT

С проблематикой, поднятой автором, происходят совершенно необыкновенные вещи. Уже много лет подряд различные авторы стараются раскрыть эту тему в печатных изданиях и в выступлениях на конференциях и семинарах. Различные коммерческие фирмы, включая крупные корпорации, предлагают решения по облачной обработке и хранению данных банкам и банковским ассоциациям. Но вопрос пока не продвигается с места и не находит своего разрешения. Поэтому то, что вопрос был поднят и обсуждался на столь представительной сессии Уральского форума, есть очень хороший знак. От души хочется пожелать успехов в решении этой задачи.

Проработка показывает, что переход на облачные технологии действительно потенциально позволит существенно повысить эффективность регуляторных и надзорных технологий, снизить издержки малых и средних банков на обеспечение информационной безопасности и поддержку IT, в целом поднимет эффективность работы клиентов сервиса и повысит уровень безопасности. Об этом уже много и убедительно сказано.

Следует отметить, что проблема носит многоплановый системный характер. Выделяются две стороны вопроса. С одной стороны, существует заинтересованность регулятора в создании универсальной платформы для реализации регуляторных и надзорных технологий, а с другой стороны, заинтересованность финансовых организаций в снижении своих издержек и получении современных сервисов и услуг, позволяющих улучшить конкурентоспособность и снизить издержки на непрофильную деятельность, под которой в общем случае следует понимать содержание информационной инфраструктуры и обслуживающей её системы безопасности. Очевидно, что обе эти задачи связаны, представляют собой две неразрывные стороны одного целого и не могут быть эффективно решены по отдельности. Но к сожалению, мы не видим даже пер-

вых практических шагов в этом направлении. Вернее, видим то, что кредитные организации с удовольствием арендуют серверные мощности в различных ЦОД, но далее аренды серверов дело заходит редко. Есть правда тенденция развёртывания небольших частных «облаков» в интересах одного собственника или владельца. Пока в направлении создания крупных облачных сервисов продвинулись только крупнейшие банки страны и прежде всего, Банк России со своим «частным облаком Банка России ЧОБР». При этом создаваемое ЧОБР не является публичным и, насколько мы знаем, ЦБ РФ предоставлять облачные сервисы кому-либо не предполагает. О развёртывании облачных технологий на ЦОДах, созданных Сбербанком, известно меньше, но и там, похоже, аналогичная картина.

Таким образом, банковское сообщество в условиях отсутствия ясной линии действий, включая «сигналы» регулятора, предпочитает пока оставаться в понятных для него рамках поведения, которые не выходят пока за рамки аренды мощностей. Или вдруг отдельные банки решаются на вынос некоторой функциональности в зарубежные облака, не имеющие никаких гарантий доверия. И то и другое плохо.

Напрашивается вывод, что есть некоторые убедительные причины, приводящие к торможению процесса. На мой взгляд, к ним следует отнести несколько разноплановых, но взаимно связанных факторов.

1. Отсутствие доверия к облачным сервисам (ключевой вопрос), понимаемого как наличие у предлагаемого сервиса:

а. Таких свойств безопасности, которые позволяют собственнику ресурса получить уверенность в том, что данные, обрабатываемые с использованием этого сервиса защищены от киберугроз и, прежде всего, от несанкционированного доступа со стороны:

- ◆ других кредитных организаций;
- ◆ атак внешних и внутренних нарушителей;
- ◆ персонала ЦОД;
- ◆ регулятора (ов).



б. Прозрачности деятельности и подотчётности оператора сервисов (облака) по обеспечению эксплуатации систем и оборудования ЦОД, а также обеспечению требований информационно безопасности, позволяющей убедиться в том, что деятельность по обеспечению защиты информации и эксплуатации осуществляется в соответствии с установленными требованиями и регламентами.

с. Гарантий компенсации возможных убытков при реализации кибератак или нарушении непрерывности предоставления услуг.

Очевидно, что доверие к сервисам должно быть обеспечено на бизнес-уровне (по аналогии — на последнем, седьмом уровне модели взаимодействия открытых систем. Такой уровень доверия не обеспечивается автоматически требованиями технического характера по защите информации в облачных средах, разработанными для использования на более низких уровнях модели и не гарантируется наличием соответствующих сертификатов и аттестатов, хотя они в обязательном порядке должны быть.

2. Отсутствие стандартных услуг, сервисов и моделей обработки и хранения данных в облачных сервисах в виртуальном пространстве.

3. Отсутствие принципов и регламентов осуществления регуляторных и надзорных действий, включая аудит информационной безопасности, что диктует необходимость создания Банком России отечественной платформы для регуляторных и надзорных технологий

для работы в централизованных защищенных облачных средах.

4. Отсутствие необходимого уровня гарантии непрерывности предоставления услуг.

5. Отсутствие внятных предложений по стоимости предоставляемых сервисов с учетом того, что облачные сервисы должны быть дешевле локальных кастомизированных решений.

6. Высокая и до конца не оцененная стоимость решения для потенциального оператора данного сервиса, неясные финансовые параметры проекта, что не позволяет подготовить ясный бизнес-план и обосновать затраты на создание системы и оценить потенциальную прибыль.

Всё это приводит к выводу, что данная тема представляет собой крупный системный проект. Размерность этого проекта такова, что его реализация требует создания консорциума заинтересованных организаций из числа кредитных и некредитных финансовых организаций, поставщиков облачных услуг и сервисов, собственников ЦОД, провайдеров телекоммуникационных услуг, возможно, инвесторов. При этом, немаловажным фактором является равноудалённость консорциума как от каждого из участников, так и от государственных регуляторов¹. При этом, в обязательном порядке вопрос требует нормативного регулирования

¹ По типу организационной структуры и юридической формы системы SWIFT

со стороны государственных регуляторов, прежде всего, со стороны Банка России. Более того, если такого регулирования не будет, вопрос так и продолжит оставаться в нынешнем положении. Подобный опыт создания крупных независимых систем для предоставления финансовых услуг и сервисов есть (например, опыт создания НСПК). Но в отличие от НСПК, ожидаемым участием Банка России в данном процессе представляется выполнение роли регулятора и потребителя специфических сервисов, что предполагает:

- ♦ нормативное регулирование вопроса, включая разработку необходимых стандартов (как бизнес-уровня, так и технических);

- ♦ создание платформы для реализации регуляторных и надзорных технологий, разрабатываемых Регулятором в интересах повышения качества осуществляемой им деятельности и предназначенной для работы в создаваемой специализированной защищенной облачной среде, предоставляющей услуги кредитным и некредитным финансовым организациям.

Представляется, что инициатором процесса в рамках приведённых параметров может выступить Ассоциация банков России, в полной мере владеющая нюансами вопроса.



Алексей ЗАБРОДИН
технический директор
РТК-ЦТ, Ростелеком

BIS-КОММЕНТАРИЙ

МАСШТАБ ЗАДАЧИ ОЧЕВИДЕН

РОСТЕЛЕКОМ РАЗВИВАЕТ СВОЮ ОБЛАЧНУЮ ПЛАТФОРМУ НЕСКОЛЬКО ЛЕТ

Наша Компания является национальным провайдером цифровых сервисов. Имея богатый опыт использования облачных технологий, могу заявить, что несмотря на кажущуюся простоту, реализовать полноценное облачное решение, удовлетворяющее всем требованиям бизнеса и регуляторным требованиям, может себе позволить только крупный игрок рынка, обладающий необходимыми вычислительными мощностями и, что немаловажно, набором компетенций в самом широком спектре областей, начиная от строительства ЦОДов, заканчивая минимизацией последствий кибератак.

Понимая это, мы несколько лет развиваем единую облачную платформу, которая позволит государственным и частным организациям, организациям банковского сектора и облачным провайдерам размещать свои сервисы в единой облачной инфраструктуре, обеспечивая при этом соответствие всем регуляторным требованиям, а также превентивно реагируя на современные киберугрозы. Создание такой платформы позволит консолидировать существующие

облачные технологии, технологии защиты информации, накопленный опыт по управлению информационной безопасностью, а также минимизировать стоимость владения системами. Одновременно будут снижены технологические риски и риски информационной безопасности.

Применяемые в платформе технологии каскадных периметров защиты позволяют отражать атаки на наиболее ранних периметрах безопасности — каналы провайдера, периметр ЦОД и т.д., доводя до серверов максимально очищенный трафик. Данный подход позволяет не только эффективно бороться с угрозами информационной безопасности, но и экономить вычислительные ресурсы заказчиков. Ситуационный центр является неотъемлемой частью единой платформы и позволяет контролировать качество предоставления сервисов, оперативно реагировать на инциденты, используя, в том числе, данные об атаках, накопленные за время функционирования Ситуационного центра, данные полученные от российских и мировых производителей оборудования, а также независимых ситуационных центров.



КРИПТОПРО NGate

Универсальный высокопроизводительный VPN-шлюз, позволяющий быстро и безопасно реализовать защищённый удаленный доступ к корпоративным ресурсам и информационным системам (в том числе к объектам критической информационной инфраструктуры) через незащищенные каналы связи, в том числе сети общего пользования.

Поддержка ГОСТ и зарубежных алгоритмов

NGate обеспечивает поддержку TLS-ГОСТ наравне с зарубежными криптографическими алгоритмами. Это позволяет реализовать плавный перевод защиты доступа к web-ресурсам на ГОСТ.

Выполнение требований регуляторов

Серверные и клиентские компоненты NGate сертифицированы по требованиям к СКЗИ и имеют соответствующие сертификаты ФСБ России по классам КС1, КС2 и КС3. Это позволяет использовать NGate для защиты персональных данных при передаче по незащищенным каналам связи (152-ФЗ). Так же NGate может использоваться для удаленного доступа непосредственно к средствам (в том числе СЗИ) значимых объектов КИИ, для обновления или управления, как со стороны работников, так и со стороны лиц, не являющихся работниками субъекта КИИ (187-ФЗ). Кроме этого NGate позволяет реализовать защищенные TLS-соединения при передаче биометрических ПДн в рамках соответствующих взаимодействий в ЕБС. В настоящее время NGate входит в состав нескольких решений по подключению к ЕБС, в том числе в состав типового решения «Ростелекома», системный проект которого согласован с ФСБ России.

Простая реализация контроля доступа к ресурсам

NGate обладает широкими возможностями по управлению доступом удалённых пользователей со строгой многофакторной аутентификацией по сертификату и/или LDAP/AD, а также гибким разграничением прав доступа к ресурсам.

Аутентификация с использованием токенов

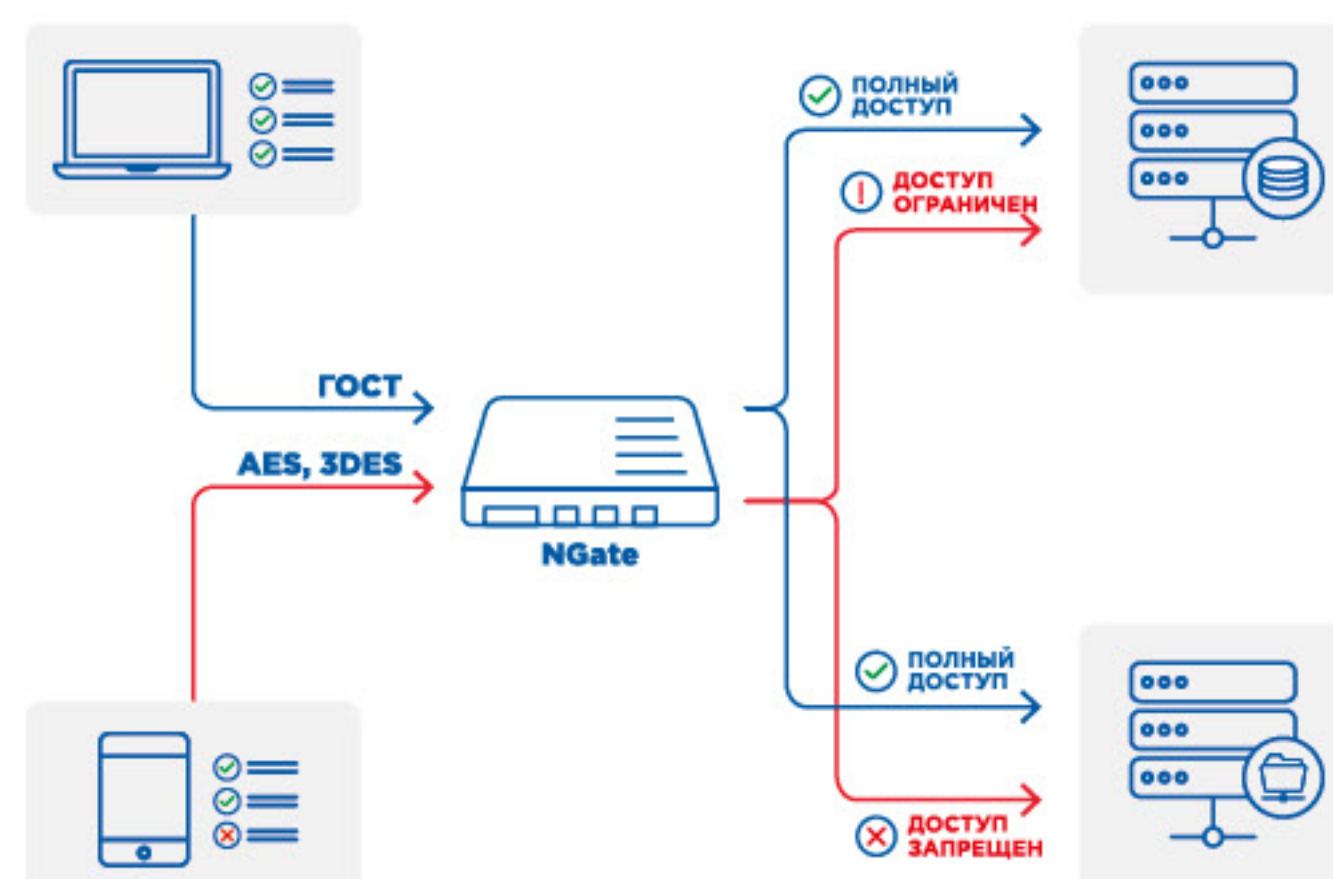
NGate поддерживает различные ключевые носители, такие как Рутокен, eToken, JaCarta, ESMART и др. – в том числе с поддержкой российской криптографии.

Три режима работы

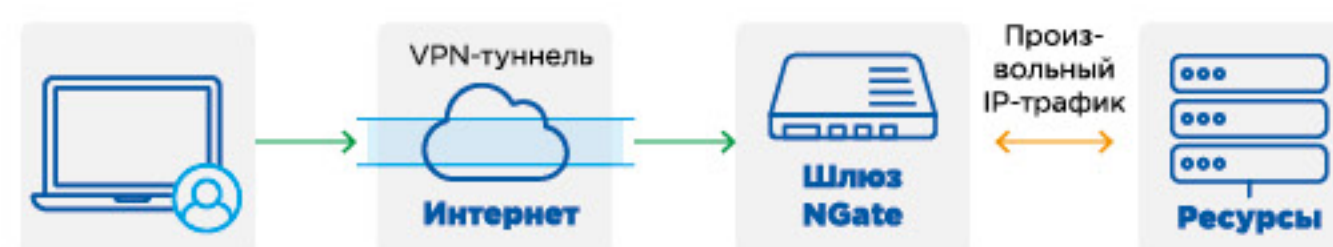
NGate может работать в трех режимах - TLS терминатора, портального и VPN доступа. Режим TLS терминатора используется для снятия нагрузки по обработке TLS-соединений с бэкэнд-серверов и серверов доставки данных.



Режим портального доступа используется для организации персонального доступа пользователей к опубликованным на портале NGate веб-ресурсам в соответствии с корпоративными политиками ИБ.



Режим VPN доступа используется для подключения к произвольным ресурсам с помощью VPN-клиента, поддерживающего все популярные платформы (Windows, macOS, Linux, iOS, Android, Sailfish). При этом разграничение доступа возможно на уровне подсетей, в том числе виртуальных (VLAN).



Масштабируемость

Один узел NGate держит до 28 000 соединений с обработкой информационных потоков до 10 Гбит/с в режиме TLS терминатора. Данные характеристики легко увеличить добавлением узлов (до 32 штук) в кластер.



Ольга СКОРОБОГАТОВА
первый заместитель председателя
Банка России

БОЛЬШИЕ ПРОЕКТЫ

ФИНАНСОВЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИИ В 2019 ГОДУ¹

ИТОГИ 2018 ГОДА

Что нам с вами удалось сделать в 2018 году? Немало. Часть проектов удалось запустить, часть пилотировать, часть подготовить в виде концепции. Перечислю.

Биометрическая идентификация. Сложный проект. Велась большая дискуссия: как это делать, нужно ли это в принципе, насколько банки готовы... Что на сегодня? 95 банков начали сбор биометрических данных, 4 тыс. отделений подключено, но контрольные закупки, которые мы провели, показали, что далеко не всё хорошо, как в процессе съёма биометрии, так и при её использовании как услуги.

Что нам не понравилось по итогам 2018 года? Во-первых, банки отчитались формально — процедура сбора биометрии не была отработана. Во-вторых, мы увидели медленное взаимодействие систем банков с системами ЕБС и ЕСИА. Причины — в том числе и объективные, например, системы Минкомсвязи не готовы оперативно реагировать на запросы. В третьих, банки очень медленно внедряют требования Банка России к информационной безопасности.

Собственно, биометрическая идентификация как национальный проект — это одна из первых систем, требующих иного подхода к ИБ. И требования, которые мы с коллегами из ФСБ и ФСТЭК выработали, признаю, очень сложные. Но мы понимали, если мы создаём столь масштабную и сложную национальную инфраструктуру, то, безусловно,

¹ Из доклада на XI Уральском форуме «Информационная безопасность финансовой сферы».

должны обеспечить конфиденциальность и корректную обработку данных. Поэтому была проведена большая работа по разъяснению банкам, что и как делать. Надеюсь, 2019-й станет годом, когда банки завершат все процедуры по ИБ.

Система быстрых платежей. Мы не первая страна, где есть такой национальный проект, но с точки зрения эффективности, для потребителя впереди нас только Швеция, Англия и Сингапур. За прошлый год мы сделали платформу, состоящую из двух частей — НСПК и ЦБ, и провели её тестирование.

Мастерчейн. На сегодняшний день это единственная технология, которую мы сертифицируем с коллегами из ФСБ.

Распределённые реестры признаны перспективными именно для банковских операций. Правда, к нам уже обратились и страховые компании, чтобы работать на платформе Мастерчейн, но мы не торопимся, нам важно идеально выстроить и отладить все процессы, причём с точки зрения клиента. Просто внедрить новые решения без изменения процесса или без создания нового процесса невозможно.

Финансовый маркетплейс. Это один из проектов, который позволяет повысить конкурентоспособность на рынке банковских продуктов и услуг. Понятно, он не заменит другие маркетплейсы, но у нас была идея сделать площадку, где маленькие и средние банки смогут конкурировать с большими. В конце 2018 года мы подготовили законопроект по бизнес-процессам, а в 2019-м планируем сделать пилот и провести ряд операций.

Цифровой профиль. Объявлен одним из приоритетных проектов программы «Цифровая экономика РФ», и в этом году ему будет уделено соответствующее внимание.

ПЛАНЫ НА 2019-Й

В 2019 году мы не стали начинать новых проектов, так как считаем, что нужно быть последовательными и полноценно завершить начатое (рисунок 1).

По биометрии мы ожидаем, что к середине года 60% отделений всех банков будет подключено, и требования по информационной безопасности будут ими выполнены. Начнётся активное развитие удалённых услуг, которые мы считаем основой этой платформы.

По быстрым платежам. Двенадцать банков уже в пилоте, начали операции B2B и Me2Me, и в 2019 году мы выйдем с ними в промышленную эксплуатацию.

Мастерчейн. Платформа опробована, крупнейшие банки пилотировали её по электронным закладным, цифровым банковским гарантиям и гарантиям аккредитивов, и она постепенно выходит в пром. Основной вопрос сейчас с Росреестром, который со своей стороны должен автоматизировать часть операций, чтобы N2N процессы проходили бесшовно для клиентов.

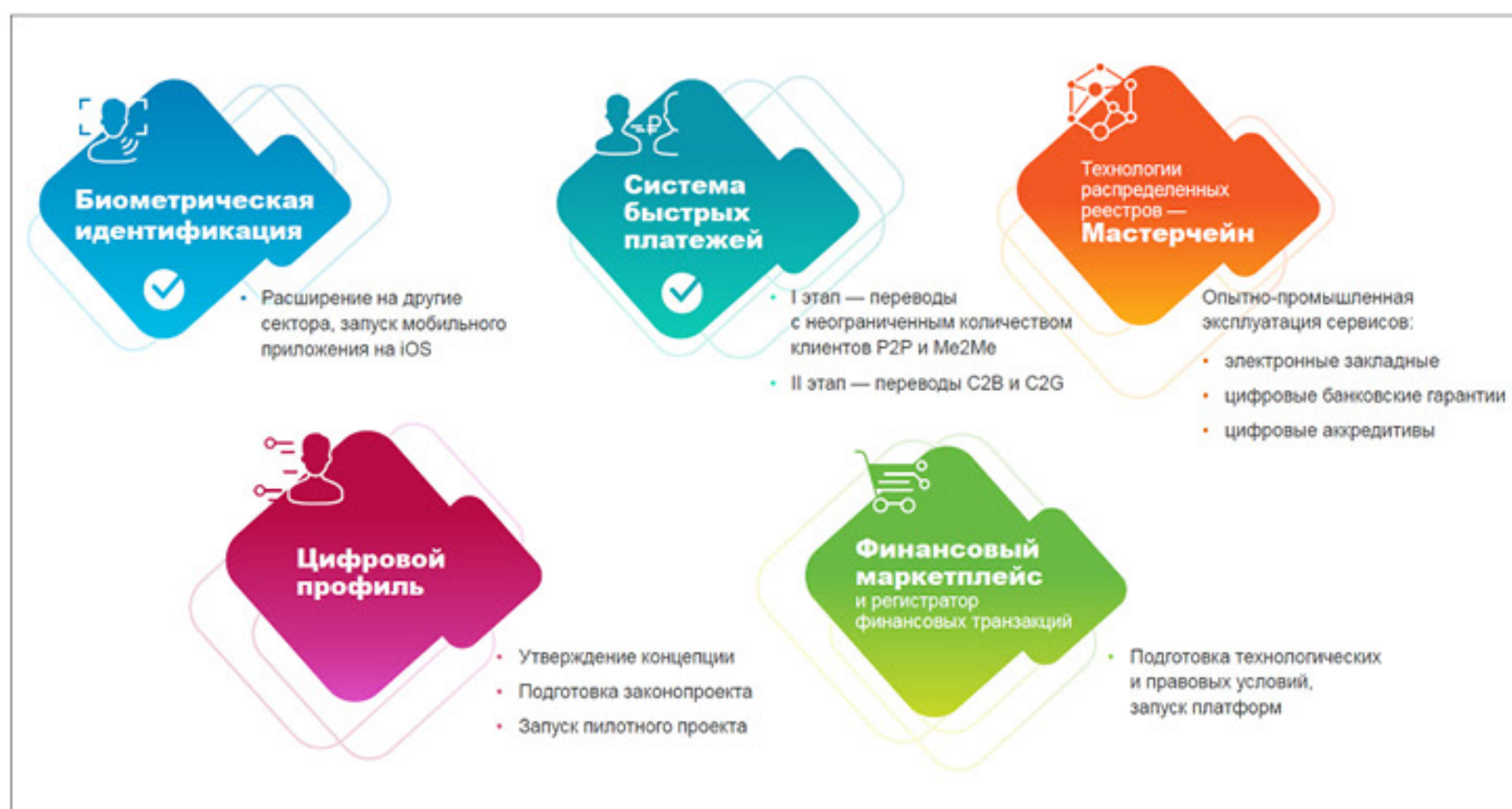


Рисунок 1. Банк России. Финансовые технологии. План на 2019 год

Финансовый маркетплейс. Тут завершается подготовка технологических и правовых условий и начинается запуск платформы непосредственно с банками.

Цифровой профиль. Осенью планируем опробовать его прототип с рядом банков.

О БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Повторюсь, биометрия — проект очень сложный, и не только с точки зрения информационной безопасности, но и технологически. Социологический опрос показал, что клиент готов участвовать в этом проекте при условии, если процесс съёма биометрии занимает пять минут. Сейчас он занимает от 10 до 25 минут в разных банках.

Я сама сдавала биометрию дважды. В одном банке мне так и не смогли её снять, хотя и сказали на прощание, мол, идите, всё хорошо, найдёте себя на портале с созданной биометрией. Через три дня я себя там не нашла. Это ещё одна тема: как банки должны правильно работать, чтобы у клиента не осталось негатива. А второй банк провёл эту операцию успешно. Но ни в первый, ни во второй раз мне, как клиенту, эта процедура не понравилась — как-то тяжело и очень долго. Когда мы стали разбираться, оказалось, что многие шаги лишние. Банки попросту не озадачились тем, чтобы сделать этот процесс удобным для клиента.

Поэтому сейчас у нас по биометрии две задачи: сделать съём данных клиента за пять минут и внедрить требования по информационной безопасности.

На рисунке 2 представлены три варианта решений по ИБ: банки могут внедрить собственное решение по встраиванию HSM в ядро инфраструктуры, могут использовать типовое решение, которое прошло сертификацию в ФСБ, или работать над облачным решением. Третий вариант, на мой взгляд, больше актуален для малых и средних банков.

Было много вопросов по поводу получения ключей проверки КЭП. Сейчас эта проблема решена, банкам стало удобно. Другая, достаточно ёмкая с точки зрения инвестиций, тема — внедрения сверхзащиты каналов связи по КСЗ.



Рисунок 2. Развитие проекта Биометрическая идентификация

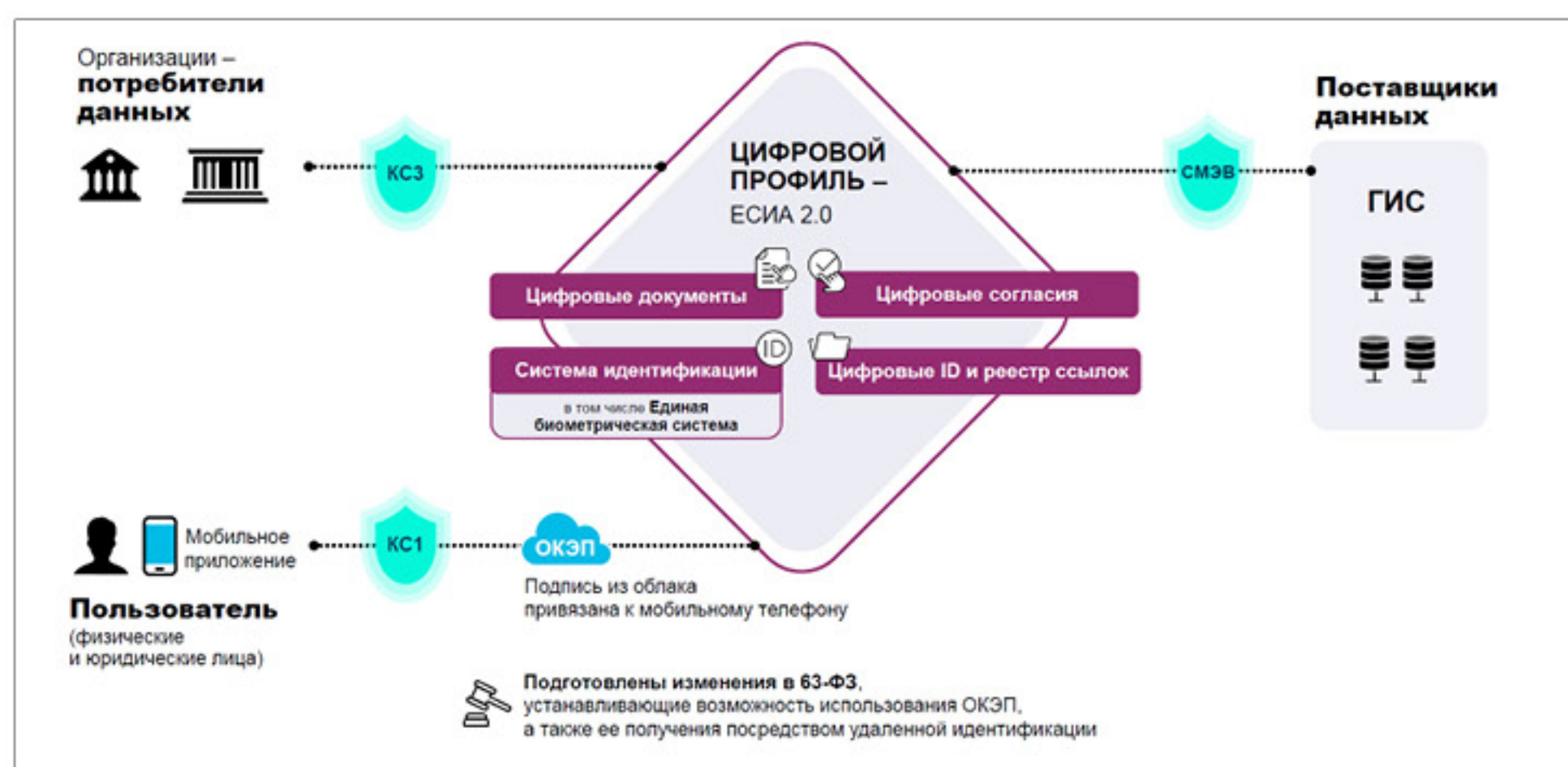


Рисунок 3. Проект Цифровой профиль

Должна сказать, что эти требования Банка России касаются не только биометрии, защита этого канала необходима для всех видов операций.

Про мобильные приложения. Наш клиент живёт в смартфонах, и в принципе ему только этот инструмент и удобен, поэтому удалённая идентификация заработает в полной мере, когда будут работать приложения на самых востребованных платформах Android и iOS. Приложение на Андроиде уже работает, iOS прошёл сертификацию и, надеемся, с марта будет доступен.

ЦИФРОВОЙ ПРОФИЛЬ

Несколько слов о цифровом профиле (рисунок 3). Не будем путать с электронным паспортом, проект которого также запущен и обсуждается как инициатива программы «Цифровая экономика РФ».

Цифровой профиль предполагает создание реестра данных, базирующегося на информации из госисточников. Речь не о создании одного, общего хранилища всех данных, существующих в госисточниках, а о возможности по определённому ключу запросить информацию из разных источников, если клиент дал на это согласие. Самое сложное тут — создать реестр согласия. Клиент должен видеть, когда и кому он

давал согласие, должен понимать технологию, как он может отозвать своё согласие и как мониторить предоставление данных о себе разным организациям и компаниям.

Эта тема, безусловно, связано с ОКЭП — достаточно защищённая электронная подпись у клиента должна быть. Мы рассчитываем на всё наше активное население, поэтому удобство и безопасность — условие и необходимое и достаточное. А также создание мобильного приложения, которое позволит гражданам пользоваться цифровым профилем комфортно.

В октябре прототип такого цифрового профиля будет готов, и мы представим его на суд правительства.

ТРЕНДЫ В СФЕРЕ ИБ

Создавая инфраструктуру национального масштаба, мы должны быть уверены, что наши потребители и госисточники будут надёжно защищены. Поэтому ни один проект по финтеху у нас не осуществляется без учёта информационной безопасности. Уже на стадии предпроектной подготовки мы ориентируемся на наших граждан и контрагентов — коллег по ИБ из разных министерств и ведомств.

Тут важно понимать местоположение России в международном контексте (рисунок 4).

По уровню кибербезопасности мы занимаем 23-е место из 60. Этого явно недостаточно, но у нас есть все шансы подняться в тройку лидеров и потеснить Японию, Францию или Канаду. Что даёт такие надежды? Не только большие проекты Банка России, хотя они, безусловно, играют важную роль: задают масштаб и уровень ИБ в стране. Но не менее важно и общее оживление в сфере нашей ИБ. Многие компании стали активно сотрудничать со стартапами и финтех-компаниями, причем именно для того, чтобы решения на выходе сразу имели встроенные инструменты информационной безопасности.

И это, кстати, мировой тренд. Недавно я была на большой финтех-конференции в Париже, и вот что бросилось в глаза. Многие проекты представлялись со сцены не одним, как обычно, ответственным лицом, а несколькими: инициатором проекта, исполнителем и представителем по информационной безопасности, которая теперь изначально является частью общего процесса. Эту тенденцию я увидела и на Уральском форуме.

Следующее. Если посмотреть, как фокусируется безопасность по секторам, то на удивление почти поровну: 36 % сетевая безопасность, 30 % безопасность приложений и 34 % безопасность данных. При этом в кулуарах международных

форумов говорят в основном о том, насколько сложно обеспечивать безопасность именно в части данных, потому что в разных странах действуют разные законодательства. Не все шишки ещё набиты. Большой вопрос: что есть персональные данные, а что — не персональные? Что считать доступными данными, обезличенными и т.д. Дискуссия не угадет, и какого-то правила, которое мы с вами могли бы взять и применить, нет. Нам придётся пройти этот путь вместе со всеми, и очень быстро.

Интересный тренд по мотивам злоумышленников (рисунок 5). По международным источникам они 45 % времени тратят на получение данных, а 33 % на финансовую выгоду. Тут, конечно, натяжка. На самом деле, данные они получают для финансовой выгоды, цель одна — получить деньги с клиента или компании, но то, что это делается через данные — весьма симптоматично.

Пугает тренд по утечке записей, это к вопросу о защите данных. С 2012 года цифра тут выросла в шесть раз, и это мягкий вариант, есть источники, где эти цифры гораздо больше.

Организация мишени атак. Интернет-порталы, понятно, самая большая, доступная и потому главная мишень — 32,3%. Банки занимают второе место — почти 20%. Почему всего 20%? Интерес к банкам, как к источнику наживы, традиционно огромный, но исторически они защищены лучше, чем другие организации и компании, в них сложнее проникнуть, и преступники это знают. С другой стороны, банки, как бы хорошо они ни защищались, всегда будут под прицелом, внимания злоумышленников им не избежать никогда.

ПОДВОДЯ ИТОГИ

Ключевая мысль следующая. Когда мы делаем масштабные проекты, то с точки зрения информационной безопасности должны максимально использовать унифицированные решения. Почему? Чтобы избежать ненужного усложнения и нагромождения. Например, в биометрии мы сначала использовали один спектр решений, а в цифровом профиле принципиально другой, хотя по модели угроз они похожи. И получается, мы нагружали участников рынка неоправданными затратами. Вывод очевиден: везде, где это возможно, мы должны искать общее решение совместно с коллегами по информационной безопасности банков. Безусловно, кастомизированные под какие-то конкретные случаи решения возможны, но не нагружая индустрию непомерными требованиями.

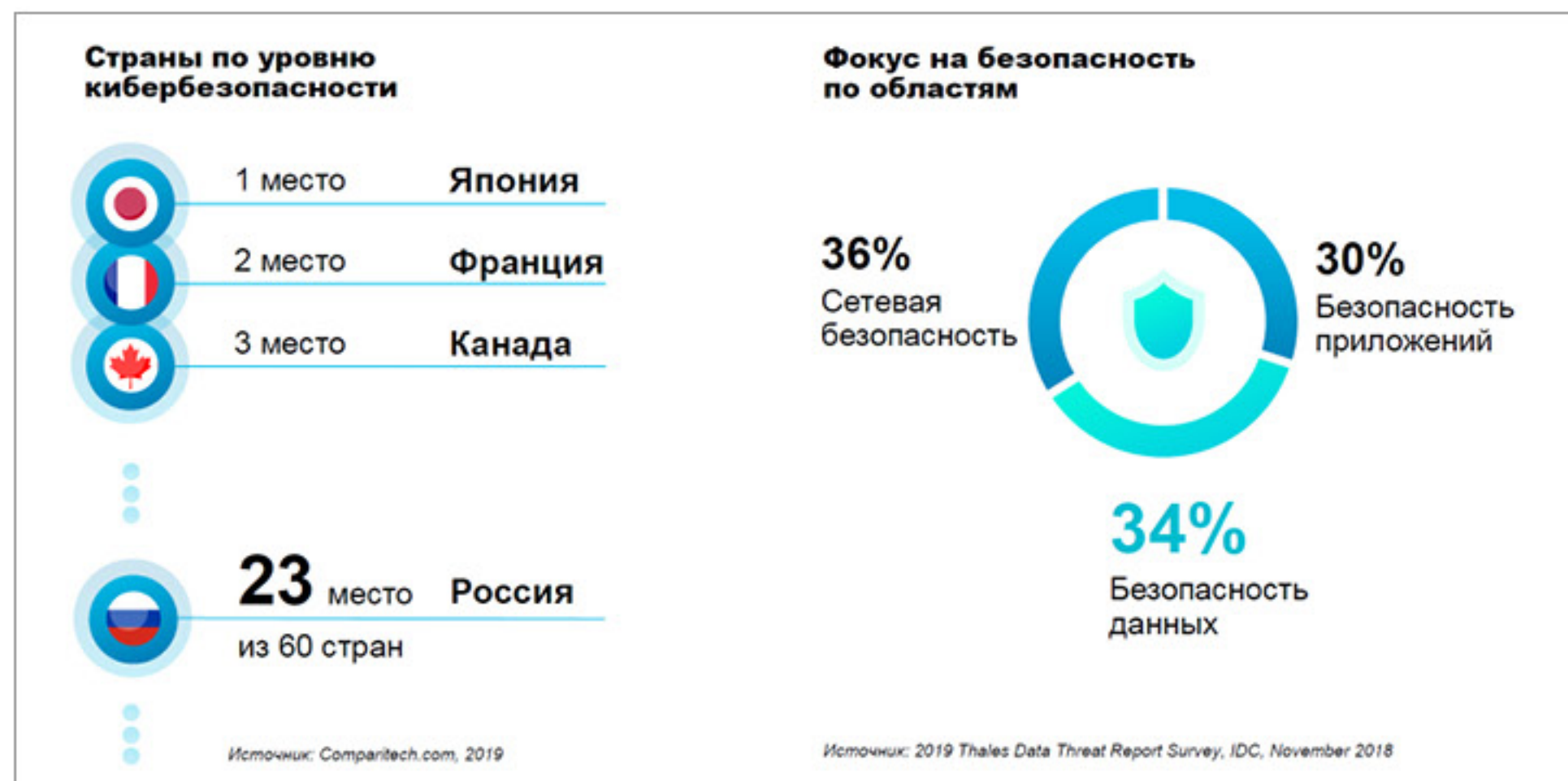


Рисунок 4. Тренды в сфере информационной безопасности

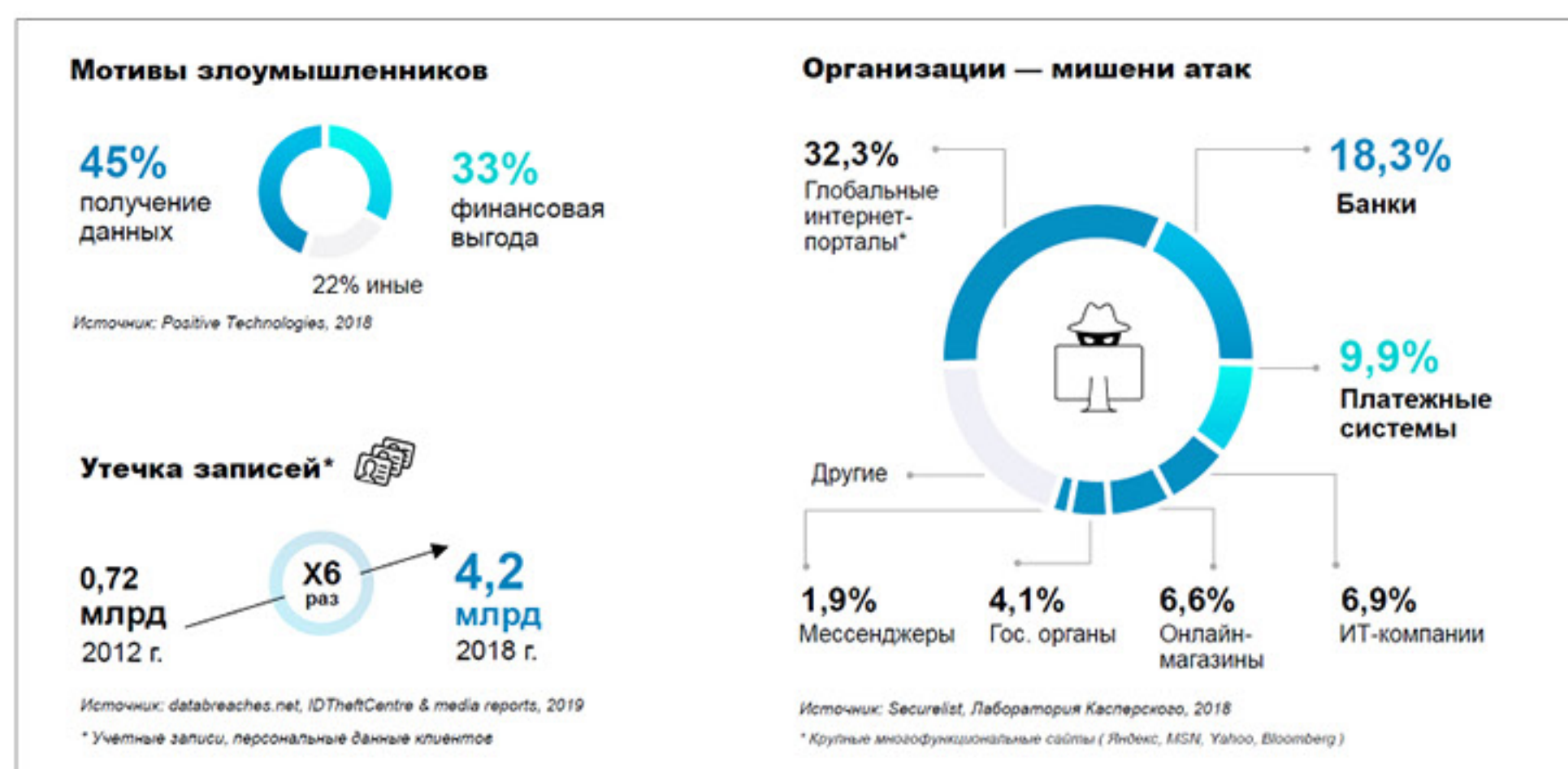


Рисунок 5. Тренды в сфере информационной безопасности — продолжение

На примере биометрии и цифрового профиля мы такой подход идеологически заложили, и тут требования по информационной безопасности теперь максимально синхронизированы. Такой же подход к системе быстрых платежей и в финансовом маркетплейсе.

Но распределённые реестры — новый зверь. Тут нет типовых решений, которые мы могли бы просто взять и встроить, поэтому тут мы с коллегами из ФСБ и ФСТЭК проходим свой собственный путь. Я думаю, что этот опыт поможет нам и в дальнейшем. Другие проекты, основанные на распределённых реестрах, могут строиться на этих наработках.

Чего Банк России ждёт от коллег по информационной безопасности? Конструктивности и гибкости. Понятно, что ИБ всегда нацелена именно на безопасность, то есть там, где встаёт вопрос: «Можно или нельзя?» — лучше «нельзя», а там, где «можно», давайте сделаем так сложно, чтобы всё равно было «нельзя». Теперь эта парадигма изменилась. Теперь мы должны находить те решения, которые дадут нам возможность быстро развивать проект, при этом, решая и задачу по безопасности.



Дмитрий СКОБЕЛКИН
заместитель председателя
Банка России

ШИРОКИМ ФРОНТОМ

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВОЙ СФЕРЫ¹

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ И РИСКИ

Безусловно, цифровая трансформация создаёт многочисленные преимущества для клиентов финансовых организаций. Увеличивается качество, скорость и доступность взаимодействия клиентов с финансовым сектором, снижается стоимость услуг. Вместе с тем отсутствие должного внимания к безопасности технологий и защищённости созданных на их основе сервисов создаёт дополнительные риски как для банков, так и для их клиентов.

Неслучайно эксперты Всемирного экономического форума (проходил в Давосе 22–25 января 2019 г.) определили кибератаки в качестве базового глобального технологического риска 2019 года (рис. 1). Очевидно, что наблюдаемый по всему миру рост масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, требует скоординированных усилий регуляторов, поднадзорных организаций и потребителей финансовых услуг.

¹ Из доклада на XI Уральском форуме «Информационная безопасность финансовой сферы»

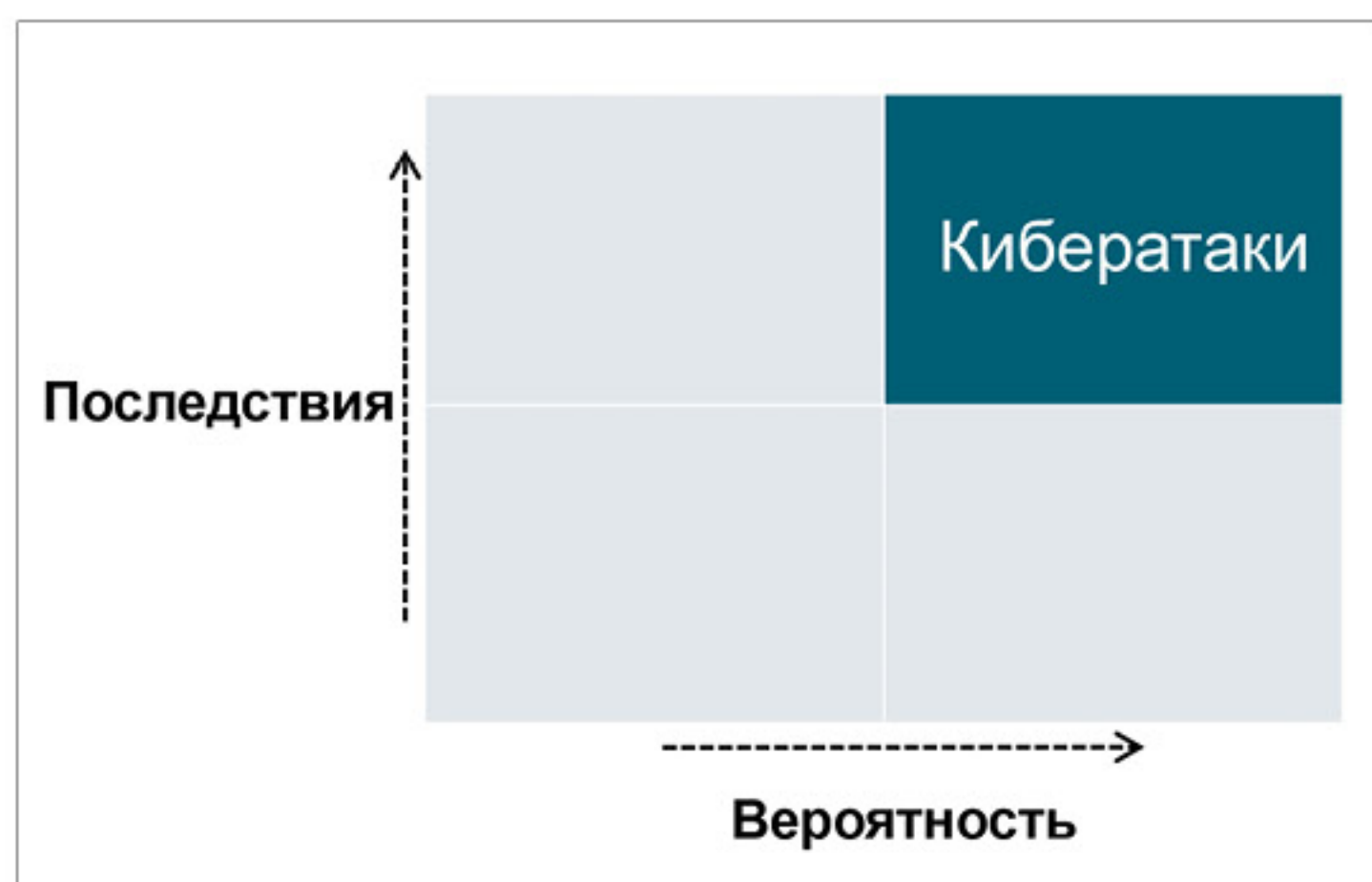


Рисунок 1. Глобальный ландшафт рисков (World Economic Forum Global Risks Perception Survey 2018–2019 (The Global Risks Report 2019. 14th Edition.))

До настоящего времени Банк России не фиксировал случаев существенного ущерба системно значимых кредитных организаций в результате кибератак. Однако нам известно об инцидентах в сфере информационной безопасности, которые приводили к нарушению непрерывности предоставления финансовых услуг и как следствие — к росту социальной напряжённости. Мы отслеживаем настроения в социальных сетях, и видим, что клиенты чутко и быстро реагируют на любые технологические проблемы банков.

Риску хищения подвержен объём денежных средств, сопоставимый с остатком по корреспондентскому счёту кредитной организации в Банке России и суммой прихода по этому счёту за день. Для небольших кредитных организаций такой объём средств зачастую сравним с размером их уставного капитала. Поэтому паника и уход клиентов на фоне компьютерных инцидентов могут стать одной из причин прекращения их деятельности.

РОЛЬ БАНКА РОССИИ В ОБЛАСТИ ИБ

В этой связи основная роль Банка России в сфере информационной безопасности заключается в обеспечении высокого уровня доверия населения и бизнеса к финансовой системе страны. В 2017 и 2018 годах мы проводили опрос среди клиентов порядка 40 кредитных организаций с целью выяснить уровень их доверия к используемым услугам с точки зрения их информационной безопасности. Если в 2017 году этот показатель составлял чуть более 40 %, то в конце прошлого года мы зафиксировали его на уровне 70 %.

Вместе с тем, главным критерием, по которому клиенты оценивают надёжность услуг и сервисов, является уровень хищений. Основной показатель здесь — доля несанкционированных переводов денежных средств с использованием платёжных карт. Наша задача состоит в том, чтобы эта доля в целом по всей банковской системе не превышала пяти тысячных процента (0,005 %) или 5 (пяти) копеек на 1000 (одну тысячу) рублей переводов.

В 2018 году доля несанкционированных переводов денежных средств с использованием платёжных карт составила 1,8 копейки на 1000 рублей переводов (0,0018%). Это несколько выше, чем годом ранее, что, по нашему мнению, связано с ростом прозрачности данных, которые Банк России получает от кредитных организаций (рис. 2).

Другими целями нашей деятельности в области информационной безопасности являются:

- ♦ ведение мониторинга компьютерных атак, оперативное принятие мер, направленных на сокращение потерь банков и клиентов;
- ♦ содействие развитию и внедрению инновационных финансовых технологий, которые позволяют более эффективно контролировать риск реализации киберугроз и снижать расходы на обеспечение должного уровня информационной защиты.

ПРЕДПОСЫЛКИ ДЛЯ РЕФОРМЫ РЕГУЛИРОВАНИЯ И НАДЗОРА

Уверен, что к настоящему времени сформировалось понимание значения информационной безопасности со стороны участников рынка как для их операционной деятельности, так и для достижения стратегических целей. Конкуренция между банками заставляет повышать удобство и качество финансовых услуг, в том числе, на основе новых финансовых и цифровых технологий. Одновременно расширяются права и интересы потребителей финансовых услуг с точки зрения их защиты от финансовых потерь.

Всё это приводит к тому, что факторы киберриска объективно интегрируются в состав основных рисков финансовых организаций.

Наша задача состоит в том, чтобы доля несанкционированных переводов денежных средств с использованием платёжных карт в целом по всей банковской системе не превышала 0,005%, или 5 копеек на 1000 рублей переводов

Как известно, в середине прошлого года был принят Федеральный закон ФЗ-167 в части внесения изменений в законодательство о противодействии хищению денежных средств.

Данным законом:

- ♦ существенно расширены полномочия Банка России по вопросам регулирования информационной безопасности и защиты информации в кредитных и некредитных финансовых организациях;
- ♦ изменён порядок взаимодействия регулятора с поднадзорными организациями.

Прежде добровольный информационный обмен с ФинЦЕРТ о случаях и попытках несанкционированных переводов денежных средств стал обязательным. Одновременно банки получили легальный инструмент обмена данными для предотвращения хищений.

Наряду с правовой основой мы создали технические условия для упрощения и автоматизации процесса обмена информацией об инцидентах и хищениях. В 2018 году в Банке России начала работу Автоматизированная система обработки инцидентов (АСОИ). Она позволяет:

- ♦ обмениваться информацией об актуальных угрозах и инцидентах, данными о совершении перевода денежных средств без согласия клиента (включая покушения);
- ♦ сообщать в Банк России о планируемых мероприятиях по публичному раскрытию информации об инцидентах.

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 платёжных карт	0,005%	0,0016%	0,005%	0,0018%	0,005%



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

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

Рисунок 2. Цель Банка России в области обеспечения информационной безопасности

Предполагается выстроить единую систему удостоверяющих центров в кредитно-финансовой сфере, где удостоверяющей центр Банка России станет головным для всего финансового рынка

Сегодня информационный обмен через АСОИ ФинЦЕРТ осуществляют более 600 организаций. Среди них:

- ♦ 437 банков;
- ♦ 39 небанковских кредитных организаций;
- ♦ 77 страховых;
- ♦ 63 иных организаций.

Отдельно стоит отметить, что на платформе АСОИ создана и введена в тестовую эксплуатацию база данных об операциях по переводу денежных средств без согласия клиента — система «Фид-АнтиФрод». С момента ее запуска мы получили информацию о более 25 000 операций, осуществлённых без согласия клиентов.

В 2019 году мы планируем:

- ♦ полностью автоматизировать информационный обмен через АСОИ;
- ♦ запустить ФИД-АнтиФрод в «боевую» эксплуатацию и начать подключать к ней некредитные финансовые организации по мере того, как для них будут вступать в силу требования ФЗ-167.

ПЛАНЫ ПО РАЗВИТИЮ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ

Что касается развития методологии обеспечения информационной безопасности, Банк России планирует выпустить нормативные документы, которые направлены:

1) на выявление в сети «Интернет» так называемых «фишинговых» ресурсов и сайтов, связанных с осуществлением незаконной финансовой деятельности.

Оперативное ограничение доступа к ним потребителей финансовых услуг требует закрепления за Банком России полномочий по их внесудебному разделегированию. Соответствующий законопроект принят Государственной Думой в первом чтении. Этот же документ, как мы надеемся, предоставит Банку России право досудебной блокировки сайтов, связанных с распространением вредоносного программного обеспечения.

2) Следующим актуальным вопросом является противодействие мобильному мошенничеству. Банк России участвует в подготовке изменений в ФЗ-115 «О противодействии отмыванию доходов, полученных преступным путём, и финансированию терроризма», предусматривающих создание единого канала обмена данными о мобильных устройствах, абонентах между операторами связи и банками.

3) Требуется доработки также механизм использования усиленной квалифицированной электронной подписи. Предполагается выстроить единую систему удостоверяющих цен-

тров в кредитно-финансовой сфере, где удостоверяющей центр Банка России станет головным для всего финансового рынка.

4) Ещё один блок связан с ожидаемым принятием закона о цифровых финансовых активах. Это потребует соразмерных требований к информационной безопасности и защите информации.

Разработка этих требований также будет вестись с участием Банка России.

5) Наконец, о национальном проекте «Цифровая экономика Российской Федерации». Здесь наша задача — координировать выработку подходов к регулированию безопасности применения на финансовом рынке таких технологий, как искусственный интеллект, большие данные, киберфизические системы, системы распределённого реестра и другие.

ПОВЫШЕНИЕ ИБ ОРГАНИЗАЦИЙ ФИНАНСОВОЙ СФЕРЫ

Мы исходим из того, что информационная безопасность и киберустойчивость организаций кредитно-финансовой сферы должны быть реализованы на трёх технологических уровнях (рисунок 3).

Это:

- 1) уровень инфраструктуры,
- 2) уровень прикладного программного обеспечения или уровень приложений,
- 3) уровень технологий обработки данных.

Развитие киберустойчивости на инфраструктурном уровне требует:

- ♦ с одной стороны, формирования комплекса отраслевых стандартов, устанавливающих требования к обеспечению информационной безопасности и управлению киберриском, а также состав и содержание соответствующих технологических, технических и организационных мер;

- ♦ с другой стороны, создания системы оценки соответствия информационной безопасности финансовых организаций требованиям национальных стандартов путём проведения внешнего аудита.

Под безопасностью на уровне приложений мы понимаем прежде всего:

- ♦ отсутствие уязвимостей в программном обеспечении, которые позволяют совершать результативные компьютерные атаки;

- ♦ введение обязательного использования прикладного программного обеспечения автоматизированных систем и приложений, сертифицированного в России или протестированного на наличие уязвимостей.

На уровне технологий и процессов обработки данных — мы ориентируемся:

- ♦ на обеспечение целостности и подлинности обрабатываемой информации;

- ♦ а также разработку требований к безопасности обработки данных для каждой новой финансовой технологии.

Уровни ИБ	Методологическая составляющая	Надзорная составляющая
Инфраструктурный уровень	домен УР – управление киберриском Защита инфраструктуры по комплексу ГОСТ домен ЗИ – защита информации домен ОН – обеспечение операционной надежности домен УА – управление киберриском при аутсорсинге и использовании сторонних информационных сервисов домен УИИСО – управление инцидентами ИБ и ситуационная осведомленность	Надзор подразделений ИБ Банка России Система внешнего аудита
Уровень приложений	Гост Р ИСО/МЭК 15408-3-2013 – критерии оценки безопасности информационных технологий, компоненты доверия к безопасности Профиль защиты для оценки уязвимости в банковских приложениях	Анализ уязвимостей приложений, критичных с точки зрения наличия уязвимостей (сертификация): - приложения клиентов - фронт-приложения Сертификация ФСТЭК России
Уровень технологий обработки данных	Обеспечение целостности информации на технологических участках ее обработки Протоколирование действий на технологических участках Взаимодействие с клиентами финансовых организаций - идентификация клиентов - получение подтверждения финансовых (банковских) операций - направление уведомлений о совершенных операциях Ведение баз данных об инцидентах ИБ, в том числе на основе претензионной работы	Анализ показателей уровня риска по операциям на технологических участках Анализ показателей, формируемых на основе претензионной работы

Рисунок 3. Основные элементы информационной безопасности

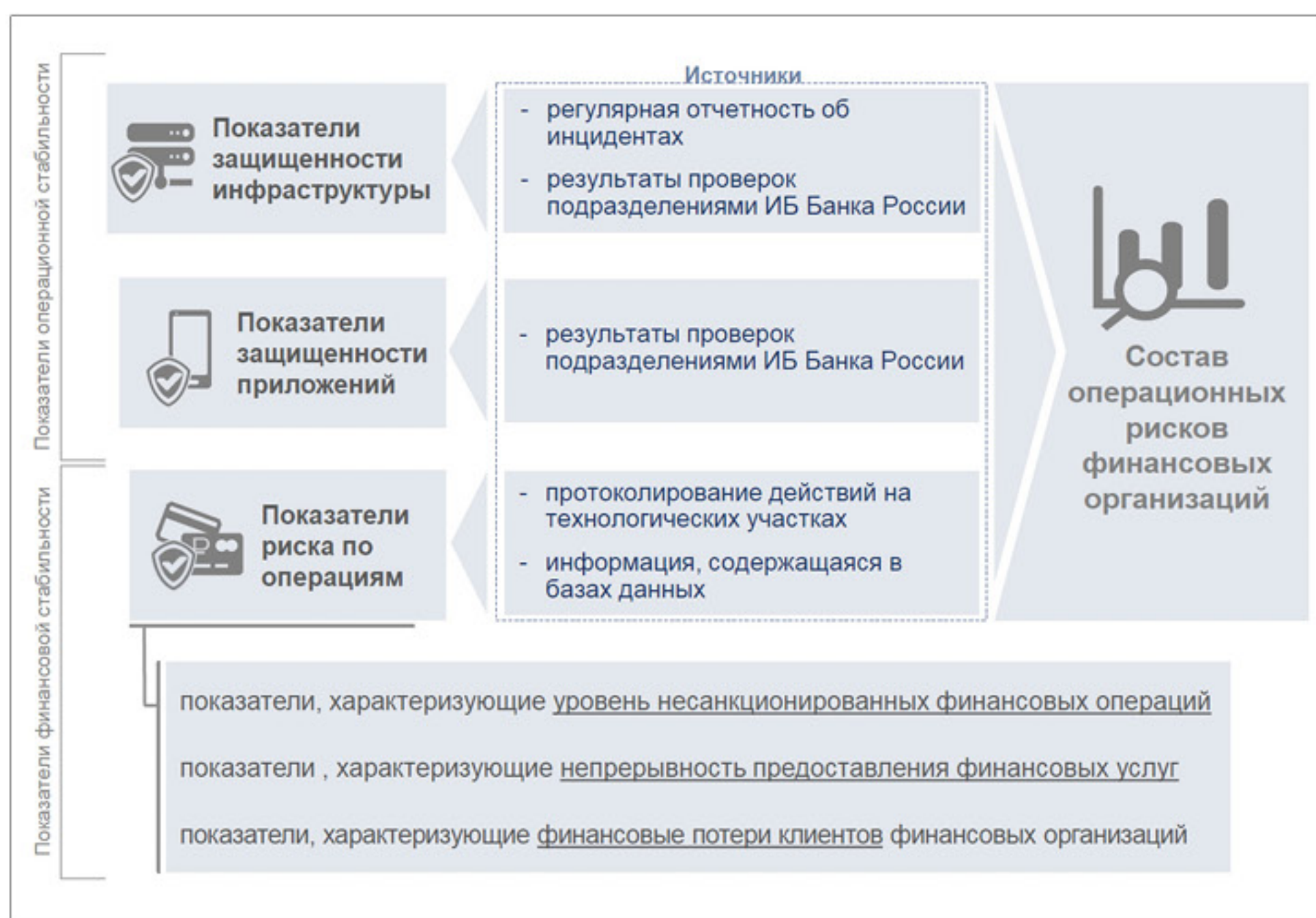


Рисунок 4. Риск-ориентированный подход. Формирование системы показателей

РИСК-ПРОФИЛИРОВАНИЕ И РЕФОРМА НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ

Обеспечение киберустойчивости финансовых организаций невозможно без осуществления контроля и надзора за состоянием их информационной безопасности. Кратко представлю некоторые планы в этой сфере.

1) Прежде всего, надзорная деятельность будет осуществляться на основе риск-ориентированного подхода (рисунок 4). Для этого Банк России будет использовать данные об уровне и качестве управления киберриском в каждой организации кредитно-финансовой сферы.

2) Участие сотрудников Банка России в надзорных мероприятиях будет, по возможности, минимизировано.

3) Также планируется использовать для оценки организаций результаты стресс-тестирований, более знакомых как киберучения.

Безусловно, формирование системы показателей потребует времени. К 2021 году мы планируем начать получение объективной информации:

- ♦ по уровню риска отдельных организаций кредитно-финансовой сферы;
- ♦ их готовности противостоять кибератакам с точки зрения обработки киберриска и его финансового покрытия;
- ♦ и как следствие уровню готовности кредитно-финансовой сферы противостоять киберугрозам в целом.

Параллельно будут разработаны методология финансового покрытия киберриска посредством страхования и установления дополнительных требований к капиталу. Данные по финансовым потерям потребителей позволят нам планировать конкретные мероприятия по защите их прав и законных интересов.

БАНК РОССИИ — КООРДИНАЦИОННЫЙ ЦЕНТР В ОБЛАСТИ ИБ

Год назад на Уральском форуме я объявил о создании в структуре Банка России Департамента информационной безопасности. С удовлетворением отмечаю, что Департамент состоялся и успешно работает. Среди основных направлений деятельности в области информационной безопасности, где требуется организация совместной работы Банка России, экспертного сообщества и участников рынка, хотел бы выделить следующие.

Во-первых, это разработка стандартов в области информационной безопасности и киберустойчивости. Она подразумевает участие представителей Банка России в работе подкомитета № 1 Технического комитета № 122 «Стандарты финансовых (банковских) операций», а также в работе международных организаций.

Вторым направлением является взаимодействие по вопросам обеспечения информационной безопасности в рамках межведомственной рабочей группы, куда входят представители МВД России, ФСТЭК России, ФСБ России, Минкомсвязи России, Росфинмониторинга, эксперты кредитных организаций.



В-третьих, Банк России активно участвует в реализации Национального проекта «Цифровая экономика Российской Федерации». Основными для нас направлениями здесь являются:

- ♦ информационная безопасность и киберустойчивость значимых платёжных систем (что включает использование российской криптографии);
- ♦ формирование подходов к киберустойчивости инновационных технологий;
- ♦ подготовка кадров для организаций кредитно-финансовой сферы.

КАДРЫ

Что касается четвёртого направления — подготовки кадров в сфере информационной безопасности, тут Банк России планирует стать связующим звеном между высшими учебными заведениями и организациями кредитно-финансовой сферы.

Это потребует от нас:

- ♦ определения потребности в специалистах;
- ♦ разработки профессионального стандарта «Специалист в области информационной безопасности организаций кредитно-финансовой сферы»;
- ♦ подготовки изменений в действующие образовательные ГОСТы;
- ♦ и разработки примерной программы профессиональной переподготовки для тех, кто уже окончил вуз.

Уверен, что все эти меры позволят создать условия для подготовки специалистов в области ИБ, которые действительно нужны рынку.

МЕЖДУНАРОДНОЕ ВЗАИМОДЕЙСТВИЕ

Наконец, пятое направление — международное взаимодействие.

Ключевыми площадками взаимодействия с зарубежными экспертами по вопросам кибербезопасности для Банка России являются:

- ♦ Международная организация по стандартизации (ISO);
- ♦ Международная электротехническая комиссия (IEC) и Международный союз электросвязи (ITU);
- ♦ Международная организация комиссий по ценным бумагам (IOSCO);
- ♦ Совет по финансовой стабильности (FSB);
- ♦ Всемирный экономический форум (WEF).

ФинЦЕРТ Банка России заключил соглашения по вопросам обмена информацией о киберугрозах и укрепления кибербезопасности с центральными либо национальными банками Италии, Испании, Турции, и Индии. Такие же соглашения действуют со всеми странами Евразийского Экономического союза.

Мы взаимодействуем с коллегами из ЕАЭС также по вопросам формирования центров реагирования на компьютерные инциденты, а также создания среды доверия в рамках единого платёжного пространства Союза. Впервые в мероприятиях Уральского форума в этом году принял участие представитель Народного банка Китайской Народной Республики.

**Артём СЫЧЁВ**первый заместитель директора
Департамента информационной
безопасности Банка России

РАСПОЗНАТЬ И ОБЕЗВРЕДИТЬ

АКТУАЛЬНЫЕ ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ «СОЦИАЛЬНОЙ ИНЖЕНЕРИИ» В СИСТЕМАХ ЭЛЕКТРОННЫХ ФИНАНСОВЫХ СЕРВИСОВ¹

Социальная инженерия, широко применяемая злоумышленниками для хищений средств в системах электронных платежей, сама по себе появилась не вчера. Мошенники всегда вводили в заблуждение людей для получения выгоды за их счёт. Обманутая жертва должна своими руками отдать злоумышленнику деньги, другие ценности, что-то сделать для него себе в ущерб. «Проделки хитрецов» описываются ещё в древних мифах и сказках, сложился целый жанр плутовского романа.

ВРАСПЛОХ, НАСПЕХ

Раньше мошенники действовали в реальном мире, лично контактируя с жертвами. В наше время к их услугам высокотехнологичные инструменты, дистанционное общение в виртуальном мире, мобильная связь и интернет. Многие граждане, пользующиеся электронными финансовыми сервисами, не задумываются, что туда могут вклиниться злоумышленники. Поэтому становятся жертвами уловок, на которые ни за что не купились бы при личной встрече в реальном мире.

Злоумышленники используют хорошо придуманные и отработанные техники дезинформации клиентов, позволяющие обманом путём дистанционно побудить перевести им деньги. «Социальные инженеры» атакуют неожиданно и стремительно, нагнетают обстановку и требуют немедленных действий. Злоумышленники застигают жертву врасплох, когда она не ожидает подвоха. Используя это временное преимущество, они спешат оказать психологическое давление.

Мошенники могут «пугать» возможной упущенной выгодой, делая акцент на том, что сроки «акции» заканчиваются. Напротив, могут и угрожать жертве мнимым ущербом, или тем, что помощь близкому человеку опоздает. Им важно вывести жертву из душевного равновесия, поставить в цейтнот. Чтобы та запаниковала, не стала тратить время на трезвую оценку ситуации и проверку информации, а скорее распростилась с деньгами.

ПРЕДУПРЕДИТЬ, ЧТОБЫ ВООРУЖИТЬ

Основная задача Банка России в противодействии «социальной инженерии» выглядит следующим образом. Это инициирование и стимулирование развёрнутой кампании информирования граждан об особенностях безопасного использования электронных финансовых сервисов. Не только о технических правилах безопасности, но и о том, как обезопасить себя от мошенников, «социальных инженеров». Чтобы граждане были начеку, знали, на что обращать внимание, как заподозрить неладное и проверить подозрительную информацию.

Эта важная и нужная работа будет усилена также финансовыми организациями, в первую очередь банками. Соответствующие требования Банком России уже установлены: информировать клиентов о рисках использования финансовых инструментов и мерах противодействия. Такое информирование в обязательном порядке должно быть доведено до каждого клиента.

Важное отличие «гуманитарных» атак на электронные платёжные средства от «технических» в том, что мишенью является пользователь, человек, а не то или иное техническое средство. Это мошенничество, а не кража со взломом.

¹ Статья подготовлена шеф-редактором BIS Journal П. Г. Былевским по материалам беседы с А. М. Сычёвым

Противодействовать «техническим» атакам сотрудники подразделений информационной безопасности банков могут самостоятельно, организационно-техническими мерами.

Для отражения атак «социальных инженеров» банкам потребуется настройка фронтального контура систем антифрода, определённое профилирование деятельности клиента. Но это не панацея, этого явно недостаточно: необходимо задействовать самого клиента. Научить его распознавать злоумышленников, не поддаваться на их уловки.

НАУЧИТЬ ОСТОРОЖНОСТИ

Общие рекомендации гражданам нужны, но сами по себе малоэффективны. Целесообразно профилировать аудиторию по группам. Злоумышленники так уже делают: для каждой группы у них есть свои подходы, техники, психологические приёмы, ключевые слова. К основным группам относятся: люди пожилого возраста, молодёжь — школьники и студенты, экономически активное население, предприниматели. В отношении молодёжи такую работу важно вести и для того, чтобы помешать её вовлечению в противоправную деятельность.

ФинЦЕРТ Банка России ведёт мониторинг и делает аналитику всех инцидентов, включая связанных с социальной инженерией. Обработывается отчётность финансовых организаций, обращения клиентов. На основании получаемых данных можно определить, какие социальные группы в какой степени подвергаются «гуманитарным» атакам, какими техниками оперируют злоумышленники, как часто добиваются успеха.

Отслеживается динамика: как появляются новые вредоносные техники, как постепенно сходят на нет, когда у граждан вырабатывается к ним «иммунитет». Банк России рассылает финансовым организациям, которые взаимодействуют с ФинЦЕРТом, оперативную информацию об актуальных угрозах со стороны злоумышленников. На этом основании можно специфицировать информирование разных групп клиентов о том, каких именно рисков, приёмов злоумышленников следует опасаться на текущий момент.

Более общая проблема в том, чтобы вообще научить клиентов осторожно, аккуратно пользоваться электронными инструментами на финансовых рынках. Это проблема не только клиентов, но и финансовых организаций, и отраслевого регулятора.

МИШЕНЯМИ СЛУЖАТ ВСЕ

В информировании населения приходится учитывать социально-психологические особенности разных групп, включая возрастные. Так, люди старшего поколения привыкли внимательно относиться к выступлениям официальных лиц, выполнять их рекомендации, в том числе к предупреждениям об опасностях, связанных с использованием электронных финансовых сервисов. Поэтому пенсионеры, которые первоначально были одной из главных мишеней мошенников, стали заметно осторожнее.

Злоумышленникам пришлось переносить «вектор главного удара» на экономически активное население. Эти изобретательные люди не сидят сложа руки. Не так давно они

выявили массовую проблему получения кредита людьми, которым нужны деньги. Для её «решения» сформировали новый криминальный «бизнес-продукт».

Рассылают якобы от имени кредитных организаций по электронной почте, посланиями в мессенджерах, SMS-сообщениями информацию о том, что «вам одобрен кредит на такую-то сумму». Но сначала надо перечислить комиссию за оформление или сделать первый регулярный платёж... Некоторые граждане спохватываются лишь тогда, когда перечислят злоумышленникам чуть ли не всю сумму, которую рассчитывали получить в кредит.

«ЖИЗНЕННЫЙ ЦИКЛ» УЛОВОК

Мошенники ведут мониторинг финансовой отрасли: новых продуктов, каналов и форм их доведения до граждан, следят за спросом, особенно за неудовлетворённым. Есть своеобразная аналогия с созданием и использованием технических решений, бизнес-продуктов.

В сфере электронных платежей набор криминальных схем регулярно обновляется. Разрабатывают, пробуют, сработает или нет, затем отработывают и продвигают всё новые и новые приёмы обмана. Запускают в «промышленную эксплуатацию». «Разработчики» используют мошеннические технологии и сами, и продают другим «коллегам», как отдельные инструменты и технологии, так и «коробочные решения».

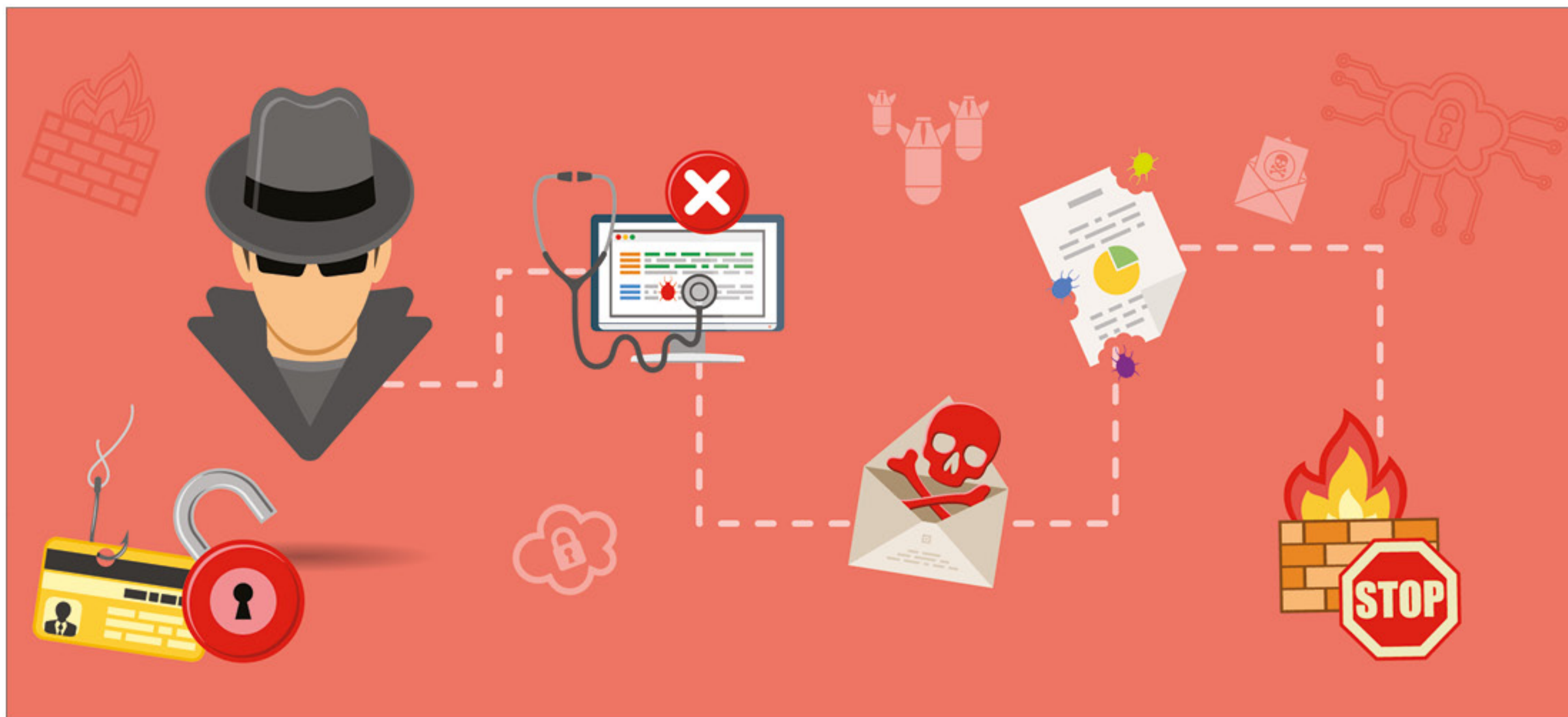
У «гуманитарных» мошеннических схем, как и у вирусов, бывает стадия начала использования, потом пик «эпидемии», и в итоге они постепенно сходят на нет, по мере выработки у граждан и организаций «иммунитета» к данной схеме. «Жизненный цикл» схем электронных преступлений в настоящее время составляет порядка трёх лет. Техники «социальной инженерии» могут трансформироваться намного быстрее.

ПОДМЕНА ТЕЛЕФОННОГО НОМЕРА

Одна из свежих криминальных новаций основана на открывшейся уязвимости определения номера входящего телефонного звонка. Делая звонок гражданину со своего номера, злоумышленники производят подмену на номер официального колл-центра, службы технической поддержки банка. Представляются сотрудниками банка и либо выведывают у клиента данные, позволяющие завладеть его деньгами, либо побуждают своими руками перечислить им свои средства. Техника эта показала эффективность, и всего за полгода её вывели на «промышленную эксплуатацию».

Совместно с банками, телеком-операторами и профильным ведомством, Минкомсвязи РФ, Банк России ищет решение этой проблемы, организационно-техническое и нормативно-правовое. Отдельный вопрос о номерах IP-телефонии. Межведомственное согласование — непростой процесс, хотя контакты налажены и взаимодействие ускорилось. Тем не менее, вопросы решаются не в одночасье: у каждого участника свой профиль, своя точка зрения, свой взгляд на проблему.

Чтобы защититься от этого вида мошенничества, гражданам нужно знать, какую информацию, необходимую мошенникам для хищений, настоящие сотрудники банков ни при



каких условиях не будут спрашивать: PIN-код, CVV-код, код из СМС. Клиентам, принимающим подозрительные звонки, рекомендуется для проверки перезванивать в банк по официальному номеру колл-центра, технической поддержки, указанному на банковской карте или сайте банка. Перезвонив по нему, попадаешь по нужному адресу, а не на скрытый номер, принадлежащий злоумышленникам. Недостаток в том, что это означает увеличение нагрузки на некоторые банки, у которых колл-центры не связаны со службами технической поддержки. Однако для клиента это самый действенный способ проверки.

ПРОВЕРЯТЬ ПОДОЗРЕНИЯ

Сейчас стоит вопрос о формировании базы данных подозрительных телефонных номеров. Это касается злоумышленников, которые не маскируют номера своих телефонов, занимаясь фишингом путём рассылки потенциальным жертвам сообщений и совершая голосовые звонки. Информация о таких телефонах могла бы поступать в банки от самих клиентов, и централизованно обрабатываться.

Однако речь не идёт о блокировке номеров. Это сложный вопрос и технически, и юридически. Нельзя, чтобы неудобства испытывали граждане, не причастные к деятельности злоумышленников, которые просто приобрели освободившийся «плохой» номер.

Есть аналогия с базой данных подозрительных банковских счетов, имеющих признаки использования в схемах хищений, которую ведёт ФинЦЕРТ Банка России. Подозрительные счета не блокируются, потому что признаки использования для мошенничеств — далеко ещё не юридические доказательства. Информация в базе ориентирует банки проявлять повышенную бдительность к операциям с этими счетами, проводить дополнительные процедуры проверки легальности.

Что касается возможной базы данных подозрительных телефонных номеров, то информация о её фигурантах мог-

ла бы автоматически выводиться на экраны смартфонов при подозрительном звонке или получении сообщения с сомнительной информацией, чтобы гражданин был своевременно предупреждён о потенциальной угрозе мошенничества и дальше действовал осмотрительно.

«ПОРТРЕТ» ЗЛОУМЫШЛЕННИКА

Аналитика ФинЦЕРТа позволяет составить «портрет» типичных злоумышленников. Сегодня это криминальные группы, члены которых могут быть рассредоточены по разным регионам страны, находиться за границей, быть знакомыми только дистанционно, под вымышленными никнеймами. Их обязанности и полномочия распределены: это организаторы, аналитики, разработчики инструментария и схем обмана, сотрудники фальшивых «колл-центров», создатели схем вывода похищенных средств и проводчики платежей, «нальщики».

Противостоять приходится не одиночкам, отдельным «социальным инженерам», а хорошо организованной преступности. Противодействие такому криминалу — общее дело и клиентов, и финансовых организаций, и государственных органов, включая правоохранительные.

Свежий пример — вынесение в начале 2019 года Мещанским судом Москвы обвинительного приговора группировке из 15 злоумышленников, обвинявшихся в хищениях у российских банков через социальные сети около 1 млрд рублей. Осудили их по ч. 1 ст. 210 (организация преступного сообщества) и по ч. 4 ст. 159.6 (мошенничество в сфере компьютерной информации) Уголовного Кодекса РФ. Члены группы получили сроки от 6,5 до 14 лет, а их главарь — 15 лет лишения свободы. Такая судьба ожидает и тех злоумышленников, которые пока на свободе, продолжают свою противозаконную деятельность.



**Георгий
ЛУНТОВСКИЙ**
президент
Ассоциации банков
России

РОСТ ЦИФРОВЫХ ТЕХНОЛОГИЙ ОПЕРЕЖАЕТ РЕГУЛИРОВАНИЕ

РАЗВИТИЕ КИБЕРФИНАНСОВОГО ПРОСТРАНСТВА: ВОЗМОЖНОСТИ И РИСКИ¹

ГЛАВНОЕ — ЗАЩИТА КЛИЕНТОВ

Сегодня мы обсуждаем кибербезопасность в цифровой экономике, ищем подходы к решению глобальных проблем, можем обменяться успешным опытом и наметить планы по повышению безопасности отечественной финансовой сферы. Ассоциация банков России разделяет всеобщую обеспокоенность этой темой, признаёт её важность и актуальность. Содействие внедрению цифровых технологий и информационная безопасность являются одними из приоритетных направлений деятельности Ассоциации. У нас активно работает Комитет по информационной безопасности, в рамках которого происходит обмен мнениями и опытом, выработка позиции Ассоциации по ключевым в этой сфере вопросам.

Колоссальные усилия в области обеспечения информационной безопасности предпринимает Банк России. Благодарю Дмитрия Германовича (Скобелкина — ред.) за понятные и актуальные задачи, которые регулятор поставил перед собой и кредитными организациями для повышения устойчивости и надёжности их работы. Необходимо помнить, что банкам надо, в первую очередь, защитить клиентов, физических и юридических лиц, а не просто формально исполнять нормативные требования. В этой связи приятно отметить, что на российском рынке, в том числе в нашей Ассоциации, есть банки, которые идут в ногу со временем, а порой даже опережают его, формируя новые направления в области кибербезопасности.

НЕПРОСТОЙ ПЕРИОД

При этом банковский сектор в последние годы переживает непростой период. Высокие риски, стагнация конкуренции, волатильность на рын-

ке, низкая рентабельность — всё это негативно сказывается на развитии бизнеса. Чтобы поддержать развитие банковской отрасли, важно обеспечить становление киберфинансового пространства, построение инфраструктуры цифровых финансов. Развитие цифровых технологий изменит конкурентную среду, будет способствовать повышению конкурентных возможностей кредитных организаций различной величины и формы собственности, откроет ранее недоступные для них ниши, создаст удобную и безопасную экосистему для клиентов и новые возможности для игроков на финансовом рынке.

НЕ ДОПУСТИТЬ МОНОПОЛИЗАЦИИ И ДИСКРИМИНАЦИИ

В текущих условиях особенно заинтересованы в уменьшении издержек банки с базовой лицензией. В то же время затраты на внедрение технологий непомерно велики для большинства банков. В силу этого технологические сервисы, скорее всего, будут запускаться на платформах крупных игроков. Важно не допустить монополизации киберфинансового пространства. И это должно стать одной из главных задач регулятора по поддержанию конкурентной среды.

Необходимо реализовать на практике систему мер по обеспечению недискриминационного доступа кредитных организаций к информации и открытым интерфейсам. Нужно продолжить работу, направленную на расширение состава и актуализацию сведений в Системе межведомственного электронного взаимодействия. Создать доступную для всех банков единую базу залогов и закладных, ускорить пилотный запуск концепции цифрового профиля, разработанную Ростелекомом.

При реализации технологичных программ и проектов, в которых задействован Банк

¹ Из доклада на XI Уральском форуме «Информационная безопасность финансовой сферы»

России, необходимо учитывать особенности банков с базовой лицензией, малых и региональных банков, углублять пропорциональное регулирование, находить и поддерживать реализацию облачных решений.

Так, по инициативе Ассоциации в Банке России, создана рабочая группа для проработки вопросов создания единой информационной платформы для содействия управлению кредитным риском. Банки, в том числе с базовой лицензией, нуждаются в централизованной базе, включающей информацию по заёмщикам Банка России, ФНС, ПФР и других источников. На первом этапе будет предоставляться информация для оценки финансового положения и расчёта минимальных резервов на возможные потери. Далее планируется размещать универсальные модели для оценки кредитного риска, одобренные Банком России. Их применение будет способствовать снижению издержек и даст возможность стандартизировать программное обеспечение.

ПЕРСПЕКТИВНОСТЬ REGTECH

Представители кредитных организаций отмечают перспективность технологии RegTech, в первую очередь, цифровизацию и стандартизацию взаимодействия с регулятором. Ассоциация выражает надежду, что обсуждение этой технологии будет продолжено в рамках формирования соответствующей дорожной карты.

ПРО БИОМЕТРИЮ

С запуском удалённой биометрической идентификации значительно выровнялись конкурентные условия на рынке. Однако низкие темпы наполнения базы биометрическими шаблонами не позволяют кредитным организациям с небольшой филиальной сетью полноценно воспользоваться всеми возможностями Единой биометрической системы. Необходимо активизировать сбор и передачу биометрии, разработать систему мотивации, рассмотреть вопрос о наделении полномочиями по сбору биометрических шаблонов многофункциональные центры (МФЦ).

О КИБЕРРИСКАХ

На фоне развития технологий, приносящих все больше удобства и пользы в жизнь клиентов, усиливаются и риски, связанные с их внедрением. Одним из ключевых становится киберриск. На протяжении последних нескольких лет наблюдается интенсивный рост киберпреступности во всём мире, мошеннические атаки приобретают всё более масштабный характер. Урон, который наносят

Необходимо находить решения, которые помогут малым и региональным банкам обеспечить безопасность своих клиентов при приемлемом уровне затрат

кибератаки мировой экономике, колоссален и оценивается свыше 1 трлн долларов. Ландшафт киберугроз с каждым днём становится разнообразнее и обширнее. При этом основной целью атак остаётся незаконное обогащение. Поэтому каждая вторая атака приходится на финансовый сектор. Так, в России за 2017 год у российских банков украли порядка 1 миллиарда рублей.

Ассоциация приветствует шаги, направленные на рост защищённости банковского сектора страны и клиентов кредитных организаций. При этом члены нашей Ассоциации, особенно небольшие банки, сообщают о неуклонном росте и ужесточении регуляторных требований по информационной безопасности. Их выполнение становится более сложной задачей, имеющиеся на рынке решения являются дорогими.

ПРО НЕБОЛЬШИЕ БАНКИ

В небольших кредитных организациях зачастую ограничены бюджеты на информационную безопасность. В некоторых регионах чувствуется нехватка специалистов высокой квалификации в сфере кибербезопасности. По оценкам, банки с базовой лицензией получают прибыль в среднем 5 млн руб. в год (по данным на 01.01.2019). На этом фоне ущерб от атаки может стать критическим для дальнейшей деятельности банка. Но и затраты на повышение уровня кибербезопасности непосильны для небольших банков. Это комплексная проблема, требующая дешёвых пакетных решений и введения ответственности для собственников и руководства за низкий уровень кибербезопасности.

Полагаем, что при подготовке Банком России документов, затрагивающих построение информационной безопасности, необходимо находить решения, которые помогут малым и региональным банкам обеспечить безопасность своих клиентов при приемлемом уровне затрат. Банку России следует активней дифференцировать требования к безопасности, так как риски, характерные для крупной финансовой организации, сильно отличаются от присущих небольшому банку. Регулятор может взять на себя

ведущую роль в повышении кибербезопасности банков и способствовать не только совершенствованию нормативной и методологической базы, но и осуществлять технические консультации, быть поставщиком информации о потенциальных киберугрозах, помогать банкам с выбором и внедрением средств защиты, инициировать процедуру возмещения налогов по инвестициям в информационную безопасность и т.п.

ПРО ЕДИНЫЙ СТАНДАРТ КИБЕРБЕЗОПАСНОСТИ

В частности, кредитные организации просят выстроить единый стандарт по кибербезопасности во всех реализуемых программах и проектах в рамках «Цифровой экономики». Это позволит банкам единожды закупить необходимое оборудование, обучить персонал и использовать их для целей обеспечения информационной безопасности всех проектов. Сейчас такого единого подхода не выработано, что несёт в себе риски дополнительных затрат по приобретению по сути дублирующего друг друга оборудования на разные проекты для соблюдения прописанных в них норм безопасности.

О СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И КИБЕРГРАМОТНОСТИ

Однако причиной уязвимости к атакам является не только слабая информационная безопасность, но и низкий уровень киберграмотности персонала и клиентов банка. По статистике, сейчас более 80 % успешных атак происходит с помощью методов социальной инженерии. Самым популярным методом сегодня являются фишинговые рассылки. По информации экспертов, около 18 % сотрудников переходят по ссылкам из фишингового письма, и примерно 9 % вводят учётные данные на сайте. Другой эффективный метод — вишинг или телефонный фишинг. Телефонный звонок, как правило, вызывает большее доверие, чем электронная почта, поэтому результативность голосовых атак на 20 % выше, чем при фишинговой рассылке.

Единственным продуктивным способом противостояния кибермошенникам является повышение киберграмотности сотрудников и клиентов кредитной организации. Для этих целей Банк России может формировать и реализовывать обучающие программы, подготавливать методологические рекомендации по организации процесса повышения их осведомлённости. Не следует также пренебрегать программными решениями, способными снизить риск утечки информации и последующей атаки.

ПЛАТФОРМА ОБМЕНА ДАННЫМИ

Рост кибербпреступлений обеспечивается эффективной и оперативной работой группировок мошенников, опережающей на шаг реакцию мирового сообщества. Признавая необходимость консолидации в вопросе информационной безопасности, Ассоциация банков России запустила платформу обмена данными. Платформа позволяет участникам автоматически в режиме on-line получать верифицированную и релевантную информацию. Преимуществами платформы является агрегация источников данных об угрозах (ФинЦЕРТ Банка России, операторы связи, BI.ZONE), выгрузка только полезной информации для защиты банка и автоматизация процесса применения этой информации. Функционал платформы может быть использован даже в небольших банках.

По итогам пилотирования в проект вовлечено 36 организаций, из них 29 — банки из 11 регионов России, их общая доля в активах банковской системы превышает 50 %. С 2019 года платформа запущена в промышленную эксплуатацию, расширен её функционал и дополнены источники данных.

КИБЕРБЕЗОПАСНОСТЬ КАК ОБЩЕСТВЕННОЕ БЛАГО

В завершение хочу отметить, что в условиях развития цифровых технологий, перехода к цифровой экономике, актуальность вопросов обеспечения информационной безопасности сложно переоценить. Риски, связанные с ростом киберугроз, требуют оперативного и своевременного мониторинга, обнаружения и эффективного реагирования. На наш взгляд, сфера кибербезопасности в банковской системе должна стать областью объединения усилий, своеобразным «общественным благом», которое создаётся с помощью компетентных структур и потребляется в равной степени всеми участниками рынка.

* * *

Развитие цифровых технологий опережает регулирование, поэтому работы предстоит много: и законодателям, и регулятору, и банкам. Предстоит как разработать «с нуля», так и доработать много законодательных и нормативных актов, которые позволят реализовать намеченные планы. При этом важно обеспечить надлежащую степень их предварительной проработки, высокий уровень экспертизы, активно привлекать банки к обсуждению всех инициатив.

У БАНКОВ ЕСТЬ И ПОТРЕБНОСТИ

В АССОЦИАЦИИ «РОССИЯ»
ПРОАНАЛИЗИРОВАЛИ ПРИОРИТЕТНЫЕ
ПРОЕКТЫ REGTECH И SUPTECH
НА РОССИЙСКОМ ФИНАНСОВОМ РЫНКЕ¹



**Алексей
ВОЙЛУКОВ**
вице-президент
Ассоциации банков
России

В прошлом году Банк России опубликовал для публичной дискуссии консультативный доклад «Вопросы и направления развития регуляторных и надзорных технологий (RegTech и SupTech) на финансовом рынке в России». Ассоциация «Россия» организовала обсуждение документа путем проведения опроса кредитных организаций, а затем в рамках совместных заседаний профильных Комитетов.

БЕДА ОТЧЕТНОСТИ

Проведение опроса сразу обозначило тему, которая много лет не сходит с повестки дня и с которой связаны основные надежды кредитных организаций, как только разговор заходит о внедрении в Банке России современных информационных технологий. Это проблема сокращения объема отчетности, направляемой регулятору. Заполнение в прошлом году 111-й формы (0409111) с результатами выполнения требований Банка России по ВПОДК оставило неизгладимое впечатление для всех сотрудников профильных подразделений кредитных организаций.

Крупные кредитные организации помимо большого объема отчетности отмечают, что программные комплексы, используемые Банком России для ее сбора, устарели и уже с трудом встраиваются в существующий процесс автоматизации, а частые изменения отчетных форм заставляют привлекать дополнительных специалистов, поскольку их реализация «на коленке» штатными средствами (типа таблиц в Excel) целесообразнее с экономической точки зрения, чем реальная автоматизация сбора отчетности. Для банков с базовой лицензией данное направление работы стало практически основным. Ярким примером является ситу-

ация, когда достаточно активно действующий банк с базовой лицензией имеет трех сотрудников в кредитном подразделении и 15 специалистов, занятых подготовкой отчетности для регулятора.

БАНКИ ЖДУТ ДРУГОГО

В Докладе приведены международные примеры применения технологий RegTech и SupTech, и такое стремление алгоритмизировать процессы взаимодействия регулятора и кредитных организаций может только приветствоваться банковским сообществом. Однако в части инициатив и проектов по внедрению Банк России описал, в основном, технологии SupTech, направленные на повышение эффективности надзора, в то время как для банков в первую очередь интересны технологии RegTech, в целях повышения эффективности и сокращения издержек. При этом важно сосредоточиться на проектах, которые дадут ощутимый результат от их реализации в короткие сроки.

НАШИ ПРЕДЛОЖЕНИЯ БАНКУ РОССИИ

По результатам обсуждения в Ассоциации ее участниками были сформированы следующие предложения для Банка России.

1. В целях обеспечения прозрачности учета сделок по оформлению залогов и выдаче

Ярким примером является ситуация, когда достаточно активно действующий банк с базовой лицензией имеет трех сотрудников в кредитном подразделении и 15 специалистов, занятых подготовкой отчетности для регулятора

¹ Из доклада на XI Уральском форуме «Информационная безопасность финансовой сферы»



закладных, ускорения принятия кредитными организациями решения о проведении соответствующих сделок, снижения мошенничества, возможности осуществления Банком России контроля за указанными сделками без излишних обращений в кредитные организации — создать реестр залогов и закладных для регулятора и участников финансового рынка. Ассоциация уже вовлечена в работу по этому проекту, и мы надеемся на его успешную реализацию уже в этом году.

2. В отношении автоматизации расчета нормативов с помощью ПО КЛИКО, указанной в качестве одной из областей применения технологий RegTech, представляется, что полномасштабная реализация в короткие сроки может быть затруднена, и в этом смысле не должна быть первоочередной ввиду необходимости внесения изменений в нормативные акты Банка России, которые позволят создать алгоритм для заполнения форм, исключая мотивированное суждение банков и сделают такой расчет «прозрачным», а значит снизят регуляторные риски.

Тем не менее необходимо рассмотреть направления развития/замены ПО КЛИКО в сторону технологий на базе Open-API, минимизировав влияние ПО в части пользовательского интерфейса на процесс заполнения, проверки корректности и передачи данных.

3. Разработать буферную базу первичных данных, необходимых для осуществления Банком России надзора за кредитными организациями, наполнение которой будет осуществляться кредитными организациями по единым принципам и стандартам. В указанной базе для Банка России будет доступна информация, на основании которой он сможет формировать необходимую отчетность. В этом направлении похожая система реализована в 2014 году в Австрии, где семь крупнейших банковских групп учредили консорциум AuRep, в рамках которого была создана единая модель данных и общая информационная система для формирования как управленческой, так и регуляторной отчетности.

О БАЗЕ ДАННЫХ ПО ЗАЕМЩИКАМ

Не могу не отметить и то, что уже неплохими темпами начал развиваться еще один проект, который тоже можно отнести к сфере RegTech. По инициативе Ассоциации в Банке России сформирована рабочая группа для проработки вопросов создания единой информационной платформы для содействия управления кредитным риском. В рамках рабочей группы признано, что банки нуждаются в централизованной базе данных по заемщикам, которая включала бы в себя информацию, имеющуюся в Банке России, а в перспективе налоговую, пенсионную и иную информацию.

На первом этапе рассматривается возможность предоставления первичной информации о заемщиках, включая стоп-факторы и транзакционную информацию, имеющуюся в Банке России. Далее возможности платформы предполагается расширять, как за счет дополнительной информации из иных государственных органов, так и возможном размещении на платформе универсальных моделей для оценки кредитного риска, одобренных Банком России. Применение универсальных моделей будет способствовать снижению издержек (в первую очередь для небольших банков). При этом, исходя из большого объема информации, имеющегося в Банке России, становится возможной объективная оценка надежности клиента и формирование адекватных резервов на возможные потери.

REGTECH В СФЕРЕ ИБ

К важным проектам в сфере RegTech мы относим и проекты, связанные с защитой информации. Для нас таким «общественным» RegTech является платформа обмена данными о киберугрозах, запущенная Ассоциацией при технической поддержке компании BI.ZONE. Платформа предоставляет сервис доверенного обмена информацией об актуальных киберугрозах внутри финансовой отрасли и позволяет участникам автоматически получать верифицированную и релевантную информацию об индикаторах компрометации.

Преимуществами платформы является агрегация различных источников данных об угрозах (банков, операторов связи, ФинЦЕРТ Банка России), включая превентивную информацию о возможных, но не реализованных на рынке угрозах, выгрузка только полезной информации для защиты кредитных организаций и автоматизация процесса применения информации о киберугрозах в системах защиты банков на основе API.

ОТ ПРОЕКТОВ SUPTECH К ПРОЕКТАМ REGTECH

Участие в проектах в сфере SupTech, как мы все понимаем, для нас неизбежно, но не оставляем надежды, что их успешная реализация может облегчить жизнь не только Банку России, но и кредитным организациям, т.к. в дальнейшем на их базе могут вырасти проекты в сфере RegTech.

1. Одним из таких проектов является графовый анализ взаимосвязанности юридических лиц. Хотелось бы надеяться, что результатами его реализации удастся воспользоваться и кредитным организациям, например, в рамках инфор-

Проект «Сбор и анализ детальных данных операционного дня банка» можно рассматривать как шаг к дата-центричному подходу в сборе информации о деятельности кредитных организаций

мационной платформы для содействия управлению кредитным риском.

2. Цифровизация регуляторных требований (так называемое машиночитаемое регулирование). Данная инициатива видится крайне желательной, поскольку позволит повысить прозрачность и алгоритмичность регулирования, минимизировать риски различной интерпретации положений нормативных актов различными банками и проверяющими. Кроме того, данный шаг является необходимым условием успешного внедрения по сути любой другой инициативы SupTech.

3. Проект «Сбор и анализ детальных данных операционного дня банка» можно рассматривать как шаг к дата-центричному подходу в сборе информации о деятельности кредитных организаций. Указано, что переход на обязательное ежедневное предоставление опердней всеми банками ожидается в конце этого года. Надеемся, что это будет шаг в правильном направлении.

НЕ ВСЕ ОДНОЗНАЧНО

Вместе с тем в документе однозначно не определено, планирует ли Банк России в дальнейшем реализовывать следующие шаги к дата-центричному подходу формирования отчетности кредитными организациями. Принимая во внимание состав информации, находящейся в опердне, банки полагают, что ожидаемого снижения нагрузки на данном этапе не произойдет, поскольку на основе только сведений опердня невозможно сформировать большинство форм отчетности.

* * *

В завершение хочу еще раз подчеркнуть: безусловно, нам интересны направления, предложенные в Докладе, но давайте сначала попробуем в относительно короткие сроки — год-полтора — реализовать озвученные проекты. Сверяя свои ожидания от их реализации с реальным повышением эффективности и сокращением издержек для банков. А затем подумаем о расширении количества проектов, которые хотелось бы реализовать.



Денис АНТОНОВ
начальник отдела
информационной
безопасности
КБ «Банк Союз»

ПАСЫНКИ СИСТЕМЫ

РЕАЛИИ СЛУЖБ ИБ «МАЛЫХ И СРЕДНИХ» БАНКОВ В УСЛОВИЯХ УЖЕСТОЧЕНИЯ ЗАКОНОДАТЕЛЬСТВА

О том, какая славная информационная безопасность в «большой пятёрке», мы слышим часто и практически отовсюду. Но мы живём в мире, где кроме «большой пятёрки» есть ещё около 300 банков, существующих в других реалиях.

ЦИТАТА ИЗ ГОСТА И ДВА ПРОЦЕССА

Начнём с цитаты из ГОСТ Р 57580.1–2017: «...для финансовых организаций угрозы безопасности информации представляют существенную опасность, а обеспечение защиты информации является для финансовых организаций одним из основополагающих аспектов их деятельности».

Что происходит в реальности в «малых и средних» банках? Как бизнес воспринимает фразу «обеспечение защиты информации является для финансовых организаций одним из основополагающих аспектов их деятельности»? Чтобы понять, рассмотрим всего пару процессов — мониторинга фродовых операций и проведение внешнего аудита по 382-П.

МОНИТОРИНГ ФРОДА

Мониторинг фрода — одно из направлений информационной безопасности, с необходимостью которого бизнес соглашается, но при этом совершенно не понимает, зачем нужна автоматизация процесса, если всё можно сделать «руками». И финансировать внедрение Анти-фрод системы бизнес не спешит.

Пока Анти-фрод «семимильными шагами» проносится по просторам банковского сообщества, усиливая свои позиции изменениями в законодательстве (167-ФЗ от 27.06.2018), подразделения ИБ продолжают «околачивать» пороги бизнеса, в очередной раз объясняя необходимость внедрения Анти-фрод системы. Как правило, в «малых и средних» банках ответственность за обеспечение ИБ (в полном объёме) возлагается всего на одного-двух сотрудников.

Так происходит потому, что владельцы «малых и средних» банков оплачивают содержание подразделения ИБ из собственного кармана, а не за счёт государственной поддержки, и согласование бюджета на дополнительного сотрудника — это боль. Следовательно, ни о каком усилении служб ИБ квалифицированными специалистами речи не идёт. Да и на повышение квалификации имеющихся сотрудников за счёт банка рассчитывать не приходится. По этой причине теми же сотрудниками осуществляется и выполнение требований в части противодействия хищению денежных средств «подручными» средствами.

Банковский антифрод — молодая профессия, которая не преподаётся в вузах даже минимально. И основные инструменты для этих Анти-фрод систем мы обычно берём из трёх «источников»:

- ♦ аудит — даёт нам различные инструменты ревизий, сплошных и выборочных проверок, инспектирования и т.д.;
- ♦ криминалистика — содержит богатый инструментарий для выявления мошенничества;
- ♦ аналитика — позволяет использовать математический аппарат для разработки антифрод-инструментов и оценки их эффективности.

Банковский «средний и малый» бизнес идёт другим путём, формируя менеджмент ИБ из одного-двух человек, и, как правило, ожидает, что эти «полтора» специалиста закроют ВСЕ дыры в рисках информационной безопасности бизнеса. Что получается?

Из года в год со стороны Регулятора идёт ужесточение требований к информационной безопасности. Безусловно, это не прихоть — таковы реалии современного мира. Государству приходится повышать защищённость банков, так как банковский сектор — это кровеносная система страны, и её нужно защищать и содержать в оптимальном состоянии. Это мы понимаем.



Но вот вопрос: правильно ли выбрана методика наведения порядка? Да, она вполне подходит банкам с господдержкой, которым набрать штат для службы ИБ, обучить сотрудников, выделить дополнительное финансирование, утвердить бюджет на защиту инфраструктуры намного проще, чем их «малым и средним» братьям. А что делать этим самым «малым и средним»? Так и хочется назвать их пасынками финансовой сферы!

Всё чаще и чаще слышу от менеджеров ИБ «малых и средних» банков, что регулятор не торопится работать с бизнесом, что безопасники постоянно сталкиваются с непониманием, доказывая руководству необходимость той или иной системы, риски от невнедрения которой очень высоки.

ПРО 382-П

Теперь про внешний аудит по 382-П. Сама идея независимого аудита безусловно полезна, такой аудит объективно показывает уязвимости внутри инфраструктуры, которые штатные безопасники порой заметить не могут. Но вот вопрос регулятору: кто несёт ответственность за этот внешний аудит или за тот же пен-тест? И другой вопрос, который хочется дважды подчеркнуть: почему нет аккредитации организаций на проведение этого вида работ?

Получается, раз вышли изменения в законодательстве, и оценка ИБ поменяла вектор

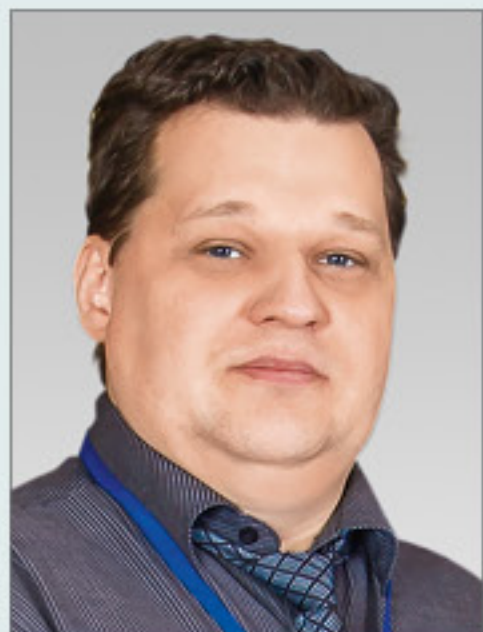
в правильном направлении, то теперь бизнесу выгоднее нанять для определённого вида работ компанию, компетентность которой подтверждена лицензией. И это хорошо. Но вот парадокс: таких подрядчиков становится всё больше и больше, а вот их компетентность и профессионализм ничем не подтверждаются.

В итоге менеджмент ИБ постоянно борется с ветряными мельницами, доказывая бизнесу и свою состоятельность, и адекватность требований тех же регуляторов. А хотелось бы, чтобы бизнес выступал в роли заказчика по отношению к менеджменту информационной безопасности.

И тут возникает следующий вопрос: как быть в такой ситуации менеджменту ИБ «малых и средних» банков? Тут, как мне кажется, нужна как раз помощь со стороны регуляторов. Необходимо их активное участие по взаимодействию с бизнесом. Это могут быть ежегодные форумы, конференции на площадках регуляторов и т.д.

* * *

Такие форумы и конференции в формате «Бизнес–Регулятор» позволят упростить взаимодействие между бизнесом и подразделениями ИБ и, соответственно, сократить временные и другие издержки при принятии решений в сфере ИБ.



Александр ВИНОГРАДОВ
эксперт ИБ

Проблема действительно существует. Но по порядку:

1. На текущий момент развитие ИБ в банках идёт семимильными шагами. Каждый год регулятор выпускает документы, и выполнять их надо. А куда деваться? То ГОСТ, то биометрия, то что-то другое. И всё это ложиться на плечи менеджмента ИБ.

Возьмём самый вопиющий пример. После упоминания в СТО БР пункта по Плану ОНВД многие банки спихнули эту проверку на менеджмент ИБ. И это выглядит смешно и грустно, когда один-единственный сотрудник ИБ бежит по банку и организует проверку пожарной безопасности, угрозы взрыва или затопления от прорвавшейся трубы отопления. А ему это надо? У него и так работы выше крыши!

2. Бизнес не понимает, что требования 382-П, 552-П, СТО БР и др. не предполагает 100 % выполнения исключительно подразделениями ИБ. В этом процессе должен участвовать весь банк, а не один человек с «богатой фантазией». Донести эту мысль до руководства бывает очень трудно.

Например, есть в банке Антифрод система. И не всегда удаётся объяснить, что в этой системе должны быть заде-

ствованы и ОПЕРУ, и клиентчики, и другие подразделения. Ведь не сотрудник ИБ должен звонить клиенту и спрашивать о легитимности его платежа!

3. Самое больное — аудит. Несколько лет назад, в основном перед сдачей самооценки по СТО БР, во всех банках звонили телефоны: «Вам помочь? У нас богатый опыт!» И хотя эти любезные фирмы никто на рынке не знал, услугами их пользовались. Потом сильно жалели. Но это было давно.

Что изменилось? Сегодня такая фирма должна иметь лицензию ТЗКИ. Чтобы её получить, требуется вложить немало средств и доказать свою компетентность. Но шарлатаны и тут не растерялись. Находят фирму с лицензией, и под её вывеской творят свои тёмные дела.

Кроме того, мало кто из работников ИБ понимает, что теперь аудит надо проводить не только для платёжной системы Банка России, но и для всех платёжных систем. Благо одно. ФинЦЕРТ стал запрашивать отчёты. Показывая тем самым, что есть недостатки. Спасибо им.

Вывод следующий: сегодня менеджмент ИБ малых и средних банков поставлен перед непростым выбором: либо аудит за меньшие деньги и соответственно с меньшим качеством... Либо у фирмы-шарлатана с лицензией, где всю работу выполняют студенты, и тут о качестве вообще говорить не приходится... Либо у фирмы, которая сделает свою работу квалифицированно и компетентно, и показать отчёт будет не стыдно.

Выбор за Вами.

BIS-КОММЕНТАРИЙ



Василий ОКУЛЕСКИЙ
заместитель начальника Службы
информационной безопасности
Банка «Возрождение», кандидат
технических наук

Статью «Пасынки системы» можно было бы назвать «Два банка — два мира — две судьбы». Не статья, а крик души. Готов почти согласиться с ней. Хотя, на самом деле, таких миров гораздо больше, а главное, что эти миры напрямую никак не зависят от размеров банка, хотя определённая косвенная корреляция усматривается.

Основное различие банков — в восприятии и возможности реализации требований регуляторов, а их, регуляторов, гарантированно более одного. Если постараться внимательно и подробно изучить применимость требований,

то получится довольно прозрачная картинка: уровень зрелости системы управления организации, в данном случае банка, определяет возможность исполнения требований, а главное — какие последствия для банка принесут результаты этих действий. Уровень зрелости организации в целом определяет и уровень зрелости системы управления информационной безопасностью (для простоты рассмотрения будем ставить тождество между системой управления и системой менеджмента, и не будем учитывать «тонкие семантические различия»).

Методологически ситуация с системами менеджмента информационной безопасности (СМИБ) очень схожа с системами менеджмента качества (СМК). Особенно в части ответственности руководства организации за результаты деятельности СМИБ или СМК. Рассмотрим, как ответственность руководства выглядит в структуре процессов СМК, которые я попытался привязать к циклу PDCA, и вот что получается (Диаграмма 1).

BIS-КОММЕНТАРИЙ

А теперь приложите эту диаграмму к СМИБ. Нужно просто *поменять* СМК на СМИБ. И всё. Мне довелось пожить в обеих системах, и поэтому могу, основываясь на этом опыте, сказать, что для различных уровней зрелости результаты внедрения систем менеджмента будут разные. Статистика результатов внедрения СМК отражена на Диаграмме 2.

Только начиная с третьего уровня зрелости организации, выполнение требований регуляторов начинает приносить не «бумажную», а реальную пользу. Можно ли построить СМИБ 3–4 уровня в организации 2 уровня зрелости?

Можно! Но в этом случае ИБ должна стать локомотивом для всей системы управления/менеджмента банка в целом. Это сложно, трудно, но *можно*! Есть примеры? Конечно. Оборонная промышленность всегда тянула за собой развитие остальных отраслей промышленности.

Неявный пример? Отнюдь. В информационной безопасности исторически применяются самые передовые технологии, она постоянно наступает на пятки и трёт мозоли информационным технологиям, хотя и не всегда они дружат. Зато там, где дружба сложилась, ИТ и ИБ вытаскивают бизнес на новые уровни развития и управления. Попробуйте привести примеры сами, из своей практики. При этом помните, что исключения лишь подчёркивают правило.

Что из всего этого следует?

В первую очередь надо *хотеть* и *искать* пути, а не тихонько плакать в жилетку и жаловаться, что вас никто не понимает и «молча гибнуть я должна». Выходить на первых лиц и объяснять-объяснять-объяснять тесную связь результатов бизнеса и активным внедрением ИБ. ИБ должна стать основой *безопасности бизнеса*, его главным конкурентным преимуществом и способом удержания рынка, и, наконец, способом повышения финансовой эффективности.

И вот здесь роль нашего уважаемого Регулятора становится ключевой —

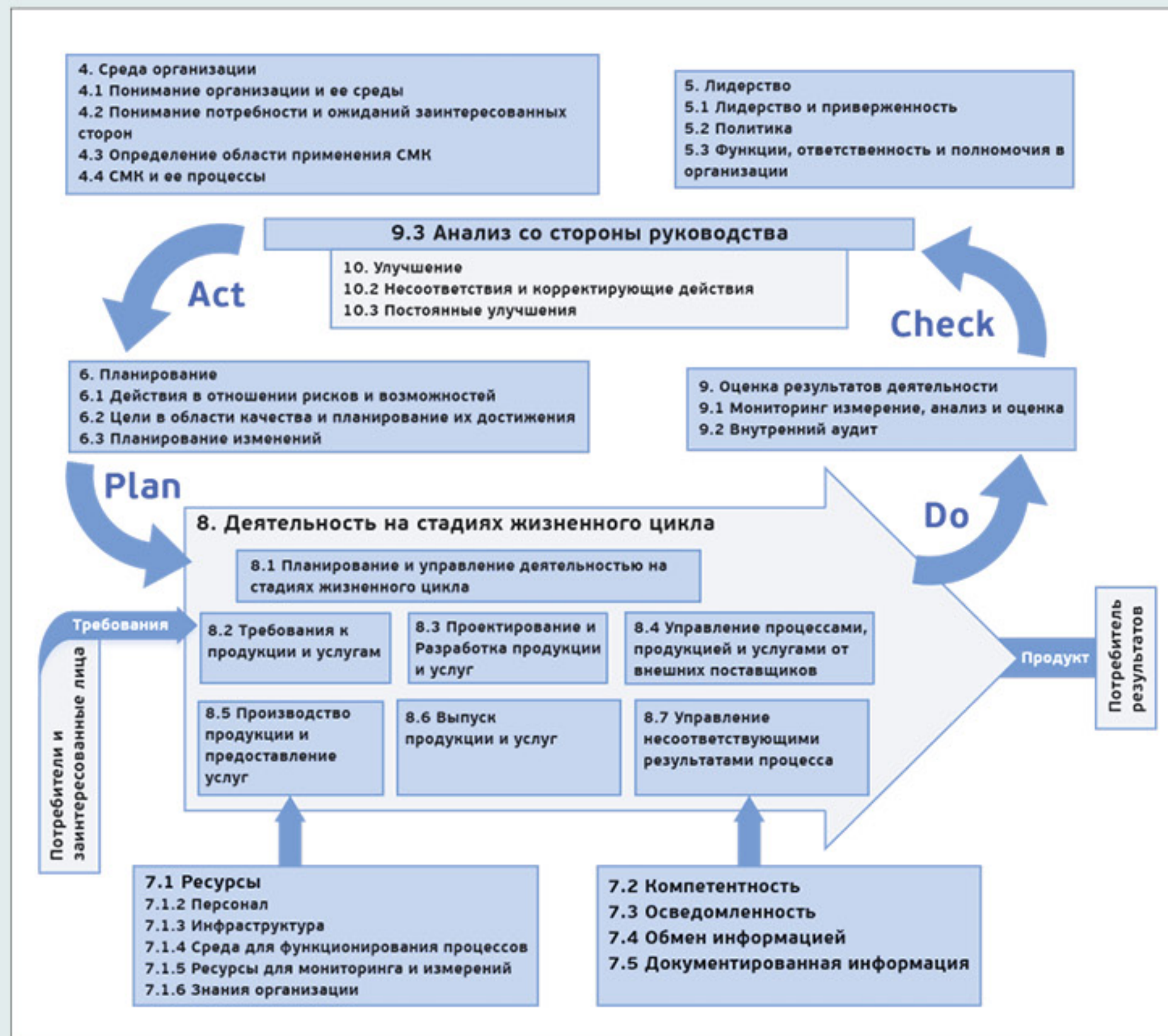


Диаграмма 1. Структура процессов ответственности руководства организации

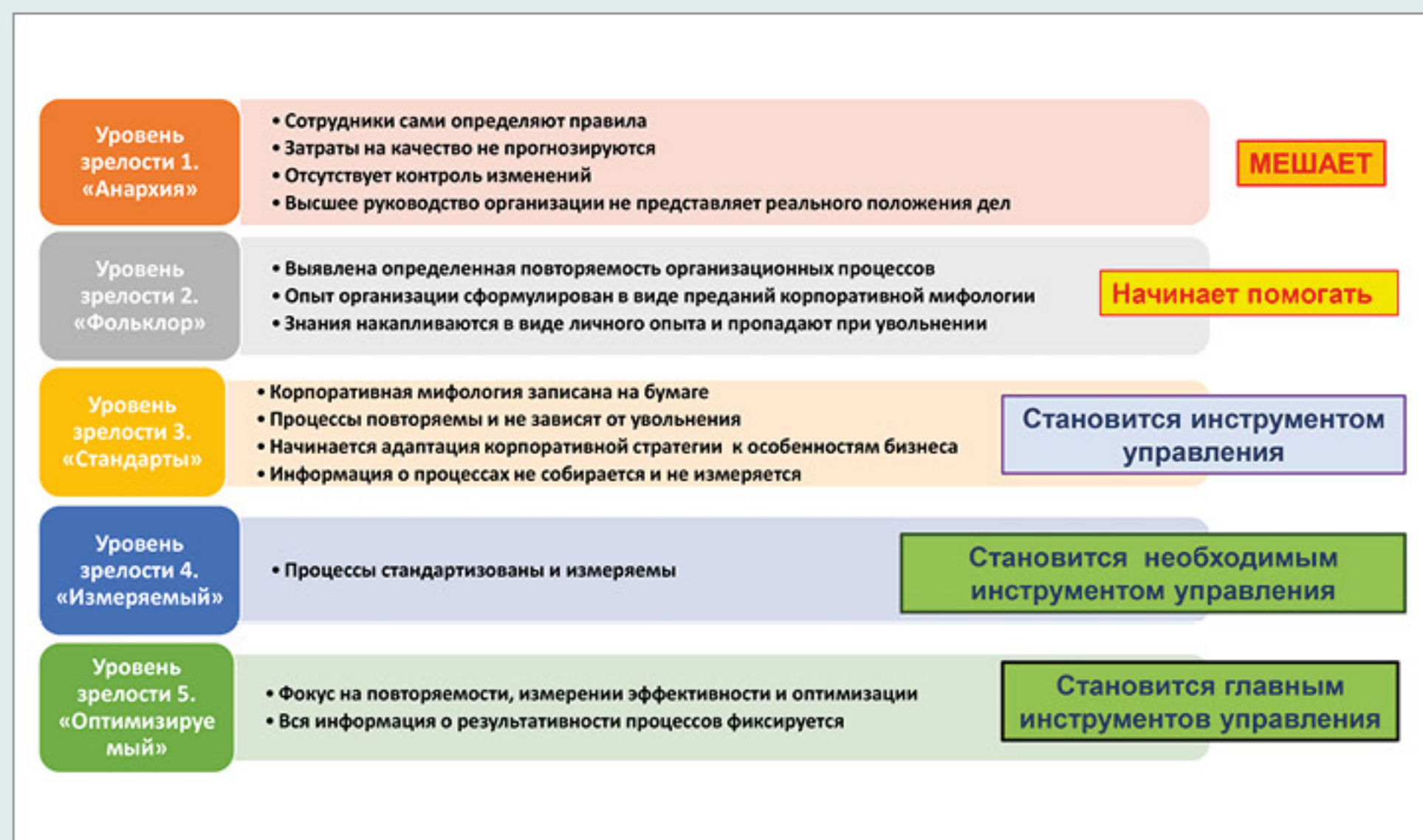


Диаграмма 2. «Полезность» результатов внедрения в зависимости от уровня зрелости

необходимо не только декларативно создать условия для этой связки (в виде нормативных требований), но и обеспечить перестройку мышления руководителей и собственников банков, что без развития информационной безопас-

ности до уровня зрелости не ниже четвертого им счастья в жизни не будет. А для такой работы у Регулятора есть всё необходимое.

Дело (а не только требования и надзор за их исполнением) за Регулятором.



Татьяна ЖАРКОВА
управляющий
директор
Ассоциации ФинТех

БАНКИ НА ВОЛНЕ ФИНТЕХА

ДРАЙВЕРЫ ЦИФРОВОЙ ЭКОНОМИКИ.
СТАТИСТИКА И ПРОГНОЗЫ

По оценке консалтинговой компании McKinsey, к 2025 г. цифровая экономика (ЦЭ) России способна обеспечить до 34 % роста ВВП страны, тем самым увеличив его объём на 4,1–8,9 трлн рублей. В соответствии с данным прогнозом, доля ЦЭ в ВВП может вырасти в три раза. Однако сегодня на ЦЭ в нашей стране приходится лишь 3,9 % от ВВП страны, что примерно в 2–3 раза ниже аналогичных показателей США, Китая и ЕС. По уровню цифровизации экономики Россия более, чем в 2 раза отстаёт от мировых лидеров — Дании, Швеции и Южной Кореи.

Несмотря на нынешние позиции в рейтинге, прогнозы по развитию ЦЭ РФ весьма положительные. В период с 2011 по 2015 гг. её совокупный объём увеличился на 59 % и достиг уровня 1,2 трлн рублей, в 10 раз опережая прирост ВВП страны. Главным драйвером здесь выступили финансовые технологии.

Пользователи финтех-услуг стали более требовательными к их качеству и скорости. По результатам опроса, 58 % клиентов европейских финансовых структур предпочитают банки, предлагающие современные технологии обслуживания, а 46 % готовы воспользоваться сервисами альтернативного банкинга. Схожую модель поведения демонстрируют и клиенты отечественных финансовых организаций. У России также есть отличная возможность избежать ошибок стран-пионеров и внедрять лучшие практики и эффективные платформы.

Лидером по внедрению цифровых технологий в нашей стране является банковский сектор, на долю которого приходится свыше 90 % инвестиций в области финтеха (75 млн долл. в 2011–2016 гг. по данным CBInsights). В связи с этим

Банк России уделяет большое внимание развитию конкуренции в финансовой отрасли, активно поддерживая проекты по созданию цифровой инфраструктуры. При этом основной упор делается на доступность и качество финансовых продуктов и услуг.

ПРЕДПОСЫЛКИ ДЛЯ НОВЫХ ФИНАНСОВЫХ ТЕХНОЛОГИЙ

По размеру интернет-аудитории Россия занимает 1-е место в Европе и 6-е в мире — 87 млн пользователей Интернета и не менее 67 млн абонентов мобильной связи. По данным ЦБ РФ, 45,1 % клиентов банков являются пользователями мобильного или интернет-банкинга. Это провоцирует повышенный спрос на электронные услуги, прежде всего, в сфере платежей, переводов и кредитования. Также на развитие цифровых сервисов влияет неравномерное распределение по территории страны представительств финансовых институтов. Зачастую клиенты банков нуждаются в дистанционном обслуживании. Это стало предпосылкой для появления нового механизма предоставления финансовых услуг — удалённой идентификации.

Летом 2018 г. была запущена Единая биометрическая система (ЕБС), ставшая одним из основных элементов удалённой идентификации. Ассоциация ФинТех (АФТ) совместно с нашими участниками предложила поправки в законодательство, направленные на урегулирование взаимодействия банков и клиентов в области цифровой идентификации. Теперь, сдав свои биометрические данные (запись голоса и динамическое изображение лица), потребитель сможет дистанционно получать услуги различных банков: открывать счета и управлять ими, получать кредиты. В будущем перечень предлагаемых продуктов планируется расширить.

Активный рост P2P платежей в прошедшие три года повлиял на создание ещё одного масштабного отечественного финтех-проекта — Системы быстрых платежей (СБП). В 2017 г. общая сумма по транзакциям достигла 19 трлн руб., что на 77 % выше аналогично-

У России также есть отличная возможность избежать ошибок стран-пионеров и внедрять лучшие практики и эффективные платформы

го показателя 2016 г. В АФТ проанализировали опыт более чем 20 стран в области Faster Payment Systems. И в 2018 году АФТ, Банк России и НСПК (Национальная Система Платёжных карт) совместно с ключевыми участниками финансового рынка разработали концепцию СБП и подходы к её внедрению. Мы учли лучший опыт таких передовых в этой области стран, как Швеция и Сингапур.

СБП позволит моментально проводить транзакции между счётами в любых банках в режиме 24/7/365, в том числе, осуществлять переводы с карты на карту и проводить моментальную оплату покупок. Предусмотрен доступный идентификатор — быстрые переводы между банковскими структурами будут осуществляться по номеру телефона.

Важнейшим проектом Ассоциации ФинТех, который реализуется совместно с Банком России и ключевыми участниками финансового рынка, является Мастерчейн. Это блокчейн-платформа, созданная на базе модификации протокола Ethereum. Эксперты Ассоциации адаптировали его в соответствии с требованиями российского законодательства по защите информации. В этом и состоит уникальная особенность платформы. Документы, зарегистрированные на Мастерчейне и подписанные электронной подписью, будут иметь такую же юридическую силу, что и бумажные. Российский блокчейн позволит ускорить и существенно оптимизировать банковские бизнес-процессы. На Мастерчейне разработаны три проекта: учет электронных закладных, цифровые банковские гарантии и цифровой аккредитив. В 2018 г. уже были успешно проведены первые пилотные сделки по электронным закладным и цифровым банковским гарантиям.

Сейчас Мастерчейн проходит сертификацию ФСБ в соответствии с требованиями к средствам криптографической защиты информации. Дополнительную гарантию безопасности дают механизмы контроля доступа в сеть. Работать на платформе смогут исключительно подтверждённые пользователи. Взаимодействие между участниками закрытой сети осуществляется благодаря применению технологии распределённых реестров.

Полным ходом идёт работа по созданию нормативно-правовой базы для использования в России открытых интерфейсов программирования (открытые API). API — это набор технологических протоколов, позволяющий различным информационным системам взаимодействовать между собой. Это технологическое решение откроет новые возможности,

Клиенты банков получают возможность раскрывать информацию о себе другим участникам финансового рынка, при этом не нарушая действующие законы по защите персональных данных

в первую очередь, для клиентов банков. Они получают доступ к широкому перечню услуг, например, по открытию и использованию мультивалютных счетов. В настоящее время на площадке Ассоциации ФинТех разрабатывается концепция внедрения открытых API.

У нас есть возможность учесть ошибки и достижения стран, где открытые API уже активно используются. Особенное внимание мы уделяем принципам деятельности Европейского Генерального регламента по работе с персональными данными (GDPR) и платёжной директиве PSD2, которая регламентирует технические стандарты открытых API. Клиенты банков получают возможность раскрывать информацию о себе другим участникам финансового рынка, при этом не нарушая действующие законы по защите персональных данных.

КИБЕРБЕЗОПАСНОСТЬ — ЗАЛОГ УСПЕХА ИННОВАЦИЙ

Ключевой фактор успеха в реализации цифровых проектов — обеспечение высокой степени кибербезопасности. Ряд проектов требует установки сертифицированного ФСБ шифровального оборудования.

Иллюстративной, с точки зрения современных требований к кибербезопасности, является и реализация проекта «Удалённая идентификация». В соответствии с Законом о персональных данных (ФЗ-152), каждый этап — от ввода информации до её хранения и предоставления предполагает значительный уровень защиты. Здесь применяется сквозное шифрование с использованием отечественных криптоалгоритмов. Также предусмотрено раздельное хранение данных биометрии.

* * *

В 2017 г. в России в кибербезопасность было инвестировано около 55 млрд рублей (для сравнения, в мире в 2018 г. объём инвестиций достигал порядка 100 млрд долларов США). С развитием инновационных цифровых проектов объём инвестиций в информационную безопасность будет увеличиваться.



Карл СУММАНЕН
независимый
эксперт

ИТ-ИМПОРТО-ЗАМЕЩЕНИЕ В РОССИИ

ПУТИ ДАЛЬНЕЙШЕГО СОВЕРШЕНСТВОВАНИЯ

В статье рассматривается модель импортозамещения в сфере информационных технологий. Рассмотрены наиболее существенные с точки зрения импортозамещения особенности ИТ-индустрии. Определены требования к оптимальной модели управления импортозамещением в ИТ с учетом указанных особенностей.

ВВЕДЕНИЕ

26 июля 2016 г. Правительством был утвержден план перехода в 2016–2018 годах госорганов и госфондов на использование отечественного офисного ПО. В ноябре 2018 Счётная палата РФ (бюллетень № 1 от 31.01.19) проанализировала затраты госорганов на импортозамещение ПО в 2017–2018 гг. Данные Счётной палаты (Таблица 1) показывают, что спустя три года с начала активных мероприятий по импортозамещению в органах исполнительной власти (ОИВ) 99% федеральных ОИВ (ФОИВ) и 100% региональных ОИВ (РОИВ) по-прежнему используют¹ иностранные системы управления базами данных (СУБД), 96% ФОИВ и 94% РОИВ используют иностранные операционные системы (ОС), 82% ФОИВ и 91% РОИВ используют иностранные системы электронной почты (СЭП).

Для некоторых типов ПО ситуация несколько лучше, например, иностранные системы элек-

тронного документооборота (СЭДО) и информационной безопасности (СИБ) продолжают использовать только 25% ФОИВ.

Судя по значительному уровню использования отечественного ПО для некоторых типов ПО, можно утверждать, что подход к импортозамещению, применяемый в России, иногда дает положительные результаты. Видно также, что в некоторых случаях импортозамещение «буксует».

Можно предположить, что «неоднородность» динамики импортозамещения объясняется тем, что действующая модель импортозамещения не учитывает какие-то важные особенности устройства ИТ-индустрии и должна быть оптимизирована с учетом объективных законов функционирования ИТ-индустрии. Возможные направления оптимизации рассматриваются ниже.

ИСТОЧНИКИ ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ

Невозможно эффективно решать проблему, не понимая ее сути и источников. Чтобы обеспечить такое понимание, ниже кратко рассматривается содержание и причины возникновения задачи импортозамещения в ИТ-отрасли России.

Задача импортозамещения связана с технологической зависимостью России в ИТ, возникшей на этапе перестройки и в течение первого десятилетия существования страны как отдельного государства как побочный эффект встраивания в глобальную систему разделения труда.

Межстрановое разделение труда является объективным явлением и неотъемлемой частью процесса глобализации. Разделение труда влечет снижение участвующими странами²

¹ К сожалению, отчет Счётной палаты не содержит количественные данные, характеризующие относительные объемы использования ПО различного происхождения.

² Наиболее сильно это выражено для стран на нижних уровнях иерархии ИТ-технологий.

ОИВ	СУБД	ОС	СЭП	СЭДО	СИБ
ФОИВ	1%	4%	18%	75%	75%
РОИВ	0%	6%	9%	-	62%

Таблица 1. Доля госорганов, использующих только отечественное ПО

уровня технологического суверенитета³, что в свою очередь приводит к появлению зависимостей между странами.

Проблема, однако, не в зависимости, которая возникает при любом разделении труда, а в том, что эта зависимость асимметрична. Глобальная система разделения труда не является простой одноранговой сетью, в которой все участники примерно одинаково зависят друг от друга. Существующая система имеет вид иерархии, на вершине которой находятся технологические лидеры — страны, владеющие базовыми передовыми технологиями, — от которых зависят все страны, находящиеся на более низких уровнях. Чем ниже находится страна, тем больше она зависит от других стран и тем меньше остальные страны зависят от нее. Благодаря асимметрии технологические лидеры могут оказывать давление на зависящие от них страны, находящиеся ниже. И это сегодня является проблемой.

С момента возникновения и до определенного момента в начале нулевых РФ добровольно встраивалась в глобальную систему разделения труда. В силу особенностей экономической и политической ситуации встраивание происходило в нижние уровни мировой технологической иерархии. Фактически РФ сознательно отказалась от технологического суверенитета во многих областях, включая ИТ⁴.

Технологическая зависимость не проявлялась, пока между Россией и технологическими лидерами не было открытых разногласий. Как только они возникли, технологические лидеры немедленно использовали зависимость для давления. Именно в этот момент задача восстановления технологического суверенитета стала актуальной как одна из задач, решение которой необходимо для обеспечения национальной безопасности.

СУВЕРЕННАЯ ИТ-ЭКОСИСТЕМА

С учетом существующей ситуации и объективных возможностей экономики России наиболее оптимальным и реалистичным способом решения задачи восстановления технологического суверенитета в области ИТ представляется создание технологически независимой и функци-

³ Под технологическим суверенитетом здесь и далее понимается возможность использования технологий независимо от позиций и действий других международных субъектов.

⁴ Следует отметить, что многие страны БРИКС, ЕС и Америки предприняли меры на государственном уровне для защиты своего технологического суверенитета, в том числе с помощью использования свободного программного обеспечения (https://en.wikibooks.org/wiki/FOSS_Government_Policy/Strategies)

Построение суверенной ИТ-экосистемы является сложной задачей, необходимым условием успешного решения которой является понимание и учет объективных законов развития и функционирования ИТ-индустрии

онально полной (обеспечивающей все критичные и большую часть наиболее существенных ИТ-сервисов и продуктов) национальной ИТ-экосистемы (далее «суверенная ИТ-экосистема»), устойчивой по отношению к внешним воздействиям и слабо зависящей от внешних ресурсов.

В результате создания суверенной ИТ-экосистемы одновременно соответствующим образом должна измениться модель встраивания национальной ИТ-индустрии в глобальную. При этом, однако, важно понимать, что создание суверенной ИТ-экосистемы не должно рассматриваться как самоизоляция в ИТ. Решая задачу достижения технологической независимости, необходимо оставаться максимально встроенными в глобальную экономику.

По понятным причинам на первом этапе приоритетным является оперативное решение задачи обеспечения технологической независимости в ИТ. Эта задача имеет инфраструктурный и частично политический характер⁵.

Одновременно должна быть поставлена задача достижения в более долгосрочной перспективе глобальной конкурентоспособности национальной ИТ-индустрии, в том числе такая амбициозная цель, как разрушение или ослабление существующих монополий в ИТ за счет создания альтернативных технологических вертикалей.

Построение суверенной ИТ-экосистемы — сложная задача, необходимым условием успешного решения которой является понимание и учет объективных законов развития и функционирования ИТ-индустрии.

ОСОБЕННОСТИ ИТ-ИНДУСТРИИ

ИТ-индустрия как сложная динамическая система.

ИТ-индустрия может рассматриваться как сложная динамическая система, включающая большое количество элементов различных типов, в том числе участников (производители и потре-

⁵ Последнее означает, что в необходимых случаях требование коммерческой успешности отдельных мероприятий может ослабляться либо полностью сниматься.

Можно воспользоваться нелинейностью ИТ-индустрии и попробовать обогнать лидеров путем «туннелирования в послезавтра», сфокусировав усилия и ресурсы на разработке технологий более отдаленного будущего

бители ИТ-продуктов, интеграторы, сервис-провайдеры) и ИТ-артефактов (ИТ-продукты, технологии, протоколы, стандарты).

ИТ-индустрия не статична, под действием рыночных процессов структура и состав ИТ-индустрии постоянно изменяются, рождаются новые, развиваются существующие, умирают устаревшие или не выдержавшие конкуренции ИТ-продукты и участники, возникают новые ИТ-технологии⁶. В любой момент времени в ИТ-индустрии сосуществует множество ИТ-продуктов и ИТ-технологий на разных стадиях развития, между которыми действуют многочисленные взаимозависимости.

Как это часто бывает со сложными рыночными системами, ИТ-индустрия является стохастической недетерминированной системой с высоким уровнем неопределенности, эволюция которой управляется не только и не столько волей участников, сколько случайными событиями.

Помимо динамики, связанной с эндогенными взаимодействиями и процессами, эволюция ИТ-индустрии подвержена сильному влиянию экзогенных, внешних по отношению к ИТ, факторов, в том числе научно-технического прогресса.

Динамика развития ИТ-индустрии нелинейна. Периоды «поступательного» эволюционного развития конечны по длительности и могут прерываться в результате критических событий, например, появления новых технологий, которые приводят к появлению «точек бифуркации» и резкой масштабной перестройке.

Специфичным для ИТ-индустрии является такое явление, как резкий рост стоимости развития технологий «в области плато». После достижения определенного уровня зрелости технологии и реализации в основном потенциала

⁶ В последнее время скорость этих изменений имеет тенденцию к росту. Заметим, что при росте частоты технологических изменений до уровня близкого к характерному времени достижения зрелости ИТ-продуктов можно ожидать качественного изменения динамики ИТ-индустрии.

развития дальнейший прогресс стоит очень дорого. Из-за этого удерживать лидерство могут только глобальные компании. Компании национального уровня технологическими лидерами, как правило, быть не могут.

Заметим, что с точки зрения задачи создания суверенной ИТ-экосистемы технологическое лидерство не нужно. Чтобы быть технологически независимым, необязательно быть лидером. Напротив, попытка решения заведомо нерешаемой имиджевой задачи «завоевания лидерства» скорее всего будет иметь обратный результат — догнать и обогнать не получится, ресурсы и время будут потрачены и шансы решить основную задачу снизятся⁷.

В условиях ресурсных и временных ограничений оптимальной стратегией является прагматичное использование любых доступных технологий, пусть даже «вчерашнего дня», при условии, что они решают задачу восстановления технологического суверенитета. Одновременно, используя высвободившиеся ресурсы, можно воспользоваться нелинейностью ИТ-индустрии и попробовать обогнать лидеров путем «туннелирования в послезавтра», сфокусировав усилия и ресурсы на разработке технологий более отдаленного будущего.

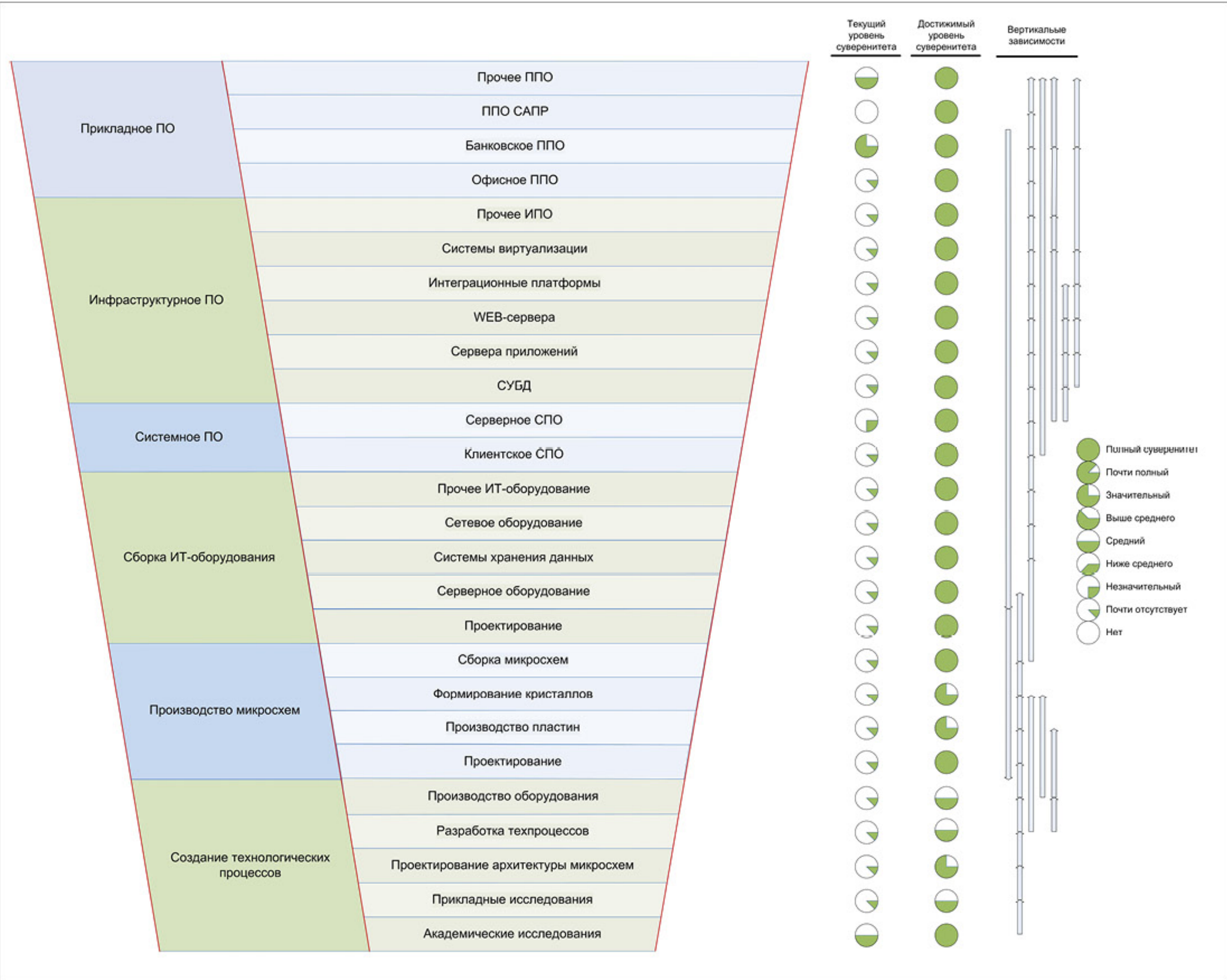
В целом разработку стратегии создания суверенной ИТ-экосистемы можно рассматривать как решение задачи теории игр с элементами военной стратегии в виде задачи преследования в изменяющемся многомерном пространстве с множеством участников с ограничениями по скорости и ресурсам.

Эталонизация

В отличие от классического рынка, подразумевающего конкуренцию однотипных продуктов, ИТ-индустрия имеет тенденцию к монополизации. Из-за больших инвестиций в развитие технологий эффект масштаба на рынке ИТ выражен сильнее, чем на рынках простых товаров. Большая доля рынка упрощает дальнейшее расширение доли рынка. Из-за этой положительной обратной связи дублирующие ИТ-продукты вытесняются с рынка, что приводит к выживанию на рынке одного «эталонного» ИТ-продукта.

Эффект эталонизации усиливается из-за некоторых других особенностей ИТ-индустрии, например, требования «операционной» совместимости, существенного для некоторых клас-

⁷ В этой связи возникает вопрос конкуренции за ресурсы (и координаты вообще) между мероприятиями по импортозамещению и программой «Цифровая экономика». Необходим анализ наличия и достаточности ресурсов и гармонизация этих программ, в том числе в части реализуемых мероприятий.



сов ИТ-продуктов, возникающего в связи с информационным обменом между потребителями таких продуктов.

Кластеризация

ИТ-индустрия имеет иерархическую организацию (упрощенно она показана на рисунке 1). На верхнем уровне детализации можно выделить следующие уровни: (1) технологические процессы; (2) элементно-компонентная база (микросхемы — процессоры, контроллеры и т.п.); (3) конечное ИТ-оборудование; (4) программное обеспечение (ПО).

Каждый укрупненный уровень может быть декомпозирован на несколько вложенных более детальных подуровней. Например, ПО можно разделить на (4.1) системное ПО (операционные системы); (4.2) инфраструктурное ПО (связующее ПО и ПО промежуточного уровня — системы управления базами данных, интеграционные платформы, системы управле-

ния бизнес-процессами, сервера приложений, системы виртуализации и т.п.); (4.3) прикладное ПО.

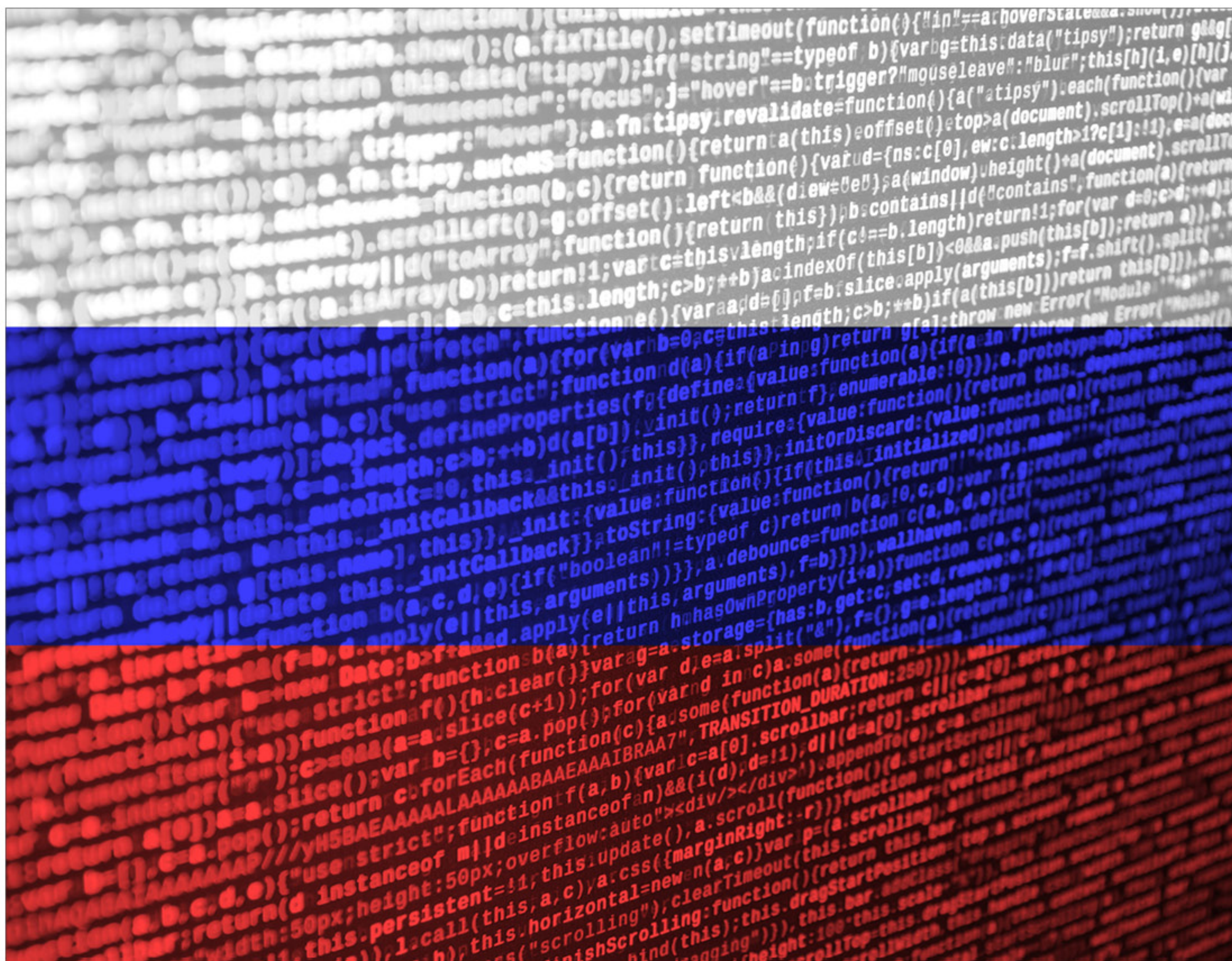
Внутри одного уровня может быть несколько «предметных» областей (на рисунке выше области показаны как детальные уровни).

Между уровнями существуют «вертикальные» зависимости, как правило направленные снизу вверх (более высокий уровень зависит от нижележащих), однако возможны и зависимости, направленные сверху вниз. Кроме того, в пределах одного уровня могут быть «горизонтальные» зависимости между ИТ-продуктами внутри одной области или между разными областями.

Из-за взаимозависимостей ИТ-продукты образуют сильносвязанные кластеры. Внутри кластера его компоненты критично зависят друг от друга. В результате изменения или замеще-

Рисунок 1. Технологическая иерархия ИТ⁸

⁸ Приведенная оценка текущего и достижимого уровней суверенитета отражает субъективное мнение автора.



ния одного из компонентов кластера требуется доработка или замещение всех или значительной части остальных его компонентов.

Из-за описанных зависимостей задачи импортозамещения, как правило, не могут решаться для отдельных компонентов, и импортозамещение кластера должно производиться целиком. Так как в случае кластера требуются значительно большие инвестиции и компетенции сразу в нескольких областях, задача импортозамещения редко может быть решена силами отдельной компании.

Ограничения и начальные условия

При выработке стратегии создания суверенной ИТ-экосистемы необходимо учитывать все значимые ограничения, в первую очередь технологические, ресурсные (финансы, специалисты) и временные, и существующие начальные условия, в частности, технологическое отставание и отсутствие некоторых элементов ИТ-индустрии.

МОДЕЛЬ УПРАВЛЕНИЯ ИМПОРТОЗАМЕЩЕНИЕМ

Ниже кратко перечислены принципы оптимальной модели импортозамещения в ИТ, вытекающие из рассмотренных выше особенностей ИТ-индустрии, в частности, понимания, что (1) ИТ-индустрия является нелинейной стохастической динамической системой, непрерывно изменяющейся во времени, подверженной внешним влияниям, поведение которой характеризуется значительными неопределенностями и критическим поведением; (2) задача создания суверенной ИТ-экосистемы и, тем более достижения глобального технологического лидерства, является исключительно сложной и её решение требует учета большого числа факторов, в том числе действий множества участников с разнонаправленными интересами, в том числе стратегических противников; (3) задача решается в условиях технологических, ресурсных и временных ограничений и неблагоприятных начальных

условий и (4) так как речь идет о национальной безопасности, цена ошибки и/или потери времени очень велика.

Стратегическое целеполагание

Сложность задачи, ограничения, неблагоприятные начальные условия и высокая цена ошибки исключают метод проб и ошибок и делают необходимым точное целеполагание, основанное на глубоком всестороннем экспертном анализе, учитывающее объективные законы функционирования ИТ-индустрии и все значимые факторы.

До начала создания суверенной ИТ-экосистемы должны быть максимально точно определены оптимальные и достижимые с учетом ограничений средне- и долгосрочные стратегические цели, в том числе оптимальная модель суверенной ИТ-экосистемы, включая схему её встраивания в глобальную ИТ-индустрию.

Стратегическое планирование

Целеполагание является необходимым, но не достаточным условием. Как и в случае целеполагания, сложность задачи, ограничения, неблагоприятные начальные условия и высокая цена ошибки исключают метод проб и ошибок и делают необходимым определение оптимальной траектории достижения поставленных целей до начала любых мероприятий по созданию суверенной ИТ-экосистемы.

Динамическая актуализация целей и планов

Поскольку ИТ-индустрия как динамическая система непрерывно изменяется, цели, определенные на этапе целеполагания, становятся «бегущими», а стратегия может со временем терять оптимальность или даже становиться невыполнимой. Как следствие, требуется постоянная актуализация целей и стратегических планов на основе непрерывного мониторинга и ситуационного анализа.

Консолидация участников

Стратегическая цель создания суверенной ИТ-экосистемы является общенациональной и её достижение зависит от действий практически всех участников национальной ИТ-индустрии, как производителей, так и потребителей. Так, многие из частных задач, например, импортозамещение кластеров взаимозависимых ИТ-продуктов или создание национальных платформ, требуют совместной работы многих производителей и потребителей.

Поскольку интересы отдельных участников часто разнонаправлены, а ресурсы и компетенции ограничены, для успешного решения за-

дач импортозамещения, которые не приносят быстрой прибыли, требуют быстрого решения, единого целеполагания, учета общенациональных интересов, широких компетенций, необходима консолидация участников, их компетенций и финансовых ресурсов.

Системность и комплексность

В силу глубины и масштабности трансформации ИТ-индустрии задача создания суверенной ИТ-экосистемы является более общей, чем простой переход на преимущественное использование отечественного ПО.

Из-за сложности ИТ-индустрии как системы, определение стратегических целей и стратегии их достижения возможно только при условии применения системного подхода на основе экспертного анализа, обеспечивающего учет всех существенных факторов и объективных законов ИТ-индустрии. Подход к трансформации национальной ИТ-индустрии должен быть всесторонним и включать проработку всех значимых направлений, в том числе юридического (права интеллектуальной собственности), маркетинга (продвижение отечественных ИТ-продуктов), международной кооперации (создание стратегических партнерств с другими странами и ведущими ИТ-компаниями) и т.п.

Приоритет решений экспертов предметной области

Поскольку содержательный анализ может быть выполнен только силами экспертов в предметной области⁹, последние должны обладать исключительной прерогативой принятия решений по всем содержательным (неполитическим) вопросам.

Экспертные решения должны быть первичными по отношению к политическим и в случае конфликта между экспертными и политическими решениями, выбор должен быть в пользу первых. Политики вправе выбирать из нескольких реализуемых и оптимальных вариантов выработанных и одобренных экспертами.

Приоритет общенациональных интересов

Интересы участников национальной ИТ-индустрии, в том числе коммерческих компаний, органов исполнительной или законодательной

⁹ Возможность создания суверенной ИТ-экосистемы критично зависит от наличия специалистов высокого уровня в соответствующих предметных областях. В связи с этим возникает проблема формирования и удержания в стране человеческого капитала в ИТ-отрасли, без которого отечественного ПО не будет вообще и Россия окажется в полной технологической зависимости. Мероприятия по формированию и удержанию необходимых специалистов должны быть частью стратегии создания суверенной ИТ-экосистемы.

власти, ведомств, не всегда совпадают с общенациональными. При определении стратегических целей должен быть обеспечен оптимальный баланс общенациональных и частных интересов с приоритетом общенациональных.

Реализм, рациональность, приоритеты, фокус

Наличие ресурсных и временных ограничений, неблагоприятные начальные условия и высокая цена ошибки превращают создание суверенной ИТ-экосистемы из решения технической задачи в искусство возможного.

С учетом вышеперечисленных факторов определение стратегических целей и планирование должны основываться на принципах реалистичности (не пытаемся делать невозможное, ставим реальные сроки), рациональности и прагматизма (делаем только то, что действительно необходимо, избегаем перфекционизма и имиджевых задач), фокусирования и приоритетов (не разбрасываемся и не пытаемся сделать все и сразу).

Использование свободного ПО

Национальный рынок производителей намного меньше глобального и закрыть все потребности в ИТ-продуктах решениями только российских производителей практически невозможно. Оптимальной представляется гибридная модель, предполагающая использование как внутренних решений, так и свободного и открытого ПО (СОПО). Такой подход упростит встраивание в глобальную систему разделения труда и поможет избежать самоизоляции.

Для организации эффективной работы с СОПО необходимо изменение государственной политики в части СОПО и создание, в том числе при участии государства, организационно-технической инфраструктуры для управления и поддержки развития СОПО, в том числе фондов СПО (по аналогии с Apache Software Foundations, СИЗИФ-АлтЛинукс и FOSS), от-

крытых центров для тестирования и развития и разработки программ, инфраструктуры поддержки управления версиями (типа GitHub и GitLab).

Централизованное управление

При организации масштабного комплекса мероприятий, часть из которых реализуется в общенациональных интересах, в некоторых из которых принимает участие несколько участников с разнонаправленными интересами, необходимо оптимальное разделение задач между рынком и централизованным управлением.

Анализ показывает, что в случае рассматриваемой задачи создания суверенной ИТ-экосистемы рыночная модель, в силу некоторых ее объективных особенностей, а именно:

- ♦ рынок — это ненаправленное движение методом проб и ошибок, что делает рыночные процессы медленными и неэффективными с точки зрения расходования ресурсов;

- ♦ рынок движим частными интересами отдельных субъектов, эти интересы как правило разнонаправлены и далеко не всегда совпадают с общенациональными. Из-за этого рынок неэффективен, когда нужно решать общенациональные задачи и любые задачи, требующие координации участников и консолидации ресурсов;

- ♦ в основе рыночных процессов, как правило, фокус на быструю прибыль. В случае задачи создания суверенной ИТ-экосистемы возможность получения быстрой прибыли и прибыли вообще есть не всегда;

- ♦ рыночный процесс формирования глобальных или национальных платформ может занимать длительное время (десятилетия), что неприемлемо при решении задачи создания суверенной ИТ-экосистемы, когда разработка национальных платформ должна быть завершена в короткое время,

имеет ограниченное применение и далеко не всегда является оптимальным выбором. Как минимум часть задач импортозамещения должна решаться с использованием централизованной модели управления.

Как общий принцип можно утверждать, что модель централизованного управления является более оптимальной в случае задач не приносящих быстрой прибыли, требующих единого целеполагания, учета общенациональных интересов, мобилизации ресурсов, координации действий многих участников. К таким задачам относятся задачи импортозамещения кластера взаимозависимых ИТ-продуктов и создания национальных платформ.

Наличие ресурсных и временных ограничений, неблагоприятные начальные условия и высокая цена ошибки превращают создание суверенной ИТ-экосистемы из решения технической задачи в искусство возможного

Для эффективной координации и контроля совокупности одновременно ведущихся по разным направлениям работ в систему централизованного управления работами по импортозамещению должна входить подсистема координации и контроля, которая должна обеспечить в том числе гармонизацию работ по взаимозависимым направлениям и анти-коррупционный контроль.

Госфинансирование

Некоторые задачи, критичные для создания суверенной ИТ-экосистемы, например, инфраструктурные и решаемые в общенациональных интересах, могут не приносить быстрой прибыли и прибыли вообще. Решение таких задач на коммерческой основе не всегда возможно и для них должно быть предусмотрено полное или частичное финансирование за счет средств государственного бюджета и/или средств, выделяемых бизнесом на некоммерческой основе.

ЦЕНТР АНАЛИЗА И СТРАТЕГИЧЕСКОГО ПЛАНИРОВАНИЯ

Как отмечено выше, трудность задачи создания суверенной ИТ-экосистемы, в том числе в силу сложности ИТ-индустрии как системы, необходимости учета нелинейной стохастической динамики, критических явлений, ресурсных ограничений, неблагоприятных начальных условий, действий множества участников с разнонаправленными интересами, включая стратегических противников, делает необходимым участие в решении задач стратегического целеполагания и планирования экспертов, представляющих все предметные области, связанные с ИТ-индустрией. Кроме того, из-за динамического характера ИТ-индустрии требуется непрерывное уточнение целеполагания и актуализация стратегии достижения цели.

Максимальная эффективность работы экспертов может быть достигнута только при условии наличия постоянно действующего Центра анализа и стратегического планирования (ЦАСП) в сфере ИТ, укомплектованного специалистами в соответствующих областях, работающими на постоянной основе.

Первоочередная задача ЦАСП — обеспечить оптимальное целеполагание и стратегическое планирование. Также целесообразно возложить на ЦАСП задачу проектирования организационно-технической инфраструктуры управления и поддержки работы с СОПО.

На этапе реализации стратегии ЦАСП должен обеспечить непрерывную актуализацию стратегических целей и планов. Кроме того,

Максимальная эффективность работы экспертов может быть достигнута только при условии наличия постоянно действующего Центра анализа и стратегического планирования (ЦАСП) в сфере ИТ

ЦАСП может осуществлять «авторский надзор» за реализацией стратегии и выступать заказчиком по отдельным стратегическим задачам.

Являясь экспертным аналитическим центром в сфере ИТ, ЦАСП должен обладать сильными компетенциями во всех предметных областях, от которых зависит выработка стратегии трансформации национальной ИТ-индустрии. по стратегическому планированию. Важно обеспечить наполнение ЦАСП лучшими специалистами в соответствующих предметных областях.

Ввиду важности решаемой задачи и необходимости приоритета национальных интересов перед частными необходимо предусмотреть персональную ответственность руководителей ЦАСП за выполнение поставленных задач.

Помимо укомплектования ЦАСП собственными специалистами, необходимо также обеспечить подключение к работе над стратегией более широкого экспертного сообщества, в том числе специалистов существующих академических и отраслевых институтов и образовательных учреждений, профильных ведомств, отдельных независимых экспертов, представителей участников ИТ-индустрии.

Работа экспертов, как сотрудников ЦАСП, так и привлеченных специалистов, над стратегией должна оплачиваться на уровне, обеспечивающем заинтересованность высококвалифицированных специалистов в данной работе. С учетом того, что ЦАСП решает общенациональные задачи, представляется целесообразным соответствующее финансирование производить, как минимум частично, из бюджетных средств.

Для создания ЦАСП необязательно создавать новую структуру. Как вариант, ЦАСП может быть создан путем расширения функций (и соответствующим расширением штата и полномочий) какой-либо из существующих «профильных» структур.

Автор выражает благодарность за содержательные обсуждения С. П. Селезневу, А. Д. Амшаринскому и Д. П. Лиходееву.



Максим ФЕДОТЕНКО
руководитель направления
Центра внутри-
корпоративного
взаимодействия
Сбербанка

ТЕХНОЛОГИЯ ЗАЩИТЫ ОТ УГРОЗЫ ПОДМЕНЫ БИОМЕТРИЧЕСКОГО СКАНЕРА

ЧАСТЬ 2. МЕТОД PUSH-УВЕДОМЛЕНИЙ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ¹

ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ В МОБИЛЬНОМ КАНАЛЕ

В качестве примера использования биометрических данных в мобильном канале возьмём лицо. Эту модальность используют как Единая биометрическая система, так и Сбербанк в собственной системе дистанционного банковского обслуживания Сбербанк Онлайн. Один раз придя в отделение банка, клиент регистрирует свой биометрический шаблон, а далее сможет использовать его для аутентификации или подтверждения подозрительных транзакций в мобильном приложении Сбербанк Онлайн. Кроме того, реализуется процесс регистрации биометрического шаблона с использованием мобильного приложения и устройства самообслуживания, а также регистрация самого мобильного приложения при помощи биометрии.

При использовании биометрии в банке в рамках мобильного приложения алгоритм действий таков. Камера телефона снимает видео клиента и отправляет в мобильное приложение (напри-

мер, Сбербанк Онлайн). Мобильное приложение осуществляет предобработку изображения, в том числе контроль качества и проверку liveness detection², то есть контролирует, что камера снимает живого человека, а не манекен, фотографию или видеозапись. Затем оно выбирает наилучший кадр, полученный из видеопотока, и отправляет его на сервер для осуществления сравнения с хранящимся в базе данных шаблоном (Рис. 1).

Банк должен определить, получив фотографию клиента, что тот действительно находится перед камерой мобильного устройства, что фотографию прислало именно банковское мобильное приложение, и вся локальная логика по проверкам была пройдена.

ПРОБЛЕМЫ БИОМЕТРИЧЕСКОГО ПРОЦЕССА

Сценарии атак можно разделить на две категории. Первая — это целенаправленная атака на клиента посредством предоставления био-

² Описание некоторых методов liveness detection для лица можно посмотреть, например, здесь: <https://arxiv.org/ftp/arxiv/papers/1405/1405.2227.pdf>

¹ Продолжение. Начало в № 1/2019

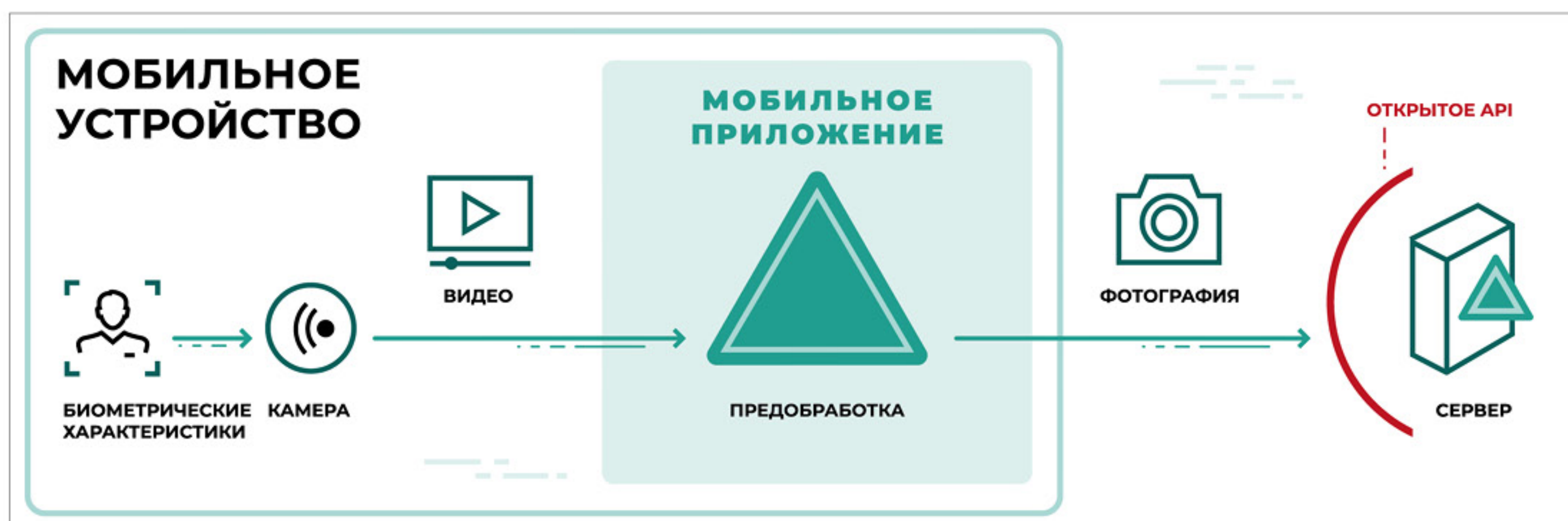


Рисунок 1. Биометрический процесс в мобильном приложении

метрических данных без присутствия самого клиента. Для неё достаточно найти хорошую фотографию атакуемого в Интернете и отправить её в открытое API серверной части в обход проверок на liveness detection: например, такими средствами, как SoapUI³ или Postman⁴. В случае регистрации мобильного приложения только по биометрии злоумышленник может зарегистрироваться от имени человека, изображённого на той самой фотографии, со всеми вытекающими из этого последствиями в виде несанкционированных переводов денежных средств.

Вторая — это вариант фишинга, когда злоумышленник может разработать собственное приложение и предлагать его для доступа к сервисам Сбербанка или вообще никоим образом не связывать его со Сбербанком (например, редактор фотографий). При этом фишер может как формировать собственную базу данных биометрических признаков клиентов, так и выполнять с помощью приложения мошеннические операции.

Следовательно, необходимо проводить аутентификацию не только пользователя, но и самого мобильного приложения.

Замечу, что в статье мы не будем рассматривать такую атаку, как модификация уже установленного мобильного приложения, например, при помощи вируса. Такая возможность обычно возникает при работе пользователя на устрой-

стве под правами суперпользователя (root/jail-break-устройство). Так может работать бот-сеть, которая выискивает рутованные устройства, модифицирует их, например, сохраняя на устройстве или в бот-сервере аутентификаторы пользователя и использует их с этого же устройства для вывода денег, но без интерактива с пользователем. Такую операцию можно провести и с паролем, и с ПИН-кодом, и с биометрией, то есть любыми аутентификаторами, которые вводятся пользователем в мобильное приложение. Зарутовав устройство, пользователь принимает риски кражи денег на себя.

ОДИН МЕТОД АУТЕНТИФИКАЦИИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

При решении задачи аутентификации мобильного приложения необходимо создать механизм не только эффективный с точки зрения кибербезопасности, но и достаточно удобный для клиента. В качестве такого механизма было выбрано распределение ключей аутентификации приложения при помощи механизма отправки push-уведомлений, реализуемых соответствующими сервисами производителей мобильных операционных систем (Apple Push Notification Service (APNS), Google/Firebase Cloud Messaging (GCM, FCM)).

Вначале немного о технологии push-уведомления для мобильных устройств (Рис. 2).

Мобильное приложение вызывает функции операционной системы устройства для регистрации в push-сервисе. ОС транслирует этот запрос в push-сервис, предоставляя информацию

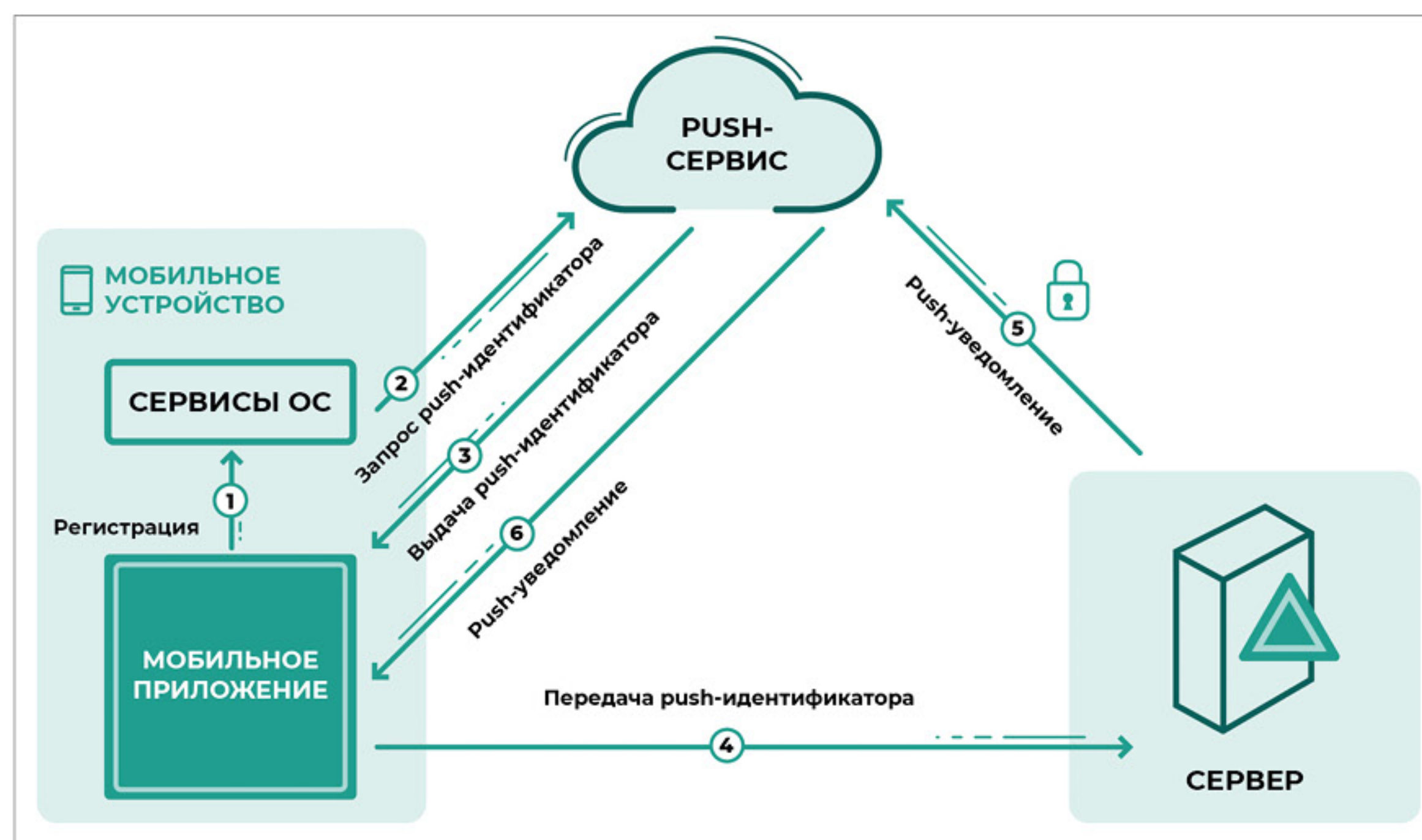


Рисунок 2. Push-уведомления

³ <https://www.soapui.org/>

⁴ <https://www.getpostman.com/>

Злоумышленнику сложно вклиниться в процесс *push*-уведомления.
Генерация *push*-идентификатора — нативный процесс мобильной операционной системы и *push*-сервиса

о приложении (например, идентификатор, про-
файл) и устройстве. На основе этой информации
push-сервис генерирует push-идентификатор —
уникальный идентификатор, привязанный
именно к данному экземпляру нашего мобиль-
ного приложения. Push-идентификатор полу-
чается мобильным приложением и передаётся
на наш сервер для того, чтобы сервер мог отпра-
вить push-уведомление в любое время в адрес
нашего приложения.

Что в этом процессе для нас существенно? Злоумышленнику сложно вклиниться в процесс push-уведомления. Генерация push-идентификатора — нативный процесс мобильной операционной системы и push-сервиса. Это взаимодействие защищено криптографически, а генерация push-уведомления про-

исходит, как минимум, на основе идентификатора мобильной ОС (идентифицируется криптографически при помощи её закрытого ключа) и сущностей, идентифицирующих приложение. Получается, что сфальсифицировать push-идентификатор практически невозможно. А если его подменить? Дело в том, что push-идентификатор передаётся на серверную часть. Если его подменить в этот момент, например, на push-идентификатор другого приложения, push-уведомление облаком не будет отправлено. Дело в том, что при отправке push-уведомления в push-сервис наш сервер должен аутентифицироваться. В случае APNS — это криптографическая аутентификация при помощи закрытого/открытого ключей, а в случае GCM/FCM — обычный API-ключ, передающийся в каждом вызове. Самое главное в этой конструкции, что эти аутентификаторы могут быть выданы только разработчику приложения и привязаны к этому приложению. А это означает, что даже если push-идентификатор был подменён push-идентификатором другого приложения, то при отправке push-уведомления на адрес подменённого push-идентификатора push-сервис об-

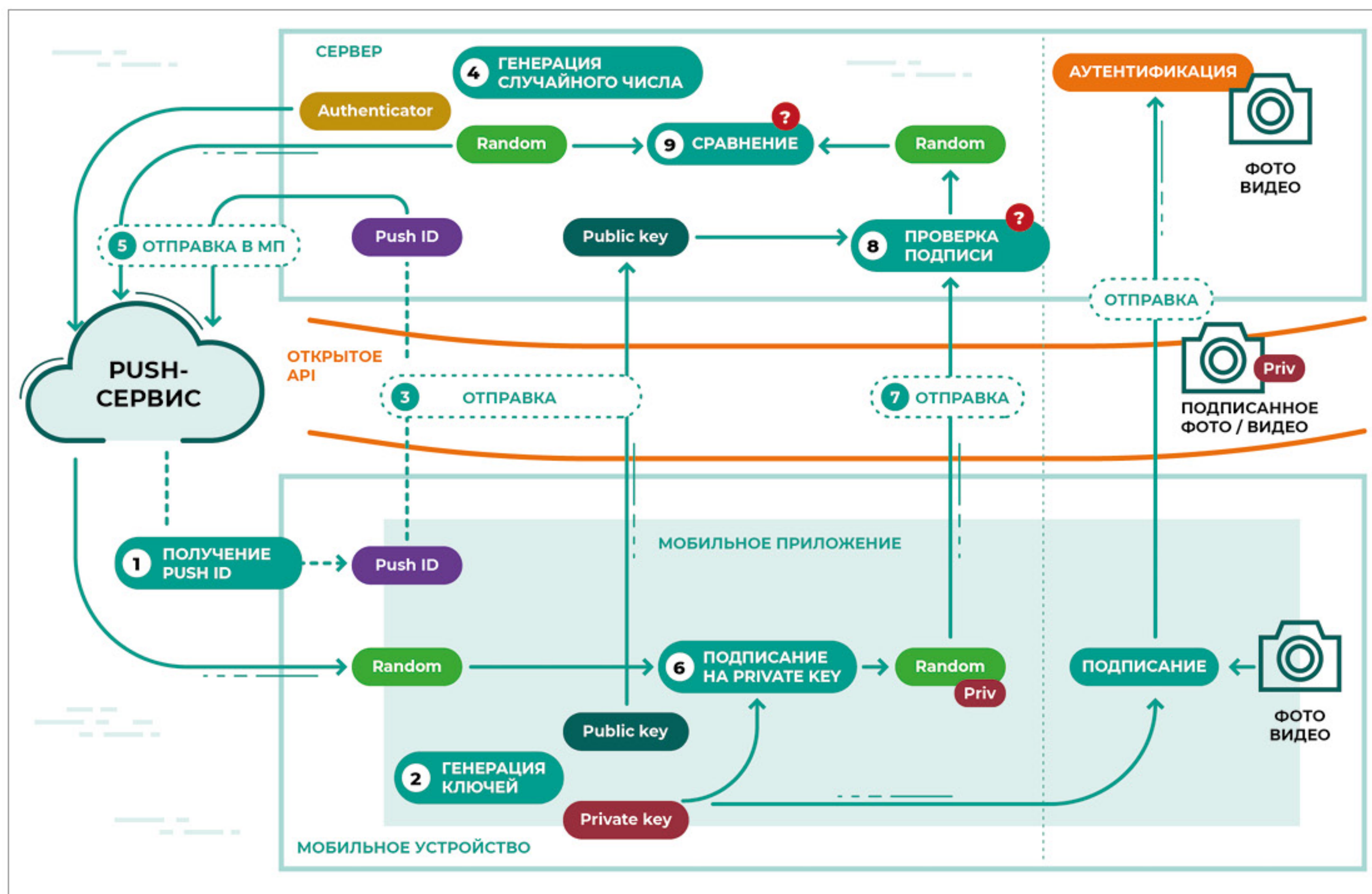


Рисунок 3. Схема создания аутентификатора мобильного приложения

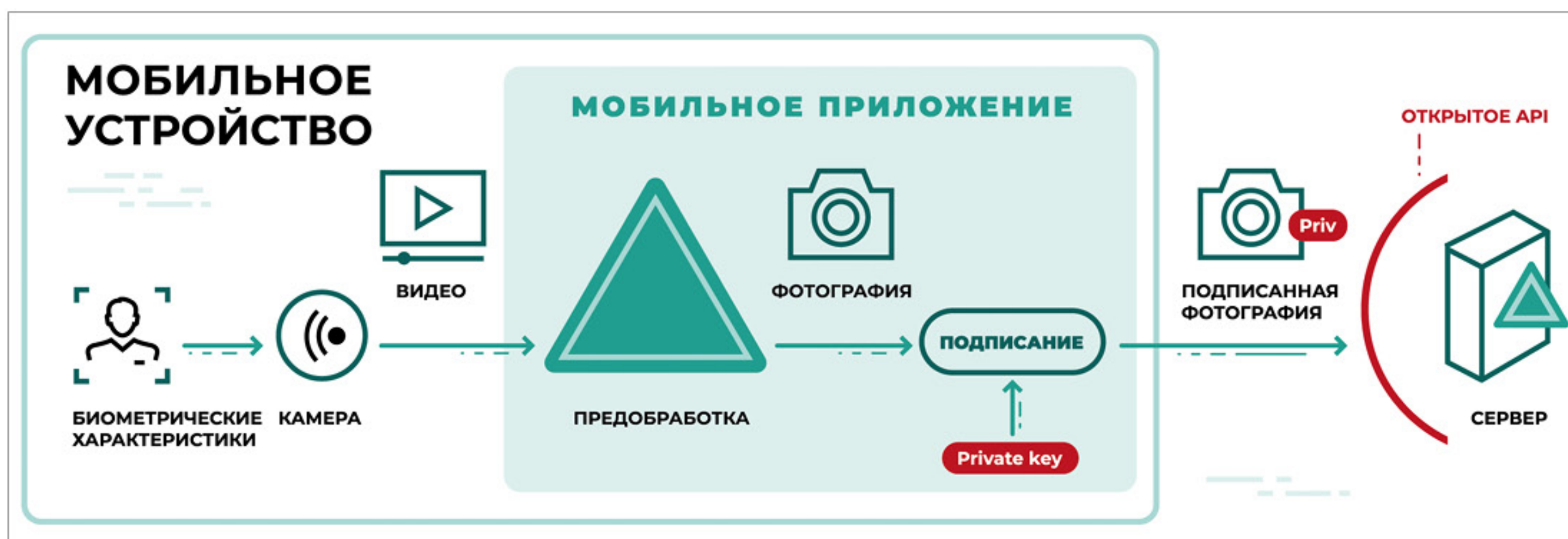


Рисунок 4. Подтверждение биометрических данных закрытым ключом мобильного приложения

наружит, что push-идентификатор выдавался для другого приложения, и сообщит нашему серверу об ошибке несоответствия push-идентификатора и аутентификатора нашего сервера. Поэтому можно сделать вывод, что при помощи push-нотификации можно однозначно определить наше приложение. Для этого предлагается следующая схема взаимодействия (Рис. 3).

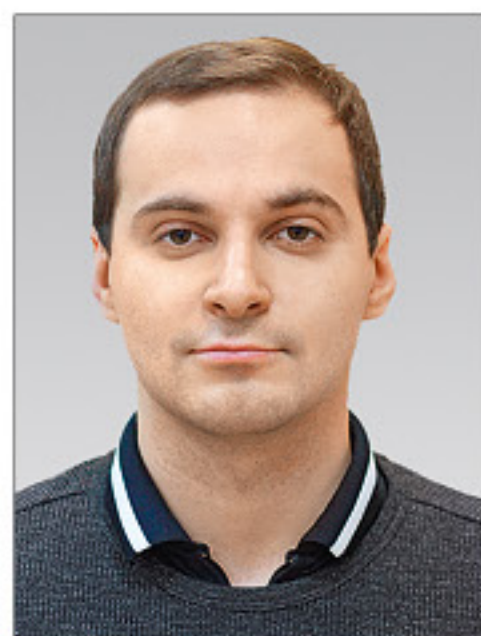
По предлагаемой схеме вначале мобильное приложение получает push-идентификатор и генерирует пару — закрытый и открытый ключ (используемый алгоритм асимметричной криптографии неважен). Далее открытый ключ передаётся приложением на сервер (по стандартному каналу взаимодействия приложения с сервером, обычно HTTP/HTTPS). Сервер генерирует случайное число и отправляет его в приложение в качестве push-уведомления. Приложение, получив push-уведомление, подписывает полученное значение своим закрытым ключом, подтверждая тем самым факт владения им, и отправляет его на сервер. Сервер вначале удостоверяется в корректности подписи пакета, используя открытый ключ приложения, а затем в совпадении случайного числа. Если проверки проходят успешно, то можно считать, что на клиентской стороне работает именно наше мобильное приложение, которое и владеет закрытым ключом. Собственно, закрытый ключ и является аутентификатором нашего мобильного приложения. Поэтому в дальнейшем все биометрические данные (фотографии) могут и должны подписываться на закрытом ключе мобильного приложения для подтверждения того, что они действительно сформированы нашим приложением (Рис. 4).

Размер push-уведомления в нашем случае небольшой, случайное число всегда меньше, чем максимальный размер полезной нагруз-

ки (для APNS и FCM на текущий момент это 4 Кб⁵). Push-уведомление в данном случае является технологическим, и желательно, чтобы оно не отображалось пользователю. В каждом из сервисов есть возможность сделать скрытое push-уведомление (silent push). Один из вариантов — убрать из полезной нагрузки push-уведомления тэг, сигнализирующий о необходимости отображения нотификации (для iOS это alert, а в Android — notification). Также нужно отметить, что для работы данной схемы необходимо разрешение пользователя на приём push-уведомлений. Причём необходимо такое разрешение только на время обмена ключами: как только произошло подтверждение закрытого ключа (аутентификатора), push-уведомления для приложения можно отключить (пользователь при желании может сделать это самостоятельно в настройках мобильной ОС). Заметим, что ни один из рассматриваемых сервисов push-уведомлений не предоставляет гарантию доставки нотификации в мобильное приложение. Например, недоставка может быть связана с отсутствием Интернета на мобильном устройстве, что приводит к невозможности держать соединение с push-сервисом. Однако в данном случае наш процесс по подтверждению аутентификатора мобильного приложения предлагается запускать при соединении приложения с нашим сервером, а это означает, что доступ в Интернет у него есть. Как показывает практика, в этом случае доставляются практически все push-уведомления.

(Окончание в следующем номере)

⁵ <https://developer.apple.com/library/content/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/CreatingtheNotificationPayload.html>, <https://firebase.google.com/docs/cloud-messaging/concept-options>



Николай МАЛЬКОВСКИЙ
научный сотрудник,
ГК ЦРТ



Дмитрий ПОПОВ
научный сотрудник,
ГК ЦРТ



Екатерина КРЫЛОВА
технический писатель научно-
исследовательского департамента, ГК ЦРТ

ЧТО ЭТО ТАМ ШУМИТ?

РОССИЙСКИЕ РАЗРАБОТЧИКИ СТАЛИ ТРЕТЬИМИ В МЕЖДУНАРОДНОМ КОНКУРСЕ CHiME

На крупнейшей мировой конференции по речевым технологиям INTERSPEECH в Хайдерабаде были представлены результаты международного конкурса по распознаванию речи the 5th CHiME Speech Separation and Recognition Challenge (CHiME-5). Третье место в нем заняла система распознавания, созданная командой учёных группы компаний ЦРТ.

О КОНКУРСЕ

Задача CHiME — обеспечить обмен опытом сильнейших команд со всего мира и продвинуть вперёд решение глобальных задач в области распознавания речи. По итогам конкурса участники выступают на конференции с докладами о своих решениях.

Команда научных сотрудников ЦРТ была единственной российской командой на конкурсе. Пьедестал почёта россияне разделили с китайским IT-гигантом iFlytek и командой крупнейшего в мире японского конгломерата Hitachi. Как видно на Рисунке 1, учёных из ЦРТ (в таблице — STC) от лидера гонки отделяют 6%, от участников, занявших второе место, — 0,2%.

Каждый год организаторы предлагают участникам разные задачи. Распознавание речи с близко расположенных микрофонов, таких как гарнитура или телефон, уже показывает хорошие результаты — IT-гиганты отчитыва-

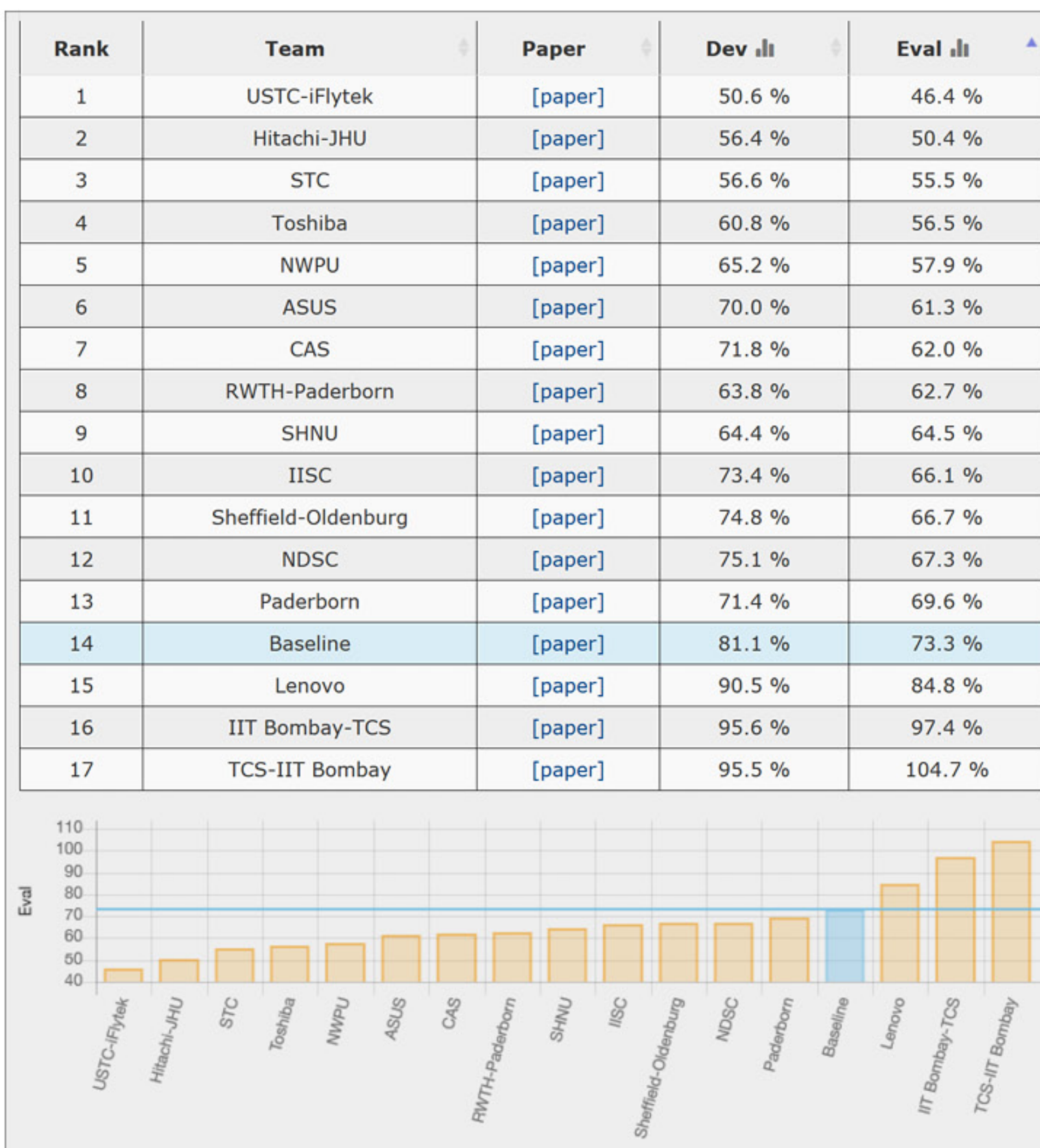


Рисунок 1. Итоговые результаты систем, представленных на конкурс CHiME5.

Жёлтые гистограммы показывают уровень пословной ошибки распознавания (WER (от англ. word error rate) — отношение суммарного веса ошибок распознавания к общему количеству слов в эталонной текстовой расшифровке), которую допустили представленные на конкурс системы на оценочной базе данных. Голубая гистограмма — так называемый baseline, то есть система, с которой начинали все участники.

ются о достижении «человеческого» уровня точности. При этом распознавание на дальней или средней дистанции (больше 1 метра) пока даёт гораздо больше ошибок.

Поэтому в этом году конкурсанты решали так называемую *cocktail party problem* — распознавание спонтанной речи нескольких дикторов в условиях частичного наложения речи и фонового шума. Такую ситуацию часто сравнивают с типичной ситуацией общения на вечеринке, однако общение клиента с продавцом розничного магазина или сотрудником банковского офиса происходит примерно в таких же «праздничных» условиях. Фоновая речь нескольких человек, типичные для офиса или торгового зала шумы существенно снижают точность автоматических систем оценки качества обслуживания.

Записи для конкурса были сделаны на 20 ужинах — в реальных домах на вечеринках, где люди готовили, ели, мыли посуду, свободно и эмоционально общались, шутили и смеялись. Для распознавания здесь сложены одновременная речь 2–4 человек, реверберация и интенсивный шум — звон приборов, льющаяся из крана вода, гул кондиционера, шаги, смех. Цель участников CHiME — создать систему распознавания, которая «прослушает» записи и выдаст полную расшифровку с наименьшим количеством ошибок.

Каждая фонограмма вечеринки делилась на три фазы (не короче 30 минут каждая). Разные фазы проходили в разных зонах квартиры; фаза «кухни» — приготовление еды; фаза «столовая» — застолье; фаза «гостиная» — общение.

ОСОБЕННОСТИ ЗАДАЧИ

Современные системы распознавания показывают отличные результаты на чистой диктовочной речи — как, например, в аудиокнигах. Даже некоммерческие системы с открытым исходным кодом показывают уровень погрешности около 3–5%. Но спонтанная речь (возникающая в обычном разговоре) отличается неравномерностью и вариативностью, одно и то же предложение может быть произнесено с разной интонацией и скоростью, а бывает, когда два разных слова произносятся одинаково.



Рисунок 2. В таких условиях записывались фонограммы для конкурса CHiME 2018. Шумы, возникающие в подобной ситуации разнообразны: это и звук кипящего масла, и звук текущей из крана воды, и звяканье вилки о тарелку, и прочие звуки, характерные для ужина в кругу друзей. Источник картинки: spandh.dcs

Интенсивные шумы ещё больше усложняют работу, мешают извлечь из звука относящиеся к речи данные. Есть один особый вид шума — реверберация, он возникает, при отдалении источника звука от записывающего устройства. Кроме того, что запись становится тише, оказывается, что и тембр звука изменяется. Этот эффект обусловлен тем, что звук отражается от твёрдых поверхностей и мы слышим не только звук, доходящий до нашего уха напрямую, но и его всевозможные отражения. Самый известный эффект реверберации — эхо, которое возникает, когда различные отражения объединяются во что-то наподобие морских волн, из-за чего и возникает ощущение периодического повторения одного и того же звука. Обычно для чёткого «эха» нужно специальное помещение, однако эффект реверберации можно услышать, даже если просто записать речь на гарнитурный микрофон или микрофон обычного

телефона, положив его в двух метрах от себя. Эффект трудно описать словами, но он хорошо заметен на слух и способен запутать даже самые современные нейронные сети, если не уделить этой проблеме внимания при их обучении.

Наконец, при разговоре нескольких человек недостаточно уметь определять, кто именно говорит в данный момент времени (хоть этого и достаточно, например, при распознавании телефонного диалога), очень часто два или больше людей говорят одновременно и необходимо выделить из звука речь, относящуюся к разным людям.

Команда ЦРТ, занявшая третье место в конкурсе, смогла улучшить показатели базовой системы, предоставленной организаторами, и повысить точность распознавания с 26,7% до 44,5%. Этот результат был достигнут с помощью эффективного сочетания традиционных методов обработки звука, например,

Возникающая в обычном разговоре речь отличается неравномерностью и вариативностью, одно и то же предложение может быть произнесено с разной интонацией и скоростью, а бывает, когда два разных слова произносятся одинаково

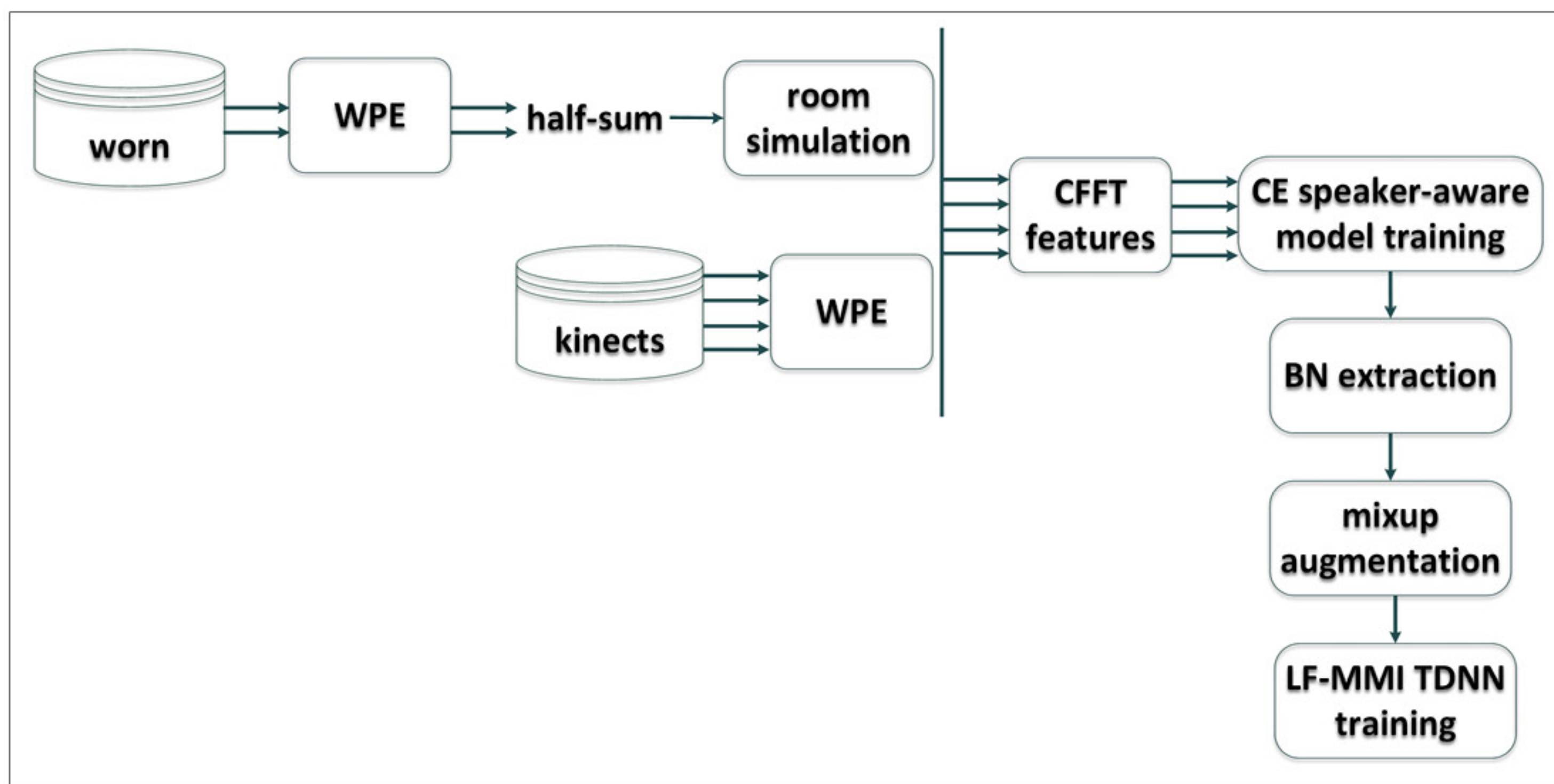


Рисунок 3. Первая система, представленная командой ЦРТ на конкурсе CHIME

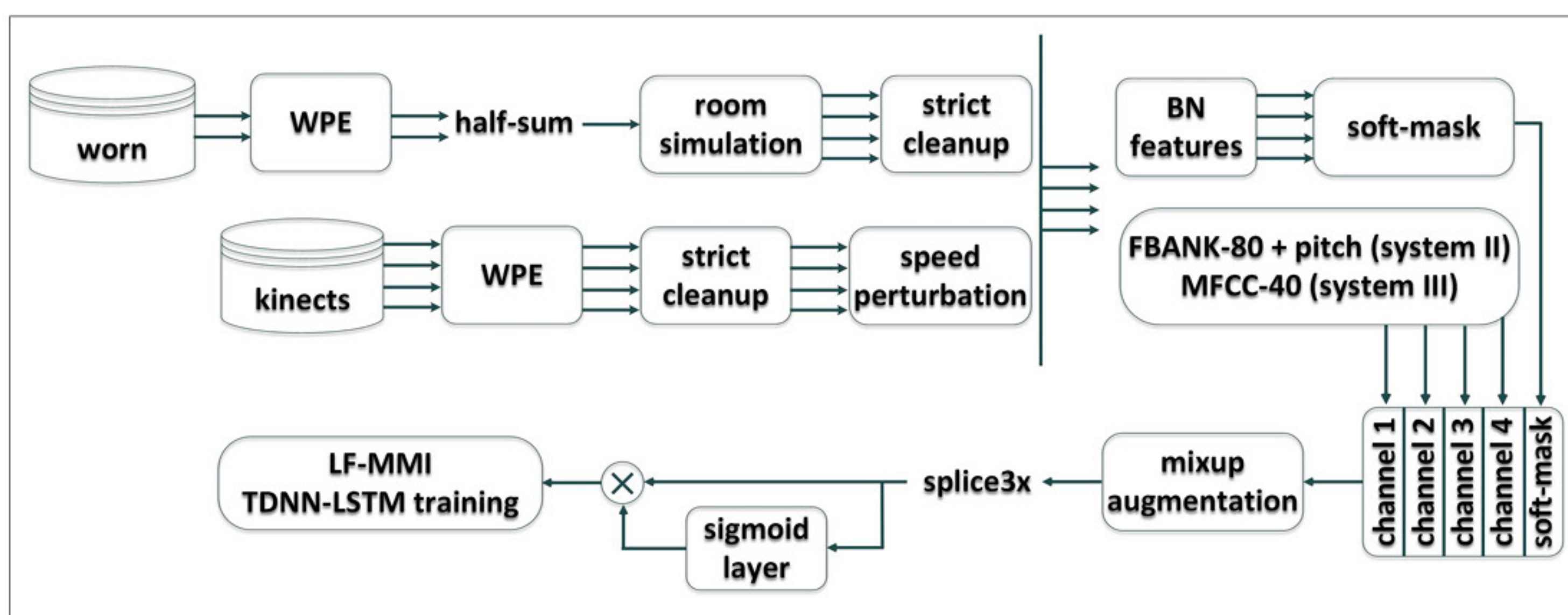


Рисунок 4. Вторая и третья системы команды ЦРТ на конкурсе CHIME

таких, как манипуляции с изменением тембра для подавления эффекта реверберации или наоборот, усиления этого эффекта, различные способы аугментации (наращивания объёма) данных при обучении статистических моделей, объединение результатов распознавания множества различных моделей; а также наших собственных наработок, таких как реализация так называемого «бимформинга» (усиления звука, исходящего с определённого направления за счёт записей с нескольких микрофонов) с помощью нейронных сетей, улуч-

шенная синхронизация между различными записывающими устройствами за счёт анализа речевого потока.

РЕШЕНИЕ ОТ ЦРТ

Мы провели множество экспериментов, в результате которых выделили 4 системы, результаты распознавания которых были объединены на последнем этапе. Схему первой системы можно увидеть на рисунке 3.

При построении всех систем используются двухканальные записи с ушных микрофонов (worn) и четырёхканаль-

ные записи кинектов (kinects), однако обрабатываются они по-разному. Например, в системе, описанной выше, как к ушным микрофонам, так и к кинектам применяется алгоритм WPE, подавляющий реверберацию, а затем к ушным микрофонам применяется алгоритм, который делает ровно наоборот — эмулирует эффект реверберации с учётом описания комнат, предоставленного организаторами конкурса. При этом используется как чистый звук с ушных микрофонов, так и ревербированный.

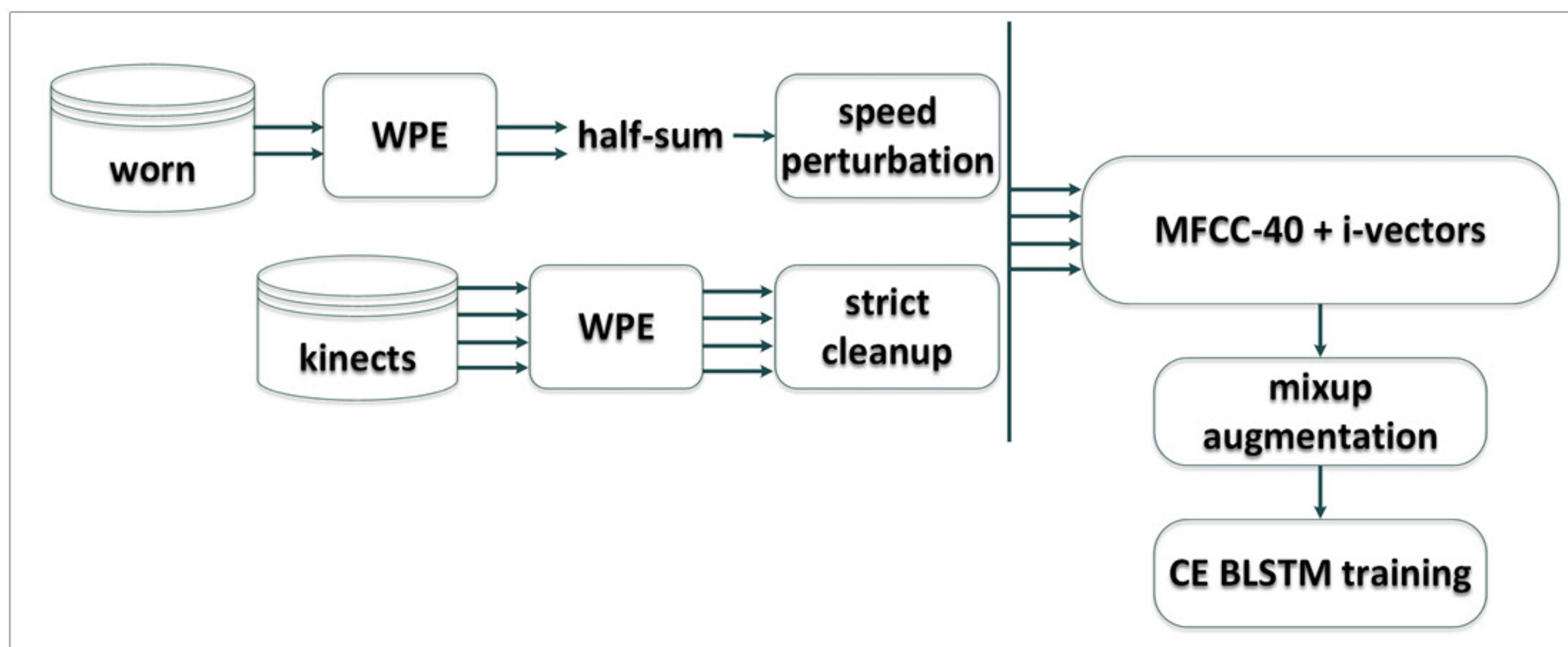


Рисунок 5. Четвертая система команды ЦРТ на конкурсе CHIME

Ещё одна особенность этой модели состоит в том, что в качестве базовых признаков используется сырой комплексный фурье-спектр вместо амплитудного спектра. Кроме того, эта модель обучена отличать дикторов друг от друга на основе информации, предоставленной организаторами.

Представленные на рисунке 4 системы отличаются только используемыми базовыми признаками — повсеместно используемыми «фильтрбанки» и «мел-кепстральные коэффициенты», а также используются так называемые «bottleneck» — признаки, извлечённые первой системой, что позволяет этой использовать информацию о говорящем, которую умеет извлекать и система 1. Наконец, последняя система представлена на Рисунке 5.

Четвертая система использует традиционный i-vector-подход для адаптации к разным спикерам вместо подхода, реализованного в первой системе. Другим важным отличием является способ обучения нейронной сети: в последней системе нейронная сеть учится отличать, какая из фонов (фонема — минимальная речевая единица) произносится на коротком проме-

жутке времени (cross-entropy training). В предыдущих же системах нейронные сети обучаются отличать целые предложения, последовательности фонов (lstm training). Обычно второй способ обучения показывает лучшие результаты, чем первый, однако использование разнородных методов обучения улучшает результаты, полученные из грамотного объединения результатов распознавания нескольких разных моделей.

РАСПОЗНАВАНИЕ РЕЧИ В БАНКАХ

Распознавание речи — востребованная технология в банковском секторе. Она уже успешно применяется для автоматизации контроля качества обслуживания в контактных центрах — в системах речевой аналитики. В то же время оценить, что говорит клиенту операционист или кредитный консультант, зачастую не так просто. Традиционно качество сервиса в офисах банка проверяют с помощью методики «Тайный покупатель», опросов клиентов и сотрудников, личного наблюдения руководителя или выборочного просмотра/прослушивания аудио/видеозаписей (например, с камер наблюдения).

Ключевое отличие дистанционного и офисного обслуживания в том, что в офисе между клиентом и сотрудником обычно нет промежуточного устройства, на котором могла бы оставаться история взаимодействия. Если мы используем в отделении микрофоны и, например, веб-камеры, у нас появляется возможность сохранять записи, но остаётся проблема их обработки. В отличие от телефонной трубки микрофон на столе находится на расстоянии от говорящих, и система распознавания сталкивается с той самой «коктейльной проблемой».

Решив проблему точности распознавания речи на средних микрофонах, мы делаем возможными автоматический анализ 100 % оффлайн-обращений в организацию, контроль соблюдения стандартов и скриптов, улучшение финансовых показателей за счёт повышения эффективности продаж и маркетинговых акций, снижения расходов на тайных покупателей, уменьшение среднего времени обслуживания. Также улучшение качества распознавания позволит использовать средние микрофоны в сфере банковской безопасности — в сценариях автоматического контроля утечек конфиденциальной информации через личные переговоры сотрудников.

Решив проблему точности распознавания речи на средних микрофонах, мы делаем возможными автоматический анализ 100 % оффлайн-обращений в организацию



Дмитрий МИХЕЕВ

технический
директор
ООО «АйТи
БАСТИОН»

КОМУ НА САМОМ ДЕЛЕ НУЖНА СКДПУ НТ В БАНКЕ

ВЫ УЖЕ КОНТРОЛИРУЕТЕ ДЕЙСТВИЯ АДМИНИСТРАТОРОВ. ЧТО ДАЛЬШЕ?

Решение СКДПУ НТ появилось как ответ на возрастающие потребности заказчиков, уже использующих систему контроля действий привилегированных пользователей СКДПУ. Специалисты «АйТи БАСТИОН» при внедрении этого решения в инфраструктуру крупных банков выявили у ответственных за информационную безопасность специалистов острую потребность централизованно контролировать действия администраторов в условиях территориально распределённой инфраструктуры, особенно когда в периметре ИТ-инфраструктуры

работают не только собственные администраторы, но и внешние подрядчики. Кроме того, для финансовых организаций важно не столько устранять инциденты, сколько не допускать их развития: слишком велики потери от любого сбоя.

Для обеспечения именно этой задачи мы создали решение СКДПУ НТ. Фактически это центр анализа действий привилегированных пользователей. Не секрет, что отдельные действия администраторов не могут быть уверенно классифицированы и определены как опасные. Их необходимо анализировать в развитии, с пониманием усло-

вий и причин выполнения — администраторы по роду деятельности обязаны совершать потенциально опасные действия. Кроме того, подготовка и опыт офицеров безопасности могут быть недостаточными для уверенного распознавания потенциально опасных ситуаций при их переходе в нарушения.

Новый программный продукт открывает для заказчиков более широкие возможности: он формирует и поддерживает цифровой профиль пользователя на основании собранных данных, проводит их глубокий анализ, что позволяет выявлять аномалии в работе. Массив данных о типичном поведении каждо-

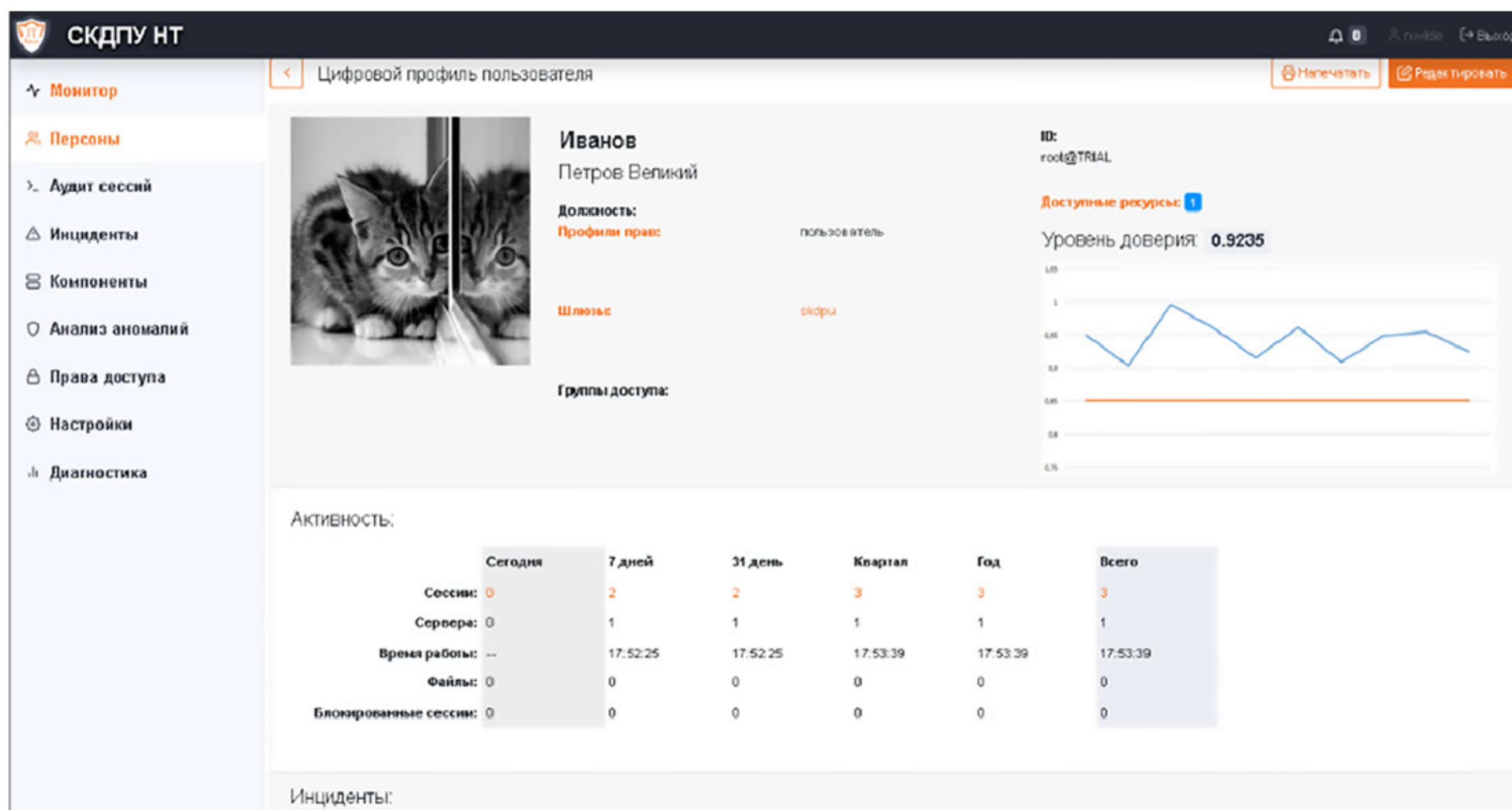


Рисунок 1. Цифровой профиль пользователя

го из администраторов позволяет выделить потенциально подозрительное поведение до наступления возможных серьёзных последствий.

Так кому же на самом деле может быть полезным это решение в банке?

ПОДРАЗДЕЛЕНИЮ ИБ БАНКА

В первую очередь, конечно, ему. Особенно если у банка множество филиалов в разных городах, а ИБ-подразделение одно на всех. Несомненно, «безопасники» примерно знают, чем занимается каждый из администраторов, какая у него сфера деятельности и ответственности. Но в случае инцидента выяснить, что конкретно делал тот или иной привилегированный пользователь в конкретный момент времени, как правило, — недостаточно. Необходимо выяснить порядок развития проблемы, отследить историю изменений, а также проанализировать действия исполнителей работ, которые могли привести к нарушению работы.

СКДПУ НТ позволит провести поиск сессий, в том числе полнотекстовый и параметрический, по настраиваемым параметрам, а также сформировать историю работы с определёнными элементами инфраструктуры. Информация собирается сразу с нескольких источников (платформа СКДПУ/решение Wallix Bastion/ОС Astra Linux). Это позволяет быстро выяснить историю работы с данным целевым устройством — сервером, сетевым оборудованием или приложением. Как следствие, специалист по информационной безопасности сможет быстро сузить поиск возможного нарушителя, а также зафиксировать его действия документально.

ИТ-ДЕПАРТАМЕНТУ

СКДПУ НТ позволяет извлекать события, связанные с активностью конкретного привилегированного пользователя. Анализируя полученные данные,

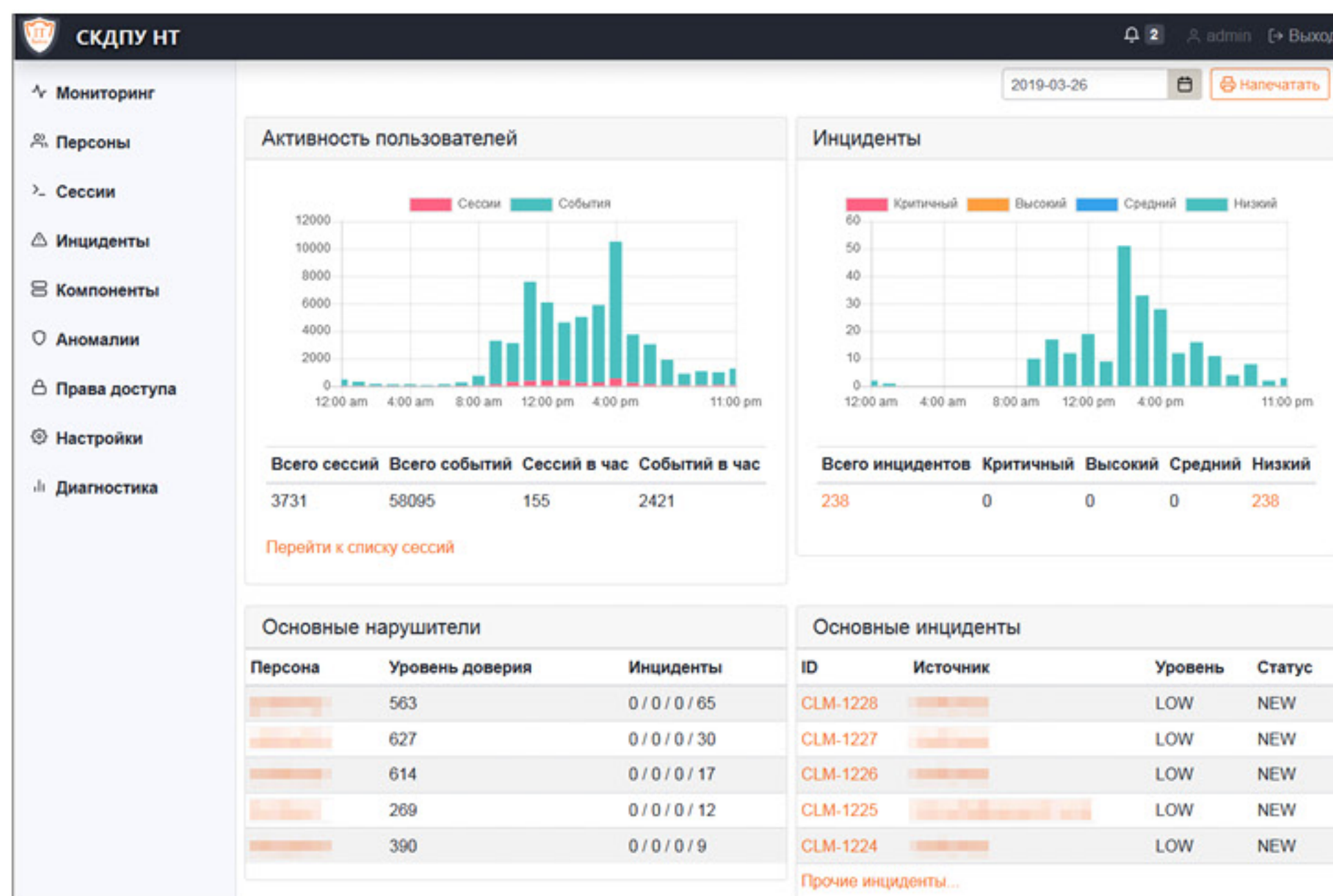


Рисунок 2. Сводный отчет по ситуации за сутки

программа составляет как карту действий, характерных для отдельного администратора ИС во время работы с ИТ-инфраструктурой компании, так и позволяет проанализировать привычные режимы работы, рабочие места и порядок действий. Цифровой профиль сотрудника создаётся именно на основании истории его действий. Информация по каждому из администраторов становится прозрачной: от количества сессий за разные периоды времени до загруженных или полученных с системы файлов.

СКДПУ НТ анализирует различные параметры действий привилегированного пользователя и ищет в этих действиях критичные отклонения от его «стандартного поведения». Примером аномального поведения может стать тот факт, что администратор вошёл в периметр ИТ-инфраструктуры после окончания рабочего дня, или ввёл нестандартные команды, или задавал команды с необычной для себя интенсивностью. Многочисленные признаки

такого рода регистрируются в СКДПУ НТ в виде инцидентов, о них уведомляются администраторы безопасности. Даже если такие ситуации не являются непосредственным нарушением, такие ситуации скорее всего свидетельствуют о наличии тех или иных проблем, заслуживающих внимания.

РУКОВОДСТВУ БАНКОВ

Система контроля действий привилегированных пользователей СКДПУ компании «АйТи БАСТИОН» позволяет банку выполнять требования ФСТЭК России в части защиты удалённого доступа, а также требования Центробанка РФ. В случае, если инцидент на банковской инфраструктуре всё же произошёл, СКДПУ НТ сохраняет в журнале все действия, совершённые администраторами и другими привилегированными пользователями. СКДПУ НТ позволяет выделить потенциальные проблемные ситуации и предоставлять регулярные отчёты о них. Система ведёт анализ постоянно и автоматически выделяет потенциально проблемные ситуации. Нагрузка на специалистов по безопасности снижается, что позволяет им работать эффективнее. А это значит, что в случае возникновения инцидентов специалисты банка смогут выяснить необходимую историю вопроса, разберутся в ситуации и сохранят непрерывность бизнес-процессов.

СКДПУ НТ анализирует различные параметры действий привилегированного пользователя и ищет в этих действиях критичные отклонения от его «стандартного поведения»



Виктор СЕРДЮК
генеральный директор
АО «ДиалогНаука»



Роман ВАНЕРКЕ
технический директор
АО «ДиалогНаука»

ВНИМАНИЕ, РОБОТ-ПЕНТЕСТЕР!

**BAS — НОВЫЙ ИНСТРУМЕНТ ДЛЯ АВТОМАТИЗАЦИИ
ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ**

В эпоху цифровой трансформации компаниям приходится заниматься защитой своих цифровых активов. Однако, как можно гарантировать, что злоумышленники не доберутся до наиболее ценных ресурсов цифрового бизнеса? Необходимо регулярно проводить оценку защищённости своих информационных систем. До недавнего времени для этого использовали либо автоматические сканеры уязвимостей, либо услуги внешних специализированных организаций, которые имитировали проникновение в корпоративную сеть — так называемые пентесты. Не так давно на рынке информационной безопасности появился новый класс решений — BAS (Breach and Attack Simulation), который и будет рассмотрен в данной статье.

ПЕНТЕСТ VS САМООЦЕНКА

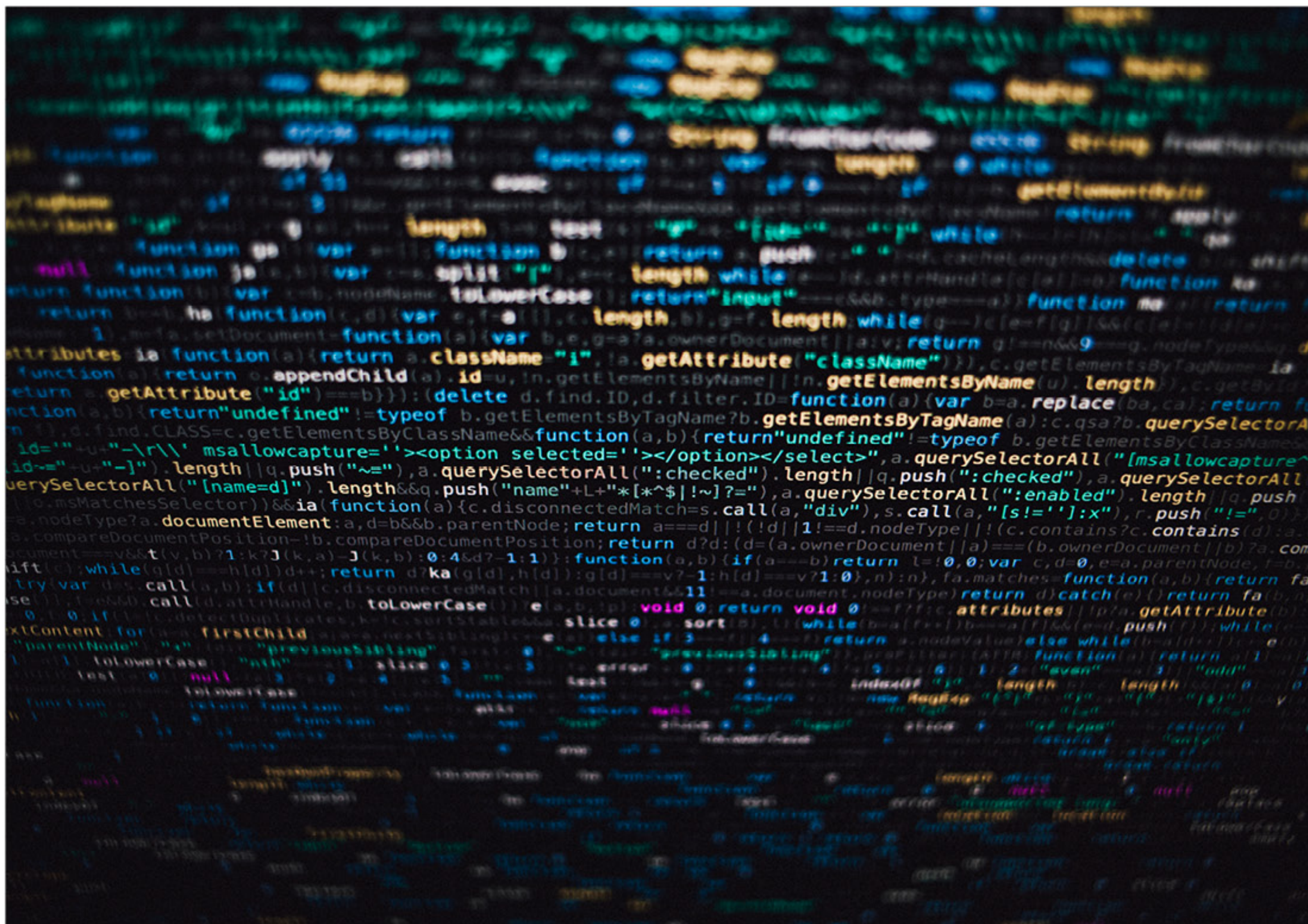
Внутренний аудит с помощью сканера уязвимостей имеет свои преимущества в том, что служба безопасности контролирует этот процесс и не допустит нарушения работоспособности системы во время проведения тестирования. Процесс поиска уязвимостей обычно запускается во время, когда возможный сбой в информационных системах принесёт минимальный ущерб. Впрочем, современные

средства поиска уязвимостей работают достаточно эффективно и не создают чрезмерной нагрузки на сеть и проверяемые узлы, как это было на начальных этапах развития этого класса продуктов. Однако не стоит забывать, что сканеры проверяют только технические уязвимости, не тестируя уязвимости в архитектуре, а также не используют так называемую социальную инженерию. Кроме того, результаты сканирования оценивают те же люди, что и создавали систему, и они не всегда могут адекватно оценить опасность тех или иных уязвимостей.

Внешние пентестеры могут использовать более широкий спектр векторов атак и методов проникновения. Они проверяют не только технические уязвимости, но также могут выявить и архитектурные проблемы, и неправильную работу персонала с внешними обращениями. Пентестеры имитируют деятельность хакеров, что позволяет более адекватно оценить защищённость информационных систем во время реальных атак. При этом пентестеры вынуждены скрываться от систем обнаружения, что позволяет проверить, в том числе, и эффективность работы средств защиты при обнаружении постороннего присутствия — работу сканеров они фиксируют достаточно быстро.

Впрочем, самое главное преимущество пентеста в том, что внешней команде исследователей приходится проходить все те же этапы проникновения, что и реальным злоумышленникам. Им также приходится собирать информацию об используемых программных устройствах, сервисах и базовых компонентах, искать уязвимости в этих компонентах и разрабатывать эксплойты для проникновения с учётом используемых в компании средств защиты. Если первичное проникновение прошло успешно, они, также как и реальные хакеры, изучают внутреннюю сеть компании и стараются получить доступ к ценной информации внутри сети. Полная цепочка действий от изучения до вывода ценной информации получила название Kill chain. Внутренние тестировщики останавливаются на первых двух этапах исследования и проникновения, не тестируя сам процесс реагирования системы защиты на реальную атаку.

В то же время большинство экспертов в безопасности уже говорят о том, что защититься от проникновения невозможно — рано или поздно будет обнаружена уязвимость, которая не учитывалась при самооценке и которую хакеры смогут проэксплуатировать. Поэтому при построении системы защиты не стоит забывать о таких важных элементах системы, как обнаружение втор-



жений, блокирование утечки конфиденциальной информации, проведение расследования инцидентов и совершенствование системы защиты. Именно эти элементы и может протестировать команда пентестеров. А главное, группа специалистов по безопасности сможет получить ценный опыт предотвращения проникновения, реагирования на атаку и проведения расследования — поучаствовать в своеобразных киберучениях.

В принципе, альтернативой внешним пентестерам может являться собственная команда аудиторов, получившая наименование Red Team. Она должна быть независимой и работать по тем же принципам, что и внешние пентестеры, однако в реальности и эта команда нарабатывает собственные приёмы, которые могут оказаться недостаточно универсальными. Поэтому и такая независимая самооценка может дать недостаточно точный результат. Необходимо также отметить, что использо-

вание собственной команды пентестеров, требует значительных финансовых затрат, что могут позволить себе только компании со значительными бюджетами на обеспечение информационной безопасности.

BAS-АВТОМАТИЗАЦИЯ

Для автоматизации работы пентестеров начали появляться инструменты, которые позволяют роботизировать все этапы проведения теста на проникновение, точнее, всей цепочки kill chain. Эти инструменты получили наименование Breach and Attack Simulation (BAS). От сервисов удалённого тестирования на уязвимости — так называемых облачных сканеров — данные решения отличаются тем, что так же как и при пентесте проверяют все вектора возможной атаки и позволяют службам ИБ предприятия на регулярной основе проверять эффективность применяемых средств защиты информации.

Предполагается, что BAS-платформы выполняют следующие функции:

- ♦ исследование / рекогносцировка. BAS-решение симулирует все методы получения первичной информации для проникновения, которые используют хакеры. Как правило, для этого используется сканирование внешнего периметра компании для выявления всех возможных узлов и сервисов, через которые потенциально может быть реализована атака.

- ♦ Проникновение. На этапе проникновения сканеры тестируют периметр на уязвимости, как это делают и другие средства поиска уязвимостей. Однако BAS-решения проводят также и имитационные тесты, например, с помощью специальных фишинговых рассылок с вредоносным кодом. Этот этап позволяет оценить не только уровень осведомлённости сотрудников компании, но и эффективность работы шлюзов безопасности, которые должны обнаружить вредоносный код. Аналогичным

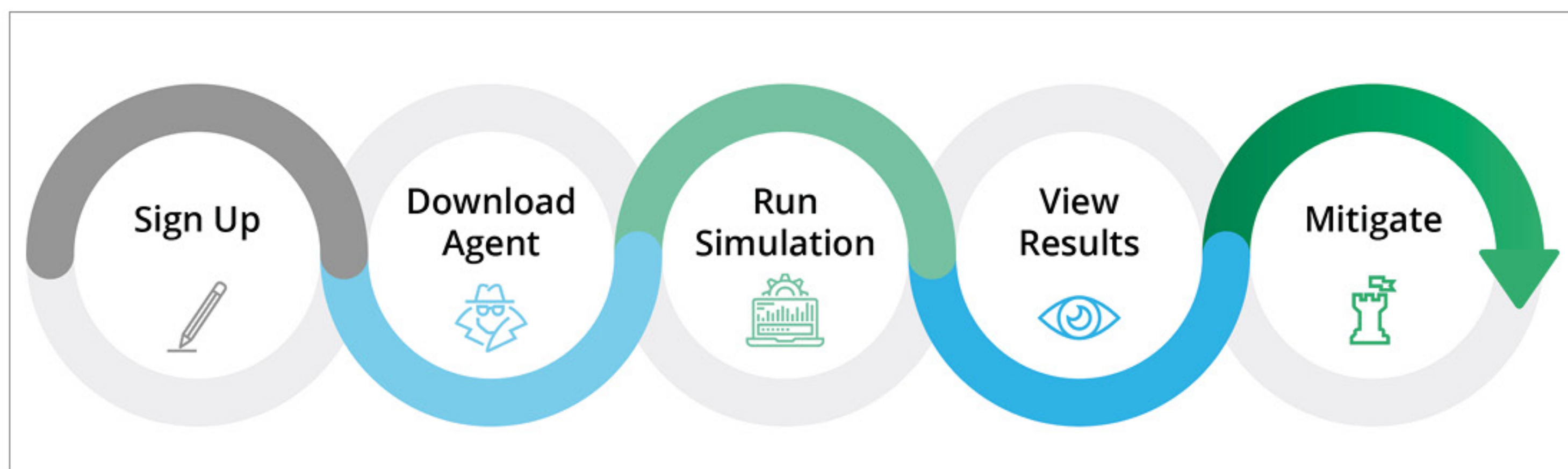


Схема работы сервиса Cymulate. Источник: <https://cymulate.com/how-it-works/>

образом тестируется и использование веб-браузеров на возможность проникновения. С помощью ссылок на специальным образом скомпрометированные сайты BAS-решение проверяет уязвимости в веб-браузерах, а также шлюзовых систем безопасности.

- ♦ Внутреннее исследование. Следующим этапом проникновения является закрепление в системе, для чего хакеры взламывают рабочие станции и сервера, устанавливая в них модули для удалённого управления. BAS-решение тестирует защиту конечных точек — антивирусов и EDR, имитируя при этом действия злоумышленников для перемещения внутри корпоративной сети с использованием стандартных средств удалённого администрирования, входящих в состав операционных систем. Для этого могут использоваться специальные программные агенты, устанавливаемые на рабочие станции пользователей.

- ♦ Кража конфиденциальной информации. Заключительным этапом хакерской атаки обычно является вывод конфиденциальной информации за пределы корпоративной сети. Поэтому BAS-решения также пытаются передать вовне корпоративной сети обнаруженную информацию, на которую DLP должна среагировать. Таким образом, в этом случае тестируется эффективность DLP-систем в части обнаружения и блокирования попыток утечки конфиденциальной информации. Причём в качестве каналов утечки используются не только стандартные векторы, такие как Web-почта или HTTP, но и скрытые, типа DNS- или ICMP-VPN.

Таким образом, BAS-решения автоматизируют проверку не только уязвимостей в используемом компанией ПО и оборудовании, но и организует своеобразные учения для служб информационной безопасности, в рамках которых появляется возможность отработать процедуры реагирования на различные этапы хакерских действий со стороны сотрудников службы информационной безопасности.

На сегодняшний день на рынке уже представлен целый ряд продуктов, относящихся к категории BAS-решений. Одним из примеров такого решения является сервис Cymulate, который позволяет реализовать каждую из перечисленных выше проверок через сеть Интернет. При этом часть проверок осуществляется удалённо, а для некоторых тестов требуется установка агента в корпоративной сети компании. Результаты работы сервиса предоставляются клиентам в виде отчётов, которые можно использовать для совершенствования своей системы защиты.

Сервис Cymulate включает в себя следующие вектора атак для тестирования системы защиты организации:

- ♦ Immediate threat alert assessment — регулярно тестирует периметр корпоративной сети с использованием актуальных на момент тестирования угроз;
- ♦ Email security assessment — проверяет работу средств защиты, контролирующих электронную почту;
- ♦ Web gateway assessment — тест веб-фильтра и других компонентов защиты, контролирующих протокол HTTP/HTTPS;

- ♦ Lateral movement assessment — тестирование внутренних средств сегментирования и межсетевого экранирования корпоративных сетей;

- ♦ Endpoint assessment — проверка работы средств защиты, установленных на рабочих станциях и серверах;

- ♦ Data exfiltration assessment — проверка для систем DLP;

- ♦ Phishing assessment — проверяет реагирование сотрудников компании на фишинговые сообщения, а почтовые шлюзы — на защиту от массовых рассылок подозрительной корреспонденции;

- ♦ SOC/SIEM simulation — комплексное тестирование на проверку и отработку действий сотрудников служб реагирования на инциденты.

Таким образом, сервис Cymulate предлагает полный спектр проверок, относящихся к категории BAS, причём без покупки дополнительного оборудования и программного обеспечения. Сервисы предоставляются по модели подписки через Интернет с помощью бесплатного агента для управления процессом тестирования.

Аналитики компании Gartner, которые ввели в обиход термин BAS, надеются, что инструменты данного класса постепенно дополняют услуги «ручных» тестов на проникновение, которые часто не дают общей картины защищённости корпоративной сети. Использование инструментов данного класса позволит на регулярной основе получать информацию о реальном уровне защищённости организации от внешних и внутренних угроз.



Максим КСЕНОФОНТОВ
ведущий инженер ДИБ АМТ-ГРУП

ЧТО? ГДЕ? КУДА?

В ВАШЕЙ СЕТИ

Пока локальная сеть состоит из десятка устройств, её схему и правила межсетевых экранов (МСЭ) может без усилий запомнить один сетевой администратор. По мере роста сети в неё добавляются новые устройства, зачастую от других производителей, появляются различные серверы управления, системы безопасности и пр. Хороший вариант, если в этом процессе удалось сохранить чёткое и задокументированное понимание структуры сети и не потерять её управляемость. В ином случае администраторы и пользователи начинают сталкиваться с проблемами, связанными со слабой управляемостью и отсутствием понимания структуры сети. Далее будут разобраны три довольно распространённых случая, характеризующих такую проблему.

Случай 1: Заявка на открытие сетевого доступа открывается слишком долго (иногда неделю или больше)

Довольно распространённая проблема: SLA не выполняется, сроки сгорели, бизнес-пользователи не получили вовремя необходимый доступ, а сетевой администратор все ищет тот самый последний МСЭ, который блокирует почти открытый доступ.

В моей практике были случаи, когда заявки на доступ открывались до двух недель: в результате доступ был открыт, а автору заявки он уже был не нужен, т.к. к этому времени он уехал с объекта, где требовался доступ.

Самая распространённая причина такой задержки — то, что администратор сети не может сразу определить, по какому маршруту должен пойти трафик и соответственно не знает, где какие правила создавать. В итоге действия сводятся либо к открытию доступа везде, что увеличивает риски ИБ, либо к вдумчивому изучению таблиц маршрутизации, что увеличивает сроки исполнения заявки.

Для решения подобных проблем существуют специальные системы управления доступами МСЭ. Одной из таких систем является Tufin Orchestration Suite. Tufin собирает конфигурации и правила фильтрации с сетевых L3-устройств и МСЭ, анализирует их и строит полные маршруты прохождения трафика.

Функционально Tufin состоит из следующих компонентов:

1. SecureTrack, собирающий и анализирующий конфигурации МСЭ;

2. SecureChange, управляющий заявками на доступ;

3. SecureApp, управляющий приложениями в сети.

Соответственно, сетевой администратор может использовать SecureTrack для того, чтобы построить карту прохождения трафика. Строится она довольно просто: необходимо задать источник, назначение и используемый порт. На рисунке 1 приведён пример такого запроса.

После получения подробной информации о маршруте прохождения трафика администратору сети остаётся только внести изменения в конфигурацию на соответствующих МСЭ. Это можно сделать самостоятельно или доверить автоматизации. Для этого в Tufin есть компонент SecureChange. Он может выступать как самостоятельной системой управления заявками, так и интегрироваться с существующей Service Desk системой. В любом случае SecureChange позволит определить МСЭ, на которых

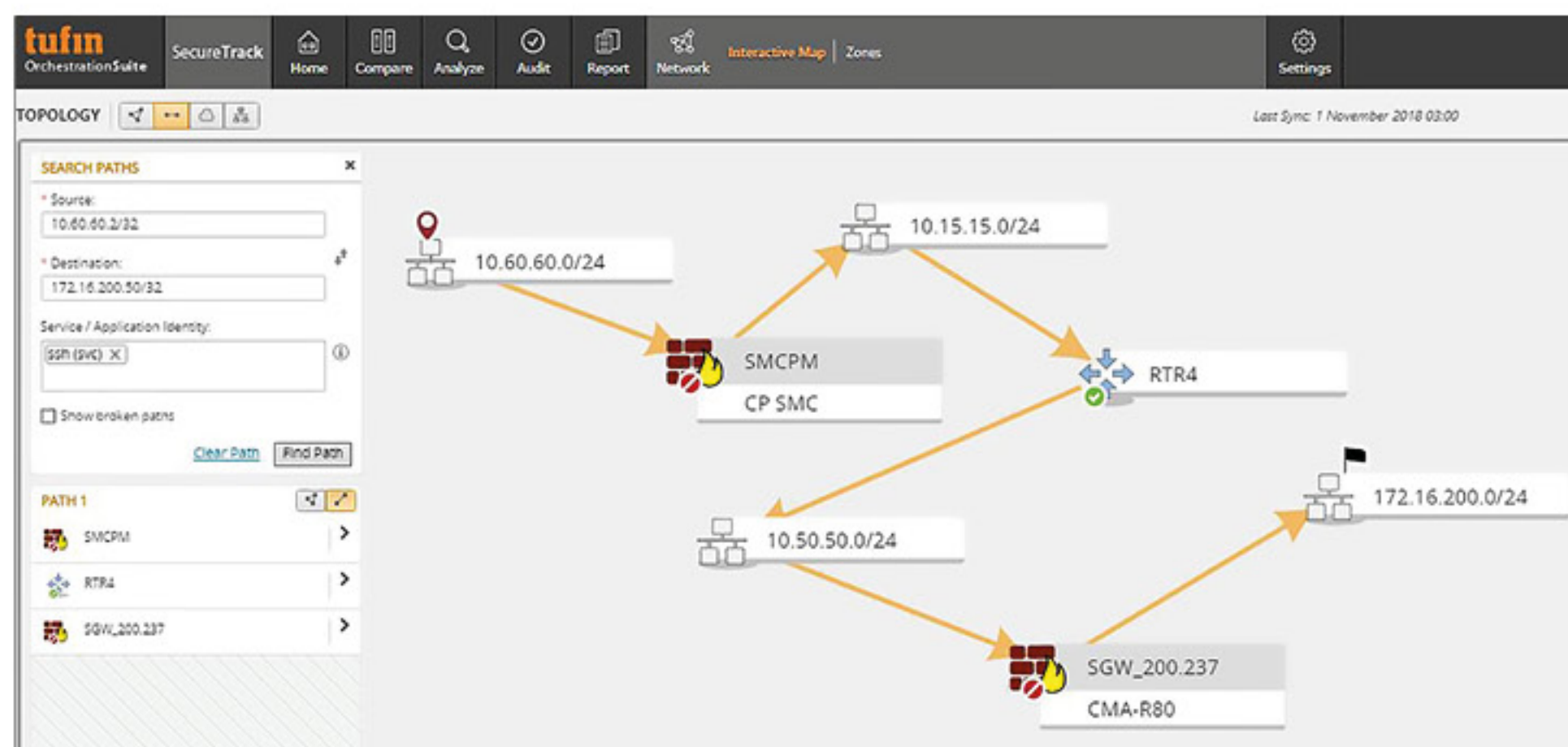


Рисунок 1. Запрос на карту прохождения трафика

требуется провести изменения, характер необходимых изменений (в чело-
векочитаемом представлении и в виде
готовых команд для ввода в интерфей-
се), риски этих изменений, а также мо-
жет сам провести все необходимые из-
менения и проверить их корректность.

Таким образом, за счёт дополнитель-
ной автоматизации ряда задач Tufin
может сократить время обработки за-
явки во много раз (вплоть до несколь-
ких минут).

Кроме того, у системы есть ряд при-
ятных особенностей:

- ♦ проверка требуемого заявкой до-
ступа и закрытие заявки, если доступ
уже есть;
- ♦ возможность делать ревизию пра-
вил на предмет их необходимости че-
рез определённое время;
- ♦ возможность провести полную ре-
визию правил МСЭ на предмет их акту-
альности, корректности и рисков;
- ♦ механизм добавления своих поли-
тик безопасности для предварительной
проверки рисков открытия доступов
(например, запрет доступа из DMZ_1
в DMZ_2 будет закрывать заявки на от-
крытие такого доступа, как несоответ-
ствующие политике ИБ).

**Случай 2. Владельцы бизнес-при-
ложений не могут явно управлять не-
обходимыми им сетевыми доступами**
Владельцы и администраторы биз-
нес-приложений (БП) в своей работе
обычно не оперируют конкретными
требованиями к настройке МСЭ: им
важен доступ, например, от этого сер-
вера к этой базе данных, и не важно,
как пойдёт трафик. Зато важно, что-
бы между хостами его БП не пропадала
сетевая доступность. Довольно не-
приятная ситуация, если приложение
вдруг перестало работать из-за сетевой

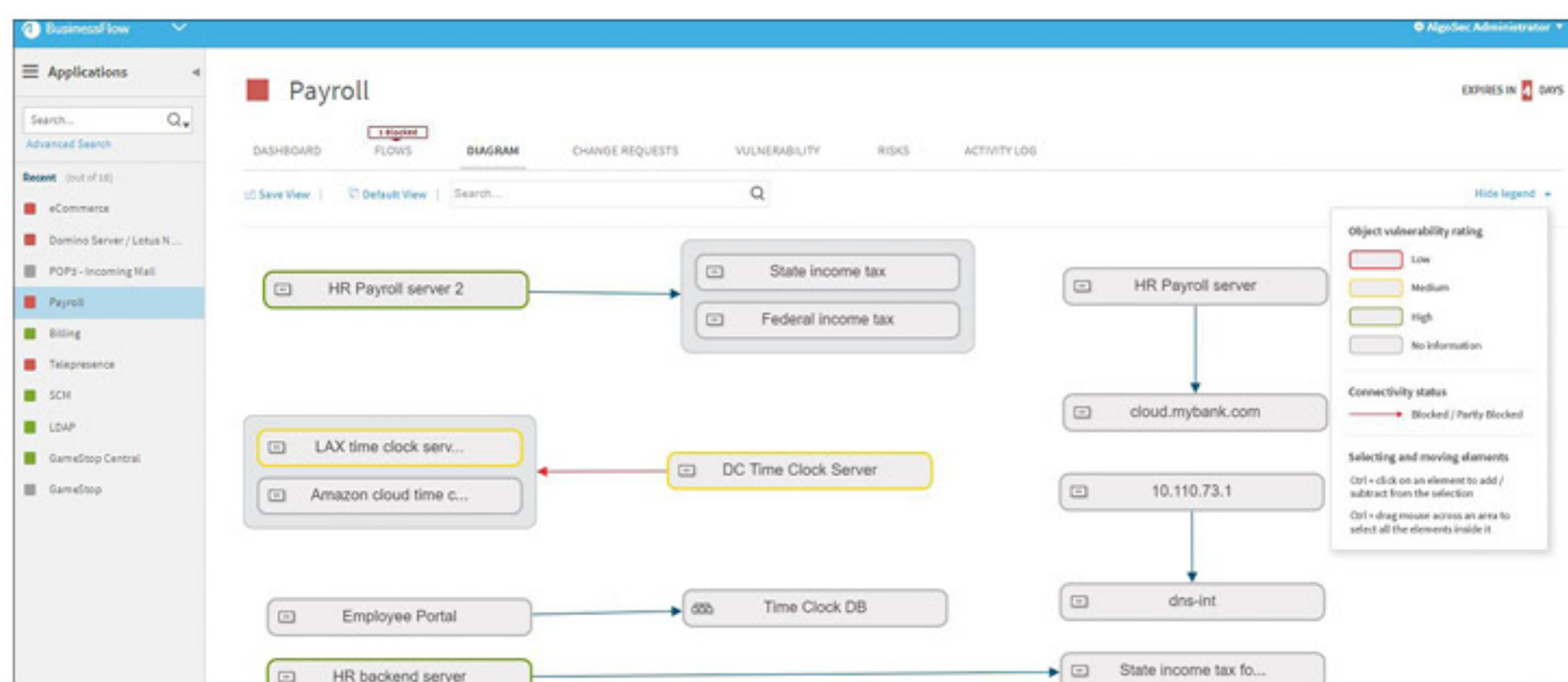


Рисунок 2. Приложение в BusinessFlow

недоступности, и владелец БП не ви-
дит, между какими хостами блокиру-
ется трафик. Для решения проблемы
администраторам сети обычно требу-
ется повторно определить требования
приложения к сетевым доступам. В та-
ком случае проблема может быть реше-
на в приемлемые сроки, если на ИТ-си-
стему есть паспорт или технические
требования к сети. Иначе, если подоб-
ных документов нет или они неактуаль-
ны (например, один из серверов пере-
ехал на другой ip-адрес), то проблема
восстановления работы приложения
может стать очень трудоёмкой или по-
требовать открытия слишком широких
правил на МСЭ.

Решение подобных проблем также
относится к задачам систем управле-
ния доступами МСЭ. Рассмотрим ре-
шение подобной проблемы на приме-
ре другой системы подобного класса,
а именно Algotsec Security Management
Solution.

Algotsec, как и Tufin, имеет три функ-
циональных модуля (три с половиной,
если считать AutoDiscovery):

1. Firewall Analyzer, содержащий
в себе всю логику анализа configura-
ций и политик МСЭ;

2. FireFlow, управляющий заявками
на изменение и обеспечивающий авто-
матическое применение изменений;

3. BusinessFlow с компонентом
AutoDiscovery, обеспечивающий поиск
и обнаружение в трафике приложений
и управляющий ими.

Нужно отметить, что модуль Auto-
Discovery является уникальным отлич-
ием от всех остальных подобных систем.
Он позволяет искать трафик приложе-
ний в копии сетевого трафика или в Net-
Flow, благодаря чему нет необходимости
вручную прописывать приложения
и его сетевые потоки, необходимо про-
сто направить трафик на AutoDiscovery.

AutoDiscovery автоматически может
выявить приложение и его сетевые по-
токи, которые можно будет в дальней-
шем импортировать в BusinessFlow.
В BusinessFlow же этими приложения-
ми можно будет уже управлять. Пред-
ставление типичного приложения при-
ведено на рисунке 2.

Среди множества функций Buiness-
Flow можно выделить наиболее инте-
ресные:

- ♦ контроль сетевой доступности меж-
ду хостами приложения с автоматиче-
ским созданием заявки, если такого до-
ступа нет;
- ♦ возможность миграции хостов
на другие ip-адреса с автоматическим
созданием и отслеживанием заявки
на изменение доступов;
- ♦ возможность видеть риски прило-
жений после интеграции со сканерами
уязвимостей (например, с MaxPatrol);
- ♦ возможность увидеть влияние кон-
кретного МСЭ на затрагиваемые при-
ложения (какие приложения «упадут»,
если мы перезагрузим данный роутер);

*Модуль AutoDiscovery является уникальным
отличием от всех остальных подобных
систем. Он позволяет искать трафик
приложений в копии сетевого трафика
или в NetFlow, благодаря чему нет
необходимости вручную прописывать
приложения и его сетевые потоки*

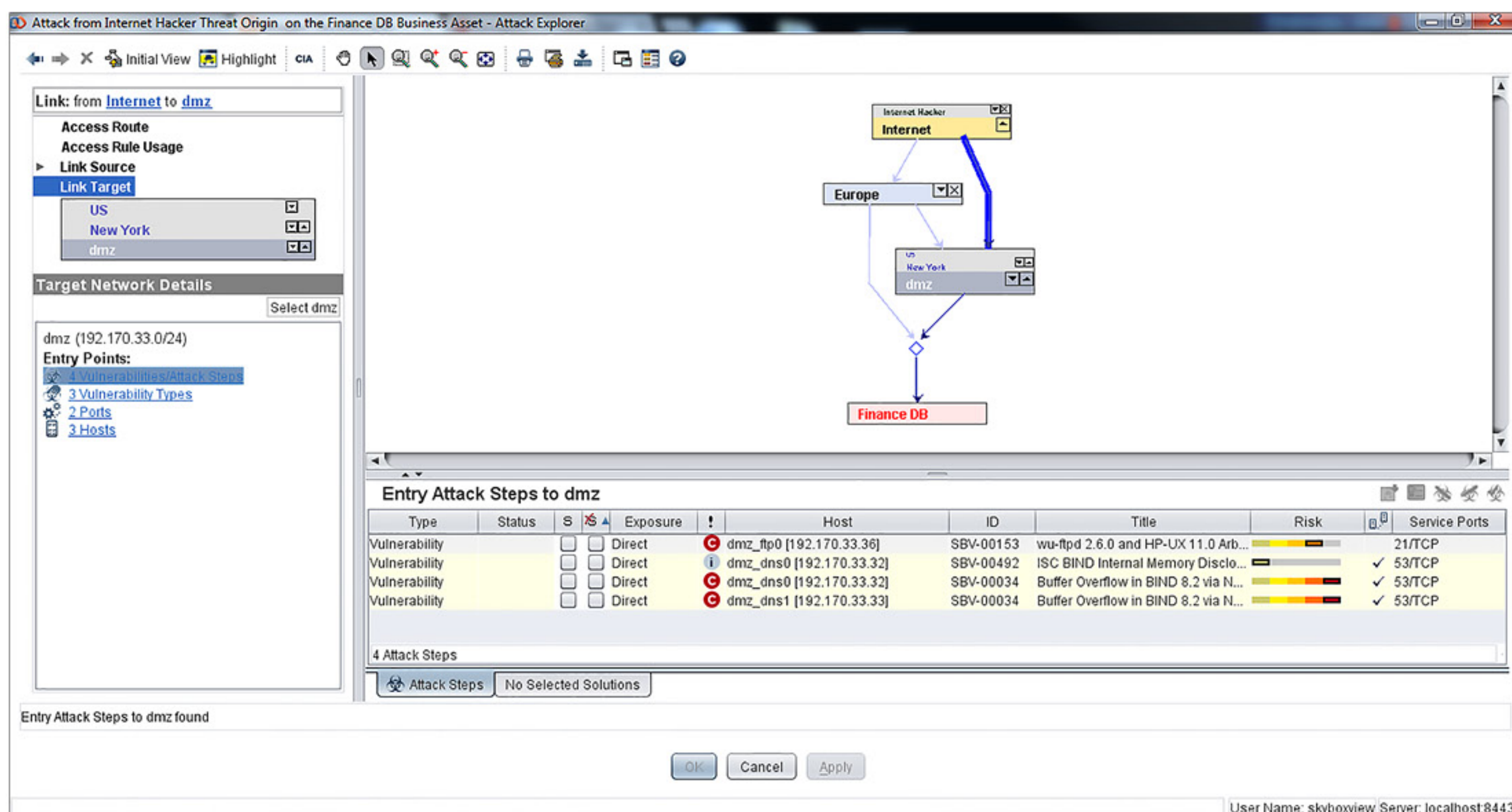


Рисунок 3. Пример вектора атаки

♦ возможность автоматической трансляции сетевых требований БП в набор правил для всех задействованных МСЭ.

По итогу, владелец приложения получает удобный и понятный интерфейс управления своими приложениями, а сетевой администратор облегчает свою работу, поскольку BusinessFlow автоматически транслируют требования типа «от этого сервера в этой СУБД» в набор команд для МСЭ и создает заявку в FireFlow.

Случай 3. Сканер уязвимостей сканирует хосты по расписанию раз в месяц, и информация об уязвимостях имеет месячную актуальность

Обычно сканер уязвимостей проводит сканирование с определённой частотой. Это связано с тем, что он не может сканировать хосты всё время из-за ограничений по вычислительным ресурсам и утилизации пропускной способности канала. В итоге каждая компания настраивает частоту сканирования по своему усмотрению, но обычно раз в месяц или в квартал. В итоге информация об уязвимостях устаревает довольно быстро и не обновляется до следующего сканирова-

ния. Это увеличивает риски эксплуатации новых уязвимостей, про которые не было известно при последнем сканировании.

На текущий момент Skybox Security Suite — одна из немногих систем, которая может справиться с этой проблемой. Skybox относится к классу систем управления доступами и уязвимостями. Он также, как и Tufin и AlgoSec, получает информацию о конфигурации МСЭ и может ими управлять, но, кроме этого, помогает управлять уязвимостями: он имеет специальный модуль, предназначенный для отслеживания векторов атак злоумышленников и расстановки приоритетов при закрытии уязвимостей.

В Skybox присутствуют следующие функциональные компоненты:

1. Firewall Assurance — получение конфигураций МСЭ и их анализ;
2. Network Assurance — анализ сетей и сетевой доступности;
3. Change Manager — управление изменениями на МСЭ;
4. Vulnerability Control — управление уязвимостями.

Последний компонент Vulnerability Control — это то, что отличает Skybox от других систем подобного класса.

Он позволяет осуществлять управление уязвимостями и контроль векторов атак.

Для своей работы Skybox получает информацию об уязвимостях от сканеров уязвимостей, информацию об используемых версиях ПО и ОС и, ориентируясь на эти данные в режиме реального времени, определяет актуальные уязвимости для каждого хоста. Далее он может с учётом информации об открытых доступах на МСЭ строить сценарии атаки и оценивать риски. Пример такого маршрута атаки изображён на рисунке 3.

* * *

Очевидно, что если доступ на МСЭ для реализации какой-либо уязвимости закрыт, то работа с ней становится менее приоритетной. Это главное различие в подходе к управлению уязвимостями по сравнению с классическими сканерами уязвимостей, которые требуют немедленно закрытия всех обнаруженных уязвимостей. В результате это серьёзно сокращает трудозатраты на управление ИБ при том же уровне защищённости.



Леонид БОНДАРЕНКО
директор департамента
поддержки продаж
ООО «Сикрет Технолоджис»

КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ

ЛУЧШИЕ ПРАКТИКИ ФАЙЛОВОГО ОБМЕНА

В корпоративной среде для обмена файлами используются разные решения: электронная почта, FTP-серверы, Sharepoint-серверы, системы электронного документооборота, файлообменники в Интернете, публичные облачные хранилища, специализированные решения для файлового обмена и т.д. Каждое из них имеет своё назначение и особенности. Далее рассмотрим принципы обмена файлами, которые, по нашему мнению, должны соблюдаться любой компанией, а также те лучшие практики, которые мы выработали в нашей деятельности. Постараемся выяснить, какие из этих решений действительно подходят для выполнения задач обмена корпоративными файлами.

1. Обеспечение передачи необходимого объёма информации

Сначала очевидное: если в рабочем процессе пользователям необходимо обмениваться файлами, в том числе большими, это нужно обеспечить. При этом нужно учитывать, что с каждым годом информации становится всё больше и размеры файлов увеличиваются.

Однако, как бы ни было очевидно это заявление, так делается не всегда. Наверняка всем знакомо сообщение следующего содержания: «Размер вложения превышает допустимый сервером пре-

дел. Попробуйте разместить файл в общей папке и отправить ссылку на неё».

В одной компании, где я работал, стояло ограничение всего в 10 МБ. И таких компаний достаточно. То есть передача больших файлов обеспечивается далеко не всегда.

2. Квотирование

В то же время объём передаваемых файлов ограничивать нужно. Для того чтобы инструмент обмена со временем не превратился в «файловую помойку», а пользователи не требовали добавления доступного им места.

Квотировать нужно как общий объём пространства, доступного пользователю, так и размер передаваемого файла. Но при этом не нужно забывать про первый пункт и квотировать объёмы, исходя из бизнес-процессов и реальной рабочей необходимости.

3. Ограничение срока жизни и доступности файла

Инструмент файлового обмена должен использоваться именно для обмена, а не как средство хранения. Чтобы этого достигнуть, нужно автоматически удалять файлы после заданного срока жизни.

Также, при предоставлении доступа к файлу, необходимо ограничивать период его доступности для получателя и количество скачиваний файла, если он предоставляется по ссылке.

4. Ограничивать передачу файлов по типу

Следующее, что нужно делать, — ограничивать передачу файлов по типам. Нужно ограничиваться только теми типами файлов, которые используются в работе. Благодаря этому, во-первых, не будут попадать файлы, не используемые для бизнеса, и корпоративные средства перестанут использоваться в личных целях. Во-вторых, нужно ограничить передачу файлов потенциально небезопасных форматов, например, исполняемых файлов.

Нужно понимать, что различные отделы по роду своей деятельности обмениваются различными типами файлов. Поэтому разные белые или чёрные списки типов файлов должны назначаться на разные группы.

Ещё нужно иметь в виду, что простой проверки расширения в имени файла недостаточно, такая проверка легко обходится переименованием файла. Нужно определять тип файла по его заголовку и структуре, независимо от того, какие буквы написаны в его названии после точки.

5. Чёткое определение участников обмена

При файловом обмене необходимо ограничивать роли пользователей: внутренние пользователи организации

и внешние по отношению к организации пользователи — контрагенты.

Контрагентам мы по умолчанию доверяем меньше. Поэтому процесс инициации обмена файлами должен лежать на пользователе. Так, если пользователю нужно что-то получить от контрагента, он должен запросить файл у контрагента. Без такого запроса контрагент не должен передавать пользователю ничего. Но и внутренний пользователь не должен иметь возможности передать файл кому угодно. Перечень контрагентов должен быть конечным.

Если список внутренних пользователей можно получить, например, с помощью синхронизации с корпоративным каталогом Active Directory, то добавление контрагентов должно согласовываться. При этом иногда требуется чтобы согласование было многоэтапным.

6. Полный аудит событий передачи данных

Для обеспечения разбора инцидентов передачи файлов нужно знать: кто, когда, кому, что передавал, какие проверки безопасности прошёл файл, кто файлы в систему загрузил, кто из системы скачал.

Кроме этого должны фиксироваться все операции, выполняемые администраторами по настройке системы, события входов/выходов. Традиционно в каждом событии должно фиксироваться время, субъекты, объекты и действия.

При этом события должны передаваться в системы лог-менеджмента и в системы управления событиями информационной безопасности (SIEM), откуда их проблематично удалить или изменить.

7. Антивирусная проверка

Все файлы, получаемые и отправляемые, должны быть обязательно проверены на вредоносность. При этом нужно учитывать, что современное вредоносное ПО имеет массу возможностей по обходу традиционных антивирусов, например, полиморфизм или вообще являются 0-day. Для детектирования таких вирусов используются решения динамического анализа файлов в т.н. песочницах.

Таким образом, для эффективной антивирусной защиты хорошей практикой будет отправка файла на анализ в «песочницу».

8. Использование защищённых протоколов передачи данных

Корпоративная информация требует защиты. Использование защищённых протоколов передачи по умолчанию — минимальный необходимый уровень защиты информации при передаче. Это также обеспечивает защиту передаваемых аутентификационных данных (логин/пароль).

Для защиты передачи могут быть использованы протоколы SSL/TLS, но и их следует правильно настраивать.

9. Шифрование файлов, содержащих конфиденциальную информацию при передаче

Если канал нужно шифровать в любом случае, то для защиты критичных конфиденциальных данных необходимо обеспечивать шифрование самих файлов. При этом, если используется симметричная криптография, то ключ должен генерироваться системой с политиками минимальной длины и сложности. Также нужно озаботиться безопасностью хранения и доставки ключевой информации.

Шифрование файлов должно осуществляться средствами самой системы, чтобы при передаче его можно было проверить.

10. Ограничивать доступ к файлам обслуживающего персонала

Злоумышленником может оказаться любой человек, в том числе и сотрудник, обслуживающий информационную систему передачи файлов. Нужно соблюдать принципы минимальных привилегий, выполнять разграничение доступа к директориям, в которых хранятся файлы и шифровать хранимые файлы.

11. Проверять содержимое файлов системами контроля утечек данных

Любая система передачи файлов — потенциальный канал утечки, который тоже нужно контролировать. Отправляемые файлы должны передаваться

на анализ в специализированные системы контроля утечек данных (DLP) и от этих систем, на основании настроенных в них политик, должен возвращаться вердикт, можно или нельзя отправлять файл за пределы контролируемого периметра.

12. Не передавать файлы, безопасность которых нельзя проверить

Если передаваемый или получаемый файл нельзя проверить описанными выше методами (файл, например, упакован в запароленный архив), то его передачу нужно блокировать, сам файл помещать в карантин, а факт попытки передачи фиксировать в журнале событий.

13. Не использовать публичные облака, а тем более файловые обменники

Зачастую пользователи за неимением корпоративной альтернативы используют сервисы типа DropBox, Яндекс.Диск или в худшем случае обменники в Интернете.

Публичное облако несёт в себе ряд существенных рисков: компрометация аккаунта, взлом сервиса, изменение условий использования: блокировка аккаунта, удаление информации, индексация информации поисковыми и т.д.

14. Использовать отечественные решения

Использование отечественного решения — это технологическая независимость, локальная техническая поддержка и быстрая реакция вендора, который находится «на расстоянии вытянутой руки».

* * *

Данные принципы не так-то легко соблюдать, не имея специализированного решения. В портфеле компании Secret Technologies имеется решение собственной разработки — Secret Cloud Enterprise, которое помогает компаниям придерживаться описанных принципов при обеспечении файлового обмена с сохранением должного уровня информационной безопасности.



Александра БЯЛЬКИНА
руководитель департамента
развития продуктов,
заместитель генерального
директора Cross Solutions
(АО «Кросс Технолоджис»)

FORENSICS FOREVER!

ПЕРЕОСМЫСЛИВАЯ ВОЗМОЖНОСТИ ИТ-КРИМИНАЛИСТИКИ

Независимо от того, в каких компаниях работают специалисты (государственных или коммерческих), на каких позициях (ИТ-специалист, аналитик, юрист), при выполнении различных задач они сталкиваются с необходимостью обработки больших объёмов данных. Сфера цифровой криминалистики ощущает на себе влияние цифровизации гораздо сильнее, чем можно себе представить. При проведении расследований, в том числе для предоставления их результатов в качестве доказательной базы в суде, важно понимать, какие подходы, направленные на поиск релевантных предмету расследования доказательств, существуют для работы с огромными массивами данных. Выявление преступлений в цифровой сфере, мошеннических схем и прочих ситуаций, сбор доказательств, а также подготовка юридически значимого заключения требует вовлечения разнообразных квалифицированных специалистов с разными целями.

РЕАЛИИ ЖИЗНИ

Мы сейчас живём в эре глобальной цифровизации. Объём электронной информации растёт в среднем на 40–50% в год, что можно наглядно проиллюстрировать статистикой по увеличению объёмов жёстких дисков, используемых в ПК. Отдельный вопрос — смартфоны, как высокопроизводительные компьютеры с возможностью хранения десятков гигабайт информации (только на аппарате). Если на одного сотрудника в компании приходится, к примеру, два ПК (личный и корпоративный)

и два телефона (личный и корпоративный), то при расследовании эксперту потребуется обработать 1–2 терабайта данных. А если речь идёт о 5–10 сотrudниках или о проведении крупномасштабных расследований с подключением внутрикорпоративных почтовых серверов, хранилищ данных?

Объём информации не был бы критичен, если бы мы могли осуществить процесс ее сбора и анализа за приемлемое время и с гарантией целостности и полноты. И если решение вопросов скорости сбора и обработки стандартно упирается в мощность оборудования и используемые технологии распределённых вычислений, то вопрос целостности и полноты собранных данных лежит в плоскости квалификации кадров.

Итак, суммируем современные проблемы:

- ♦ задержки первичной экзаменации компьютеров и других носителей данных (многообразие оборудования, операционных систем, типов файлов, типов информации);
- ♦ несоответствующая задачам производительность отдельных рабочих станций;
- ♦ нехватка компетентного персонала, необходимость привлечения сотрудников с компетенцией в различных направлениях (ИТ-специалисты, юристы);
- ♦ одно следствие — один аналитик (отсутствие возможности распределения задач);
- ♦ отсутствие централизованной инфраструктуры (а значит, и возможности хранения данных в одном месте с ретроспективным поиском);

♦ большинство следователей, адвокатов и прокуроров не понимает преимуществ компетентного использования ИТ-криминалистики. Многие ИТ-криминалисты не понимают контекста отдельных следствий и периодически пропускают релевантную информацию;

♦ доказательства обрабатываются и рассматриваются в разных местах (дублирование информации, возможность её потери и нарушения целостности, большие объёмы хранимой информации);

♦ постоянно растущее количество и объём данных;

♦ сложность обработки объёмов данных без автоматизации процесса.

ЮРИДИЧЕСКАЯ ЗНАЧИМОСТЬ

Отдельно стоит отметить, что обязательным условием эффективности процесса работы с доказательствами является наличие стандартов и законодательных актов, которые однозначно описывали бы требования к процессам сбора и анализа информации, а также к процедурам ее передачи для рассмотрения в судах. На текущий момент основную роль в определении значимости на себя берут эксперты, привлекаемые судами для проведения анализа собранных данных и подготовки отчётов (экспертных заключений). Открытыми остаются следующие вопросы:

- ♦ каковы требования к экспертам (образование, опыт работы)?
- ♦ меняются ли требования к эксперту в зависимости от состава экспертизы?
- ♦ каковы требования к процедуре анализа?
- ♦ каковы требования к формату и составу экспертного заключения?

Ввиду отсутствия ответов на эти вопросы процесс выглядит следующим образом:

- ♦ эксперт привлекается на каждое отдельное «дело»;
- ♦ квалификация эксперта относительна, и определяется зачастую на основе места его работы (бренда компании, которому «доверяют»);
- ♦ отчёт — это творчество отдельного человека, в котором нельзя оценить полноту проведённого анализа, потому что нет объективных критериев.

ПРО ВЕЛОСИПЕД

В 1948 году в Англии была организована Ассоциация офицеров полиции (The Association of Chief Police Officers — АСРО), участники которой разрабатывали практики, процессы работы полиции и принимали участие в формировании подзаконных актов. В процессе развития цифровых технологий при переходе к электронному документообороту АСРО предложила четыре принципа работы с электронной информацией:

1. Любое действие не должно изменять собираемые с электронных носителей данные (целостность).
2. Если необходимо обеспечить доступ к электронным данным, то специалист должен быть компетентным для сбора релевантных доказательств.
3. Процесс сбора данных должен быть воспроизводим и повторяем, чтобы третья сторона могла осуществить ту же последовательность действий и получить тот же результат.
4. Соответствие (непротиворечивость) первых трёх принципов законодательным актам.

Эти принципы успешно используются как сотрудниками правоохранительных органов, так и персоналом корпораций, вовлечённым в процессы сбора и анализа данных, в том числе, с их последующим использованием в гражданских судопроизводствах. Применяются они в Великобритании, Европе, США и вполне могут быть заимствованы нами.

Ещё одним документом, содержащим методологические рекомендации, является «eDiscovery in digital forensic investigations» 2014 года. Разработанный при участии сотрудников полиции метрополитена Англии, он содержит необходи-

мую информацию о процессе работы с электронными данными. Документ включает требования к программным продуктам, которые должны применяться при сборе и анализе электронных доказательств, а именно на следующих этапах:

- ♦ управление процессом
- ♦ идентификация релевантных данных (источников данных)
- ♦ сохранение
- ♦ сбор
- ♦ обработка
- ♦ оценка релевантности
- ♦ анализ
- ♦ экспорт в отчёты
- ♦ представление заинтересованным сторонам.

Документ предлагает следующее определение форензики:

«Форензика — использование научно обоснованных и доказанных методов в целях сохранения, сбора, идентификации, анализа, документирования и представления электронных доказательств, полученных из цифровых источников в целях облегчения или содействия реконструкции событий, которые могут иметь характер преступных».

За последние 30 лет коллеги выработали проверенные временем практики работы с цифровыми доказательствами, которые (особенно ввиду наличия прецедентного права) принимаются в качестве доказательств в судах.

А ТЕМ ВРЕМЕНЕМ У НАС...

В 2014 году в России был опубликован ГОСТ Р ИСО/МЭК 27037–2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме», который является аналогом международного стандарта ISO 27037.

«Эти процессы необходимы при проведении расследования и предназначены для поддержки целостности свидетельств, представленных в цифровой форме, т.е. являются приемлемой методикой получения свидетельств, представленных в цифровой форме, которая будет способствовать их допустимости для правовых и дисциплинарных действий, а также для других необходимых случаев. Настоящий стандарт

также предоставляет общее руководство по сбору свидетельств, не представленных в цифровой форме, которые могут быть полезны на этапе анализа потенциальных свидетельств, представленных в цифровой форме».

Помимо подтверждения приведённых выше принципов АСРО, стандарт ГОСТ включает детальные алгоритмы работы с информацией, а также дополнительные рекомендации, такие как:

- ♦ описание основных навыков и компетентности (применимых к специалистам);
- ♦ минимальные требования к документации для передачи свидетельств.

ПОДХОДЫ К ПОСТРОЕНИЮ ЭФФЕКТИВНЫХ ПРОЦЕССОВ

Для построения процессов и автоматизации деятельности в области цифровой криминалистики многие компании давно используют специализированное ПО по сбору и анализу данных. Его применение открывает массу возможностей (примерно, как при переходе от счетов к калькулятору):

1. Применение интегрированного в инфраструктуру компании комплекса решений AccessData позволяет при возникновении инцидента через агентское решение осуществить предварительный просмотр информации:

- ♦ статической (неизменяемые данные);
- ♦ динамической (полученные от источника во время работы решения).

Динамические данные могут собираться с компьютеров в сети, включая информацию в ОЗУ и данные с дисков. Кроме того, используя удалённую систему управления дисками (RDMS), можно подключать любой диск, просматривать его содержимое, а затем создавать собственный образ того, что является значимым.

2. Если есть необходимость сбора полной информации, возможно осуществить клонирование дисков с доступом только на чтение к жёсткому диску физически или программный сбор — клонирование с помощью ПО.

3. Для оптимизации объёмов собираемых данных в AD можно использовать библиотеку известных файлов (KFF) для категоризации конкретной информации во время сбора и анализа

доказательств. KFF также позволяет автоматически присваивать файлам статусы «Alert» и «Ignore» для более удобной последующей работы. Примером игнорирования могут быть легитимные файлы операционной системы, которые не несут в себе значимой для расследования информации.

4. Во время сбора доказательств можно создавать индексы данных и фиксировать хэш-значения всех файлов, содержащихся в данных, для осуществления быстрого поиска по индексам. Если необходимо, можно использовать прямой поиск в реальном времени небуквенно-цифровых символов или поиск по шаблонам (регулярные выражения и шестнадцатеричные значения).

5. При анализе данных можно применять технологию OCR для извлечения текста, содержащегося в графических файлах. Также можно расшифровывать многие типы зашифрованных файлов, используя автоматическое дешифрование инструментом восстановления паролей PRTK.

6. В дополнение можно применять функционал Cerberus для анализа исполняемого бинарного файла, который находится на диске, на сетевом ресурсе или в системной памяти. Работа с Cerberus проходит в несколько этапов:

- ♦ Анализ угроз — это общий анализ файлов и метаданных для быстрого разбора исполняемого бинарного файла по общим атрибутам, которыми он может обладать. Он идентифицирует потенциально вредоносный код, генерирует и присваивает оценку угрозы для исполняемого бинарного файла.

- ♦ Статический анализ — это анализ путём дизассемблирования, для которого требуется больше времени для изучения кода внутри файла. Он оценивает возможности бинарного кода, не запуская фактический исполняемый файл.

7. При проведении анализа можно гибко настраивать доступ к файлам для экспертов по типам файлов и предоставлять доступ нетехническим экспертам к файлам для их изучения (рис. 1).

Это малая толика возможностей систем, которые направлены на автоматизацию процессов при расследовании инцидентов на примере AccessData. Главное — результат — это гарантия

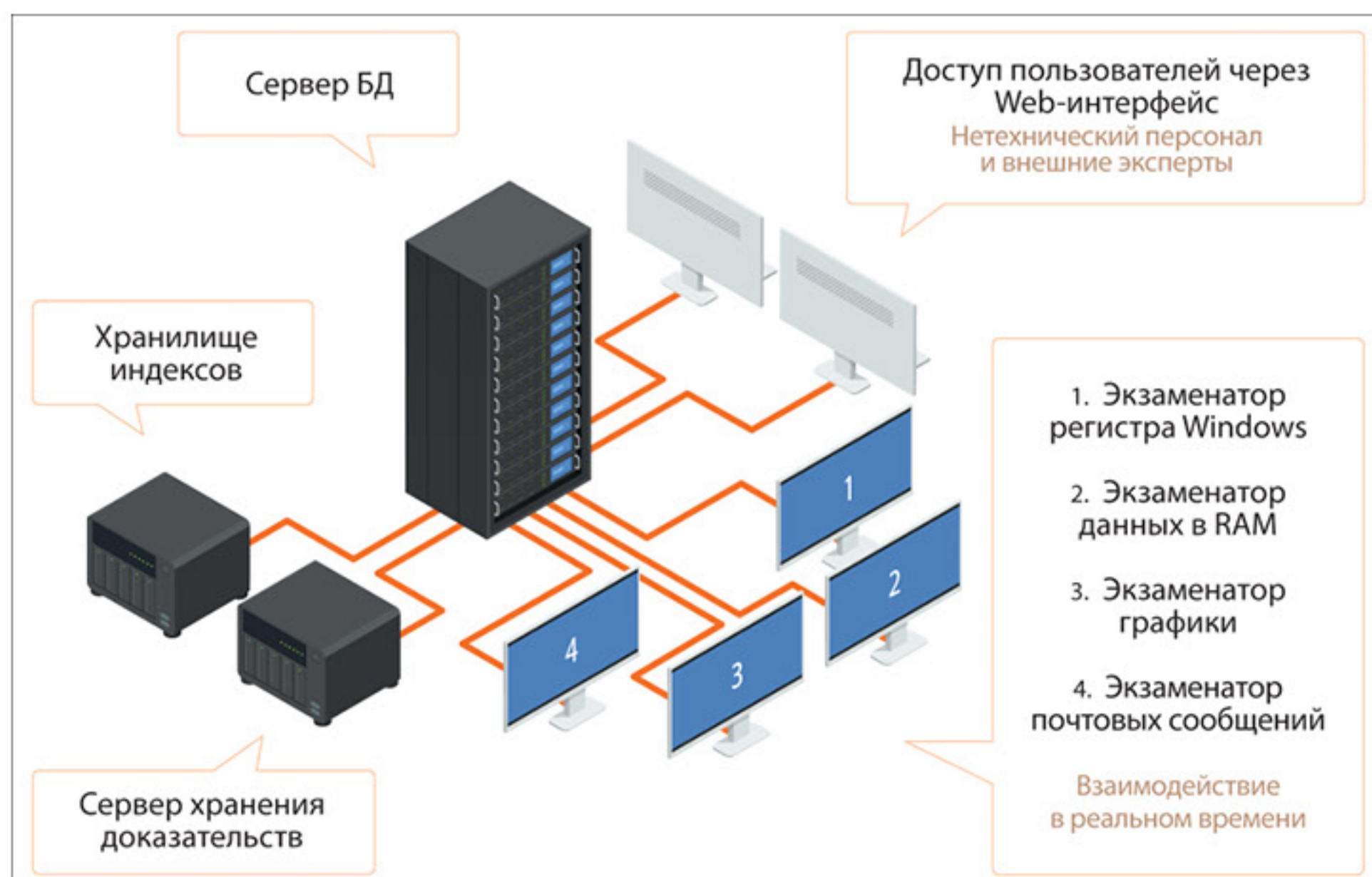


Рисунок 1. Настройка доступа к файлам при проведении анализа

полноты, целостности данных, которые могут быть использованы для дальнейшего судопроизводства.

ЗАКЛЮЧЕНИЕ

Проблематика необходимости работы с большими объёмами данных при проведении цифровых расследований одинакова для всех государств. Построение эффективного процесса работы возможно при выполнении следующих условий:

- ♦ автоматизация процесса сбора данных — скорость сбора, корректность, отсутствие зависимости от квалификации ИТ-специалиста;
- ♦ унификация форматов и процессов сбора, хранения и обработки данных;
- ♦ подтверждённая целостность собранных данных (включая протоколирование процесса сбора);
- ♦ придание юридической значимости собранным доказательствам (судебная практика);
- ♦ использование компаниями и следственными органами инструментов, которые работают с криминалистическими форматами AD 1, EO 1.

Если говорить об опыте иностранных коллег, то они применяют унифицированные форматы сбора данных, что позволяет отказаться от необходимости дополнительной экспертизы корректности полученной информации (в каждом отдельном случае), перенести эту ответственность на разработчиков ПО (требования к которым явным об-

разом зафиксированы в национальных стандартах и практиках). Задачи сбора информации сводятся к корректному использованию ПО и минимизируют потенциальные ошибки ИТ-персонала. Возможность применения ПО с централизованным хранением данных и возможность распределения задач между сотрудниками позволяет сокращать издержки и эффективно управлять временем персонала. Наличие у нас аналогичных национальных стандартов позволяет нам использовать все наработанные ранее практики, неся в том числе и значительные выгоды для бизнеса:

- ♦ отсутствие влияния на бизнес-процессы (удалённый сбор данных с конечных точек, распределение задач, исходя из компетенций персонала (безопасности своё — аналитикам и юристам своё));
- ♦ снижение рисков повреждения, видоизменения информации при её сборе, анализе и/или подготовке отчёта (нарушение принципа целостности приведёт к нивелированию юридической значимости);
- ♦ снижение издержек на сбор и анализ доказательств.

Помимо всех приведённых плюсов автоматизации и унификации при использовании единых технологий корпорациями, следственными органами и судами, результатом может стать единая прозрачная для всех сторон работающая экосистема в сфере «Digital Forensics».

РЕШЕНИЯ ДЛЯ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ И СБОРА ДОКАЗАТЕЛЬСТВ

✓ ЦИФРОВЫЕ РАССЛЕДОВАНИЯ

Желаете получить полное представление о том, что именно произошло и кто был вовлечен? AccessData предоставит инструменты для анализа компьютеров, мобильных устройств и сетевых коммуникаций. Когда вы знаете больше, вы можете сделать больше.

✓ СБОР И АНАЛИЗ

Хотите обойтись меньшими затратами и ресурсами при сборе доказательств? Нужно снизить риски или обеспечить соблюдение требований? Инструменты AccessData для сбора, хранения, хранения, обработки и оценки данных снижают затраты и риски.

✓ РИСК И СООТВЕТСТВИЕ

Находите информационные риски на всех конечных точках предприятия и снижайте их с помощью корпоративного поиска, криминалистического сбора и анализа данных и оценки соответствия. Вносите исправления: удаляйте файлы, уничтожайте процессы и останавливайте несовместимые действия на конечных точках.

ПРОЦЕССЫ, КОТОРЫЕ ПОЗВОЛЯЕТ РЕАЛИЗОВАТЬ ACCESSDATA:

- ✓ Сбор – сбор данных, хранение цифровых доказательств;
- ✓ Анализ – создание кейсов, обработка доказательств;
- ✓ Рассмотрение – создание отчетов о кейсах с полным документированием и обобщением результатов;
- ✓ Управление – обслуживание, включая резервное копирование, архивацию, восстановление и удаление кейсов и собранных доказательств.



Cross Solutions – Российский разработчик и дистрибьютор решений для защиты вашего бизнеса от утечек информации и проведения расследований инцидентов ИБ.

www.cross-solution.ru
info@cross-solution.ru
+7 (495) 741-88-64



ЛОГИКА В МАСШТАБЕ

ИТОГИ XI УРАЛЬСКОГО ФОРУМА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВОЙ СФЕРЫ»

Банк России при организационной поддержке «Медиа Группы «Авангард» провёл одно из главных и наиболее представительных деловых мероприятий отрасли — XI Уральский форум «Информационная безопасность финансовой сферы».

С 18 по 22 февраля форум собрал более 600 ИБ-специалистов из более чем 30 городов России. Приехало много иностранных гостей, шесть из десяти стран-участниц были представлены официальными

делегациями. В этом году заметно возросло число участников финансовых организаций — 146 представителей. Увеличилось и представительство регулятора — Банка России — 54 делегата, среди них первый заместитель председателя Ольга Скоробогатова и два заместителя председателя: Дмитрий Скобелкин и Василий Поздышев.

Актуальность и важность поднятых тем подтвердило активное участие представителей некредитных финан-

совых организаций — страховых компаний, бирж, инвестиционных и микрофинансовых компаний, а также государственных структур, организаций в области профессионального образования, общественных организаций и профессиональных объединений. Заметным было и представительство партнёров форума — более 40 компаний-интеграторов и вендоров.

Стоит отметить высокий интерес со стороны СМИ — на форуме работа-



Круглый стол «Диалог с регулятором»



Пресс-подход к руководству Банка России

ли более 30 корреспондентов и обозревателей специализированных и массовых изданий, опубликовавших в ходе мероприятия и по его итогам более 100 эксклюзивных материалов. Кроме того, организаторы сами вели онлайн-трансляцию новостей со всех площадок Форума.

Ярким моментом стала традиционная церемония награждения отраслевой премией «Информационная безопасность банков», учреждённой BIS Journal, за выдающиеся заслуги российских банков, компаний-лидеров, регулирующих органов, а также отдельных деятелей, внёсших значительный вклад в развитие отрасли.

Новой традицией форума обещает стать впервые проведённый конкурс стартапов в сфере ИБ. Он прошёл



Дискуссия «Перспективы применения RegTech и SupTech»



Вручение отраслевой премии «Информационная безопасность банков»



Демо-зона Уральского форума



Первый заместитель директора Департамента информационной безопасности Банка России Артём Сычёв



Ужин на свежем воздухе



В хоккей играют настоящие банкиры!

успешно, привлёк внимание участников форума и, по словам Ольги Скоробогатовой, стал свидетельством того, что отрасль информационной безопасности в России достигла определённой зрелости, начав, наконец, трансформировать довольно абстрактное до последнего времени творчество масс в полезные и коммерчески выгодные продукты.

Деловая программа Уральского форума в этом году отличалась особой насыщенностью. За четыре рабочих дня прозвучало 60 докладов, прошло 12 дискуссий, 8 мастер-классов, вечерние дебаты, круглые столы, закрытые секции, в том числе международная, и три больших пресс-подхода к руководителям Банка России.

Обсуждение конкретных вопросов информационной безопасности проходило в контексте наиболее актуальных тем, таких как:

- ◆ система быстрых платежей;
- ◆ единая биометрическая система;
- ◆ проекты RegTech и SupTech;
- ◆ непрерывность предоставления финансовых услуг;
- ◆ контроль уровня несанкционированных операций;
- ◆ противодействие мошенническим сайтам;
- ◆ гибкая разработка программного обеспечения;
- ◆ система «Фид-Антифрод».

Уже традиционные для Уральского форума закрытые секции в этом году работали на международном уровне:

за закрытыми дверями участники говорили о международном обмене информацией, сотрудничестве кредитно-финансовых организаций с регуляторами, а также о гармонизации подходов к стандартизации ИБ финансовых организаций стран-участниц.

В заключение XI Уральского форума прошла командная интеллектуальная игра «Где Логика?» и традиционное выступление Алексея Лукацкого «Уральский форум за 15 минут». Подвёл итоги и закрыл Форум Первый заместитель директора Департамента информационной безопасности Банка России Артём Сычёв.

НА СЦЕНУ ВЫХОДИТ МОЛОДЁЖЬ

НА XI УРАЛЬСКОМ ФОРУМЕ СОСТОЯЛСЯ ПЕРВЫЙ КОНКУРС СТАРТАПОВ В СФЕРЕ ИБ

Первый конкурс стартапов состоялся по инициативе Банка России, прошел успешно, хотя и без особого фурора, и, по мнению многих, открыл новый этап в истории как Уральского форума, так и отечественной информационной безопасности в целом.

Предварительно на конкурс было подано 30 заявок, из которых после отбора на форум пригласили шесть команд. После публичной защиты проектов победителем признали команду Qgate, разработавшую программу квантового распределения ключей. «Это наш упреждающий ответ квантовому апокалипсису, то есть квантовому компьютеру, появления которого мы все с нетерпением ждем, но против которого симметричная криптография будет бес-

сильна», — так представил разработку капитан команды Олег Гурин.

Второе место присудили команде СНЕСКУ за проект удаленной верификации личности и распознавания подделок в сканах документов. Третье — команде IT-Expertise за проект организации доверенной среды в распределенных информационных системах. И специальный приз ФинЦЕРТа получила команда Secret cloud за продукт, позволяющий банкам более эффективно использовать данные ФинЦЕРТ.

Награждая победителей, первый зампред Банка России Ольга Скоробогатова пригласила их на работу в Банк России, на что организатор конкурса Антон Арнаутов воскликнул: «Вы их испортите!» В каком-то смысле Антон

лукавил, поскольку, по его же словам, природа стартапов на Западе и у нас принципиально разная. Если на Западе в ее основе лежит венчурная индустрия, которая довольно равномерно опыляет деньгами молодые дарования и тем самым позволяет им и свободно творить и сносно жить, то в России иначе. Тут венчурная индустрия так и не сформировалась, поэтому молодые стартаперы — это те же подрядчики, которые вынуждены мыкаться в поисках заказов и всегда рады, когда крупная компания берет их под свое крыло.

В этом смысле Уральский форум оказался тем самым заветным местом, где встретились молодые таланты и те, кому они нужны. По крайней мере, несколько состоявшихся контактов обещают быть перспективными.



Первый зампред Банка России Ольга Скоробогатова награждает победителей конкурса стартапов. В центре — Артём Субботин (команда СНЕСКУ, II место), слева — Антон Арнаутов, генеральный директор АНО «Финтех Лаб» (председатель жюри конкурса)

ИНФОФОРУМ 2019

К СУВЕРЕННОЙ КИБЕРБЕЗОПАСНОСТИ ЧЕРЕЗ
ГАРМОНИЗАЦИЮ ЗАКОНОДАТЕЛЬНОЙ И ПРАКТИЧЕСКОЙ ИБ

Участников ИНФОФОРУМА 2019 приветствовали представители законодательной ветви власти, входящие в круг первых лиц Комитета Госдумы по безопасности и противодействию коррупции, Комитета Госдумы по информационной политике, информационным технологиям и связи и Комитета Совета Федерации по конституционному законодательству и государственному строительству. Участие таких людей убедительнее их выступлений отразили серьёзность задач, которые предстоит решить для обеспечения безопасности текущей цифровизации. Среди главных проблем были особо выделены две:

1. Осознание бизнесом необходимости следовать не только нормам, но и духу закона 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»; рассматривать ИБ как часть критически важных бизнес-процессов.

2. Нахождение путей решения кадровой проблемы в сфере ИБ и повышения «цифровой» культуры населения страны.

МАСШТАБ КОНТЕКСТА

Тема этого Инфофорума: «Цифровая трансформация и информационная безопасность России». Мероприятие прошло на фоне активизации киберугроз для КИИ, происхождение которых принято считать «интернациональным». Этому вопросу касались неоднократно, начиная с выступления председателя Комитета Госдумы

по информационной политике, информационным технологиям и связи Л. Левина.

Мировой масштаб, вкупе с тем, что наряду с «интернациональными» атаками отчётливо слышны и «национальные» угрозы, вызвал к жизни в 2018 году ряд знаковых международных инициатив. Например, «Парижский призыв к доверию и безопасности в киберпространстве» — инициатива Франции на глобальном Форуме по управлению интернетом, «Сингапурский пакет», подготовленный Международной комиссией по киберстабильности и резолюция ООН от 5 декабря, посвящённая вопросам кибербезопасности.

На одной из секций заместитель руководителя отдела внешних коммуникаций Координационного центра доменов .RU/.РФ М. Анисимов отметил, что «эти три документа имеют много общего... везде отмечается очень сильное повышение роли государств в обеспечении информационной безопасности, а главной ценностью провозглашается стабильная и надёжная работа ядра интернета».

КАК ЭТО ПОНИМАТЬ

Подобная характеристика международных инициатив вызывает сложные чувства. С одной стороны, внушает оптимизм признание того, что свободная конкуренция и частная инициатива не способны ставить ИБ в качестве безусловного приоритета цифровой трансформации. В лучшем случае для бизнеса таким приоритетом является оптимизация рисков.

С другой, провозглашение высшей ценностью стабильной и надёжной работы «ядра интернета» — весьма сомнительно. Государственных чиновников нельзя упрекать за дежурные реверансы в сторону международных институтов (по словам того же М. Анисимова, «наибольшим доверием пользуются «наднациональные» наблюдательные структуры на уровне ООН или ЕС»), но мы это не раз видели, как «наднациональные» структуры устраивали травли в стиле «все на одного».

Троцкизм в ИБ так же недопустим, как троцкизм в политике, а «стабильная работа сети Интернет» в условиях контроля конкретными странами её технической политики — такая же утопия, как стабильная экономика под контролем ВТО. Не лишним будет вспомнить, что многие войны, распорядившись ядерного оружия, поспешив Договор о нерушимости послевоенных границ в Европе, уничтожение государственности Ирака, Ливии, Югославии, переход Евросоюза в «метастабильное» состояние — всё это происходило под патронажем «наднациональных» структур.

Киберпространство, объединённое платформой, обеспечивающей «безграничную свободу всемирных коммуникаций и общения», для них — новое «поле боя».

НА ПУТИ К СУВЕРЕННОЙ КИБЕРБЕЗОПАСНОСТИ

В этих условиях закон 187-ФЗ «О безопасности критической информационной инфраструктуры РФ», положивший начало инвентаризации всей ИТ-инфраструктуры страны, кажется весьма своевременным. По оценке ФСТЭК, озвученной заместителем директора ФСТЭК В. Лютиковым, в стране имеется без малого 200 000 объектов КИИ во владении более десятка тысяч субъектов КИИ.

Мировой масштаб, вкупе с тем, что наряду с «интернациональными» атаками отчётливо слышны и «национальные» угрозы, вызвал к жизни в 2018 году ряд знаковых международных инициатив



Заместитель директора ФСТЭК России Виталий Лютиков
(фото: infoforum.ru)



Заместитель руководителя ДИТ г. Москвы Александр Горбатко
(фото: infoforum.ru)

И всё бы хорошо, но все обсуждения 187-ФЗ выходили на проблему катастрофической нехватки квалифицированных кадров как для субъектов КИИ, так и для регуляторов. В стане регуляторов это приводит к запаздыванию с подготовкой нормативных и методических документов, а «на местах» замедляет проведение в жизнь требований Закона. А ведь наряду с «категорированием» необходимо отражать и массированные «интернациональные» атаки!

В результате инвентаризацию и категорирование в рамках 187-ФЗ к началу 2019 года прошли всего 10%-15% от общего числа субъектов КИИ. Печально, что этот процесс задерживают в первую очередь банки. Некоторые эксперты объясняют это тем, что финансовые структуры находятся в зоне более сложного регулирования: «... помимо основных регуляторов 187-ФЗ у них есть ещё и отраслевой регулятор — ЦБ. Поэтому процесс согласования критериев, объектов и результатов категорирования более сложный и многоэтапный».

ЧТО НАМ МЕШАЕТ

«ИТ-развитие обгоняет развитие систем информационной безопасности», сказал заместитель руководителя Департамента информационных технологий города Москвы А. Горбатко. И банки тут, в отличие от консервативных ОПК, медицины и ТЭК, в передовиках. Например, новые технологии ДБО (включая и «биометрию») заметно отстают от анонсов высоко-технологичных угроз ИБ в этой сфере.

И это происходит на фоне как дефицита финансовых и кадровых ресурсов, так и ужесточения требований к КИИ.

Вывод прост: цифровая трансформация общества невозможна без серьёзных изменений в правовом регулировании гражданских и экономических отношений, и это отдельная болевая зона «цифровой экономики». Если говорить о банках, то речь не только о 152-ФЗ, 167-ФЗ и 382-П. Эксперты уверены, что так и не решены казавшиеся простыми, «канцелярскими», а на деле оказавшиеся базовыми вопросы цифрового документооборота. Обсуждению этой и других проблем законодательства на форуме была посвящена секция «Проблемы правового регулирования информационной безопасности», прошедшая весьма активно.

ЮРИСТЫ ГОВОРЯТ

Блокчейн на «юридической» секции был упомянут лишь в качестве примера хайпа, несвоевременно предлагаемого для правового регулирования. А вместо приевшегося регламента GDPR с большей пользой было обсуждено сообщение доктора юридических наук Л. Терещенко «Тенденции правового регулирования информационной безопасности личности». Людмила Константиновна заострила внимание на угрозах правам и свободам личности со стороны законодательных актов, порождённых попытками превратить персональные данные в коммерческий продукт.

Среди прикладных как всегда муссировался вопрос использования разных

типов электронных подписей. Среди общих — вопрос конкретизации понятий «цифровой трансформации» и «цифровой экономики».

«Перезревшим» был признан вопрос необходимость законодательного оформления сквозной процедуры законотворчества (от ТЗ на закон до его принятия) с обязательным обсуждением между этими двумя «реперными датами». Пугающе низкое качество поступающих в Думу проектов законов ставит, по мнению экспертов, в повестку дня вопрос об ответственности за подготовку проектов, противоречащих действующему законодательству и нормам русского языка.

Несомненным положительным результатом Инфофорума 2019 стал диалог между государством, бизнесом и наукой о нормативном обеспечении и правовом регулировании в сфере цифровой трансформации и кибербезопасности. Были обозначены приоритеты работы технических специалистов, чиновников, учёных и преподавателей в интересах безопасной цифровизации производства, бизнеса и экономики в целом. Подверглись критическому обсуждению проблемы, решаемые в ходе работы государственной системы ГосСОПКА, закона 187-ФЗ и ряда нормативных актов, важных для проведения управляемой и безопасной цифровой трансформации.

ТБ ФОРУМ 2019

О РАДОСТИ БУДУЩЕЙ И БОЛИ СЕГОДНЯШНЕЙ

ТБ форум — одно из немногих мероприятий, охватывающих все аспекты безопасности государства, общества и экономики. В этом массовом марафоне конференций организаторы выделили отдельное направление SECUFINANCE, посвящённое исключительно вопросам ИБ финансовой сферы. В числе докладов были и те, что представляли не столько технологии защиты, сколько перспективные технологии банковского сервиса, о защите которых предлагалось думать уже сегодня. Хотя, откровенно говоря, правильным было бы сначала определиться с тем, какой будет финансово-кредитная организация будущего в целом.

ФОРУМ, ДАЙ ОТВЕТ!

Будет ли «банком будущего» единый мегаБанк или маркетплейс инвестиционных стратегий, появятся ли криптовалютные биржи, о которых говорилось на секции «Цифровая экономика и новейшие технологии в финансовом секторе»? А может, все эти термины и понятия — всего лишь фантазийный «пузырь», а финансовые услуги будут оказывать старые добрые банки с офисами, уличными банкоматами и ДБО на основе смартфонов? На эти вопросы ТБ форум не дал ответа.

Зато реальная ситуация достаточно полно была представлена на секциях «Удалённая биометрическая идентификация. Технологии предикативного распознавания» и «Информационная и компьютерная безопасность в финансовом секторе». Речь шла о видеонаблюдении с элементами биометрии и централизованном управлении системами мониторинга.

ГЛАЗА И УШИ + МОЗГ

Безопасность современного банка самым причудливым образом сталкивается и с вызовами классическими, и с угрозами, которые ещё недавно казались футуристическими. Деньги по-

хищают как методом примитивного взлома банкомата кувалдой, так и в результате кибернетической спецоперации с использованием вредоносного ПО.

В некоторых случаях, если не предотвратить, то хотя бы расследовать и ту и другую атаку помогает система видеонаблюдения, в основе которой уже не просто аналоговая видеокамера, а система камер со встроенными процессорами обработки изображения и звука. Такая обработка — не просто очистка сигналов от помех, а система предикативной аналитики происходящего в поле «зрения и слуха». В результате к инциденту не только привлекается внимание сотрудника, но и автоматически выполняются упреждающие действия. О подобных возможностях системы рассказал представитель корейской компании Hanwa Techwin, предлагающей как интеллектуальные камеры видеонаблюдения, так и ПО для интегрированных систем видеонаблюдения на больших площадях. В портфолио компании несколько проектов с российскими банками, включая Сбербанк.

Александр Долженко из Газпромбанка анонсировал решение на основе системы видеонаблюдения, которая помимо помощи при инцидентах выполняет вполне «мирные» функции разграничения доступа в служебные помещения. Утомительное манипулирование смарт-картами — в прошлом!

Алексей Данилевский из Райффайзенбанка представил проект интеллектуальных видеокамер, позволяющих выполнять не только функции безопасности, но и предоставлять сотрудникам информацию для повышения скорости и адресности обслуживания клиентов. Видео сопровождает клиента в течение всего времени его пребывания в банке. По интонациям докладчика была видна его неподдельная заинтересованность, но, как отметил Алексей, пред-

стоит ещё защита проекта и оценка его возможностей относительно текущего бизнеса банка.

СКОРАЯ ПОМОЩЬ

Защитные технологии невозможно развивать без знаний об угрозах, исходящих из киберпространства. О деятельности ФинЦЕРТ Банка России рассказал Павел Ревенков, заместитель начальника ФинЦЕРТ. Его сотрудники сегодня выступают не только в роли аналитиков и координаторов борьбы с киберугрозами, но и активно работают «в поле», играя роль «скорой помощи» для небольших периферийных банков и решая проблемы по «горячим следам».

ДИСКУССИЯ-БОЛЬ

Все сообщения выслушивались с неизменным интересом и сопровождались дозированными дискуссиями под контролем модераторов. Однако после доклада «Антифрод — неравный бой с бизнесом» чинная дискуссия-обсуждение вдруг превратилась в дискуссию-боль, в ходе которой представители служб ИБ «небольших и средних банков» продемонстрировали дружное желание «выплакаться в жилетку».

Выступающие уже хотели не «найти истину», а только разделить с коллегами всю тяжесть забот о безопасности бизнеса, что ежедневно сваливается на их плечи... А также тяжесть требований 382-П, 167-ФЗ, 187-ФЗ... И тяжесть внедрения откровенно сырых биометрических технологий. Внедрения в условиях дефицита финансов, кадров, ужесточения «нормативки» и просто плохого отношения со стороны начальства.

* * *

Этот всплеск боли понятен, ведь кредитно-финансовые организации сегодня — в числе аутсайдеров по выполнению требований 187-ФЗ «О безопасности КИИ РФ», и в этих условиях говорить о «банке будущего» явно рановато.

ВІТ-2019

О «КОРОБОЧНЫХ» ТЕХНОЛОГИЯХ ДЛЯ БЕЗОПАСНОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Не все обладают ресурсами Сбербанка, и для таких рынков предлагает «коробочные» решения, «оптимальные по соотношению цена/качество», из которых с помощью API или стандартных интерфейсов и кабелей можно собрать свой пазл для интеграции в цифровую экономику страны. Международный Гранд Форум «ВІТ-2019» оказался той ярмаркой решений, которая позволяет взыскательному, но небогатому СМБ стать «Smart». ВІТ — это только на первый взгляд всего лишь три буквы. ВІТ — это «Бизнес и ИТ. Вокруг ЦОД. Вокруг Облака. Вокруг Данных. Вокруг IP. Вокруг IoT. Smart SMB». Приятной особенностью форума оказалось внимание к вопросам кибербезопасности Smart СМБ, выстраивать которую было предложено с защиты инженерной инфраструктуры.

Доклад «Новинки безопасности от Zuhel» стал хорошим началом, ядром же Форума выступили доклады, представившие возможности и экспертные рекомендации в сфере, кратко именуемой сегодня аббревиатурой ЦОД.

Сообщение компании Cloud4Y оказалось заманчивым коммерческим предложением «облака», в котором по ценам на порядки меньшие зарубежных можно размещать и обрабатывать свои данные, резервно хранить ценную информацию (с гарантиями восстанов-

ления в течение пары десятков минут). Среди заказчиков, уже использующих возможности Cloud4Y не только неназванный агрохолдинг, но и вполне себе осязаемый Сбер. Заказчики платят деньги, а внешний ЦОД от Cloud4Y обеспечивает непрерывность их бизнеса.

А вот выстраивать информационную безопасность собственного «Smart СМБ» надо с инженерной инфраструктуры того, что является вашим личным ЦОДом. На ВІТ-2019 это обосновывалось вполне конкретными примерами из практики Алексея Конхина, представленного в качестве независимого эксперта. Алексей напомнил, что современное «цифrofизеющее» оборудование для электропитания является такой же целью для кибератак, что и серверы и ПК. Ведь его системы управления всё чаще «висят» в Сети и зачастую под теми же паролями, что были установлены ещё изготовителями. А если учесть, что искусственный «интеллект» современных систем электропитания зачастую близок к человеческому, задействованному при их создании (о нём можно судить по анекдотам про программистов), то с потерей информации после «падения» электропитания можно столкнуться и без участия хакеров.

Помимо нестандартного взгляда Алексея Конхина на то, откуда начинается ИБ современного предприятия,

на Форуме были предложены решения и услуги для создания систем ИБ, которые сегодня кроются за аббревиатурами DLP, SIEM, UEBA.

Кроме «центровых» (в прямом и переносном смысле) проблем цифровизации на Форуме были представлены и приятные «мелочи». Например, решения и продукты для создания систем телефонии, которая будет и интеллектуальная, и VoIP, и для «унифицированных коммуникаций». Речь шла и о том, как эффективно обеспечить беспроводную передачу видеоданных в ходе совещаний и презентаций; и о дисковых накопителях с «квантами» хранимой на дисках информации, измеряемыми десятками терабайт.

Своеобразным открытием Форума стало то обстоятельство, что ситуация с госуправлением в нашей стране совсем не безнадежна. С теплыми словами в адрес чиновников, пришедших в отечественные министерства из бизнеса, выступил Алексей Солдатов, генеральный директор DataPro, рассказавший собравшимся, как легко и выгодно стало заниматься в нашем государстве экспортом ИТ-услуг. К его оценкам присоединился Владимир Рубанов, управляющий директор Росплатформы, поведавший о перспективах обретения Россией цифрового суверенитета на основе гиперконвергентных программно-определяемых вычислительных платформ.

Современное «цифrofизеющее» оборудование для электропитания является такой же целью для кибератак, что и серверы и ПК. Ведь его системы управления всё чаще «висят» в Сети и зачастую под теми же паролями, что были установлены ещё изготовителями

Подводя итоги, можно с уверенностью и не кривя душой сказать, что Форум позволил пополнить копилку знаний о современных предложениях для цифровой трансформации бизнеса. А уж совсем приятным бонусом оказалась возможность оперативно «перетереть» эту информацию с коллегами.

«В ТЕОРИИ НЕТ РАЗНИЦЫ МЕЖДУ ТЕОРИЕЙ И ПРАКТИКОЙ. А НА ПРАКТИКЕ ЕСТЬ»

НТЦ «ВУЛКАН» ПРЕДСТАВИЛ СВОЮ МЕТОДИКУ КИБЕРУЧЕНИЙ

Криминогенная ситуация в киберпространстве сегодня — это причудливое смешение индивидуального киберхулиганства, маховских рейдов кибергруппировок с причудливыми названиями и изящных тихих спецопераций «вежливых хакеров». В этих условиях специалисты всё чаще рекомендуют бизнесу дополнять «простое» тестирование на проникновение реальными киберучениями на живом персонале. Об одной из таких методик и её практических результатах рассказали на своём мероприятии «Анализ защищённости и киберзащита» эксперты НТЦ «Вулкан».

ИНСТРУМЕНТ СОВЕРШЕНСТВОВАНИЯ

Киберучения — прямой и объективный способ получить информацию о положении дел в ИБ организации, а также понять степень вовлечённости персонала в процессы защиты.

Эксперты НТЦ «Вулкан» рассказали об испытанной на практике трёхуровневой методике киберучений. Их высшей «формой» является имитация проникновения (при негласном контроле ситуации со стороны посвящённых) и фиксация поведения непосвящённых с измерением их реакций в реальном времени. Минимум посвящённых и абсолютная правдоподобность угрозы позволяет без чрезмерных потерь, но не совсем даром, вскрыть недостатки в системе ИБ.

СОТРУДНИК, ЗАГНАННЫЙ В УГОЛ

Специалисты НТЦ «Вулкан» имеют основания утверждать, что эти тезисы перестали быть их умозрительными построениями, поскольку методика прошла проверку в одном из банков. Как это было? О предстоящем событии — имитации атаки вируса-шифровальщика знали считанные сотрудники, включая единственного посвящённого

руководителя высшего звена, который и должен был ответить за всё в случае, если «что-то пошло не так». Сразу отметим, что ни один байт банковской информации в ходе учений не пострадал, хотя не все сотрудники оказались на высоте и решили свои плановые задачи.

Подготовительный этап учений, помимо разработки плана, заключался в подготовке средств для замера показателей процесса реагирования на атаку и оценки действий работников. А также в разработке имитатора вируса-шифровальщика, обеспечивающего реалистичность происходящего.

Проведённые «замеры» включали серию экспресс-интервью с людьми, находящимися во время атаки в сильном стрессе. Реакция испытуемых была весьма бурной, вплоть до желания причинить интервьюерам боль разной степени тяжести. Таких интервью было много, и именно они составили своеобразный Big Data-набор, позволивший выработать рекомендации по совершенствованию системы ИБ банка.

РАЗНЫЕ ВИДЫ КИБЕРУЧЕНИЙ

По мнению экспертов НТЦ «Вулкан», помимо имитации массового заражения вирусом-шифровальщиком, на сегодняшний день наиболее актуальны ещё и киберучения, имитирующие массовое вовлечение в бот-сеть и DDoS-атаки. И во всех этих случаях киберучения в реальных условиях — это не «коробочное решение»!

Следует также понимать, что обратной стороной такого рода учений являются материальные потери, связанные с возможным нарушением непрерывности бизнеса (или принятием дополнительных мер, чтобы этого не случилось) и необходимостью восстановления тех



Бизнес-завтрак «Анализ защищённости и кибербезопасность» (фото: ntc-vulkan.ru)

«разрушений» в ИТ-инфраструктуре, что возможно появятся в результате паники персонала. Слушатели мероприятия отметили также, что для банков необходимо предусмотреть «откат» информации об учебной атаке и её последствиях в отчётной документации, связанной с работой ФинЦЕРТа.

ПРЕДВАРИТЕЛЬНЫЕ ЭТАПЫ

В связи со сказанным и для минимизации негативных последствий имитации

атаки на организацию, эксперты НТЦ «Вулкан» обратили внимание слушателей на необходимость постепенного продвижения к высшей фазе киберучений через менее затратные предварительные этапы:

♦ «штабные учения «на картах», когда имитация внештатных ситуаций анализируется с документацией в руках с детальной фиксацией выполнения процедур специалистами и проверкой адекватности их действий;

♦ пентестов с последовательным воспроизведением этапов кибератаки и анализом выполнения персоналом регламентированных процедур.

Помимо знакомства с методикой адаптивных киберучений на мероприятии были представлены коммерчески доступные программные инструменты для выявления и подавления активности киберпреступников в ИТ-инфраструктуре организации и анализа уязвимостей ИТ-инфраструктуры.

ЖУРАВЛИ И СИНИЦЫ

НА ЗАСЕДАНИИ КОМИТЕТА АПКИТ ПО МОНИТОРИНГУ РАЗВИТИЯ ИТ-ИНДУСТРИИ

Традиционный телекомовский конгресс в Барселоне акцентировал своё внимание на сегменте Enterprise; бизнес в задумчивости глядит на 5G, не вполне понимая «а ему это надо?»; Nokia ищет себя в IoT и энергомониторинге; хайп вокруг Big Data в мире утихает... Эти темы и слухи были озвучены на очередном заседании Комитета АПКИТ по мониторингу развития ИТ-индустрии, опекаемого российским IBM. Вишенкой же на торте проведённого 15 марта заседания оказался доклад о технологии RPA, интерес к которому в очередной раз продемонстрировал, что в мире серьёзных потребителей ИКТ синица в руках по-прежнему остаётся желанней журавля в небе.

ЧУДО СТАРОЕ И НАДЁЖНОЕ

На фоне избыточно многочисленных ИТ-хайпов заказчики из сферы офисного бизнеса (банки, страховщики, дистрибьюторы, реселлеры и пр.), приходя на работу, с надеждой и уважением «ощупывают» надёжное «оружие» в виде т.н. унаследованных систем автоматизации компьютерно-мейнфреймовской эпохи и доброго старого Excel. В зарубежных банках они, бывает, исчисляются многими десятками. Технология программной «роботизации» (RPA) до сих

пор позволяет избежать проблем «переездов» на новую ИТ-инфраструктуру (которые и в этой области можно измерять в «пожарах») или не менее утомительных интеграционных проектов. А также освободить людей от выполнения рутинных утомительных операций, а сами операции — от влияния человеческих ошибок.

В свете возможности недорогого, относительно быстрого и, что самое главное, надёжно работающего чуда RPA-трансформации был совершенно понятен ажиотаж, выраженный в массе вздыбленных смартфонов, снимающих слайд за слайдом RPA-презентацию. И это, несмотря на заверения хозяйки мероприятия Натальи Бердыевой, что все презентации будут своевременно разосланы участникам заседания.

ПРОЩАЙ, ХАЙП!

Прохладная и местами скептическая реакция зала на доклад о возможностях превращения Больших Данных в новую нефть только подтвердил слухи о тенденции к затиханию международного хайпа вокруг Big Data. Хотя само выступление, если не вдумываться глубоко и критически в его утверждения, отличалось качественной драматургией, выразительной инфографикой и содержало изображение обязательного в ны-

нешней ситуации документа о включении в Реестр отечественного ПО.

БЛОКЧЕЙН, СЭР!

Сложные чувства вызвал доклад о блокчейне. Сегодня в обществе воспитанных людей о блокчейне принято или не говорить ничего, или говорить в контексте конкретного проекта с демонстрацией объективно измеряемых показателей полезности и (sic!) информационной безопасности. 15 марта в клиентском центре IBM в Москве о проблемах информационной безопасности технологии блокчейн не говорилось ничего, лишь вскользь было упомянуто о возможных эксплуатационных проблемах ИТ-систем на основе распределённых реестров.

* * *

Конечно же, это заседание Комитета АПКИТ по мониторингу развития ИТ индустрии не претендует на аналитичность и общий уровень ежегодной итоговой конференции, но некие ощущения всё же сформировались. И в первую очередь о смещении ИТ-вендорами маркетинговых акцентов на укрепление сбытовых позиций в корпоративном сегменте. Причём при отсутствии внятной аргументации в пользу 5G&IoT инноваций.

DLTREG 2019

КОНФЕРЕНЦИЯ ПРЕДСТАВИЛА КАРТИНУ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В РОССИИ

В конце апреля Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) и IP Club провели Вторую конференцию по регулированию распределённых реестров DLTReg 2019.

В ЕВРОПЕЙСКОМ КОНТЕКСТЕ

В этом году конференция была посвящена вопросам регулирования технологии блокчейн, в частности, стандартизации, как основе нормативного регулирования, и смарт-контрактам, как наиболее интересному механизму оптимизации бизнес-взаимодействий. В ходе конференции организаторы попытались собрать и систематизировать мнения экспертов в части юридических проблем, регулирования и применения технологий блокчейн и распределённых реестров.

Преподаватель Женевского университета, консультант по юридическим технологиям, блокчейну, смарт-контрактам и защите данных Йорн Эрбгут рассказал, как соотнести применение

технологии блокчейн и принципы защиты персональных данных, заложенные в GDPR. Он также представил пять способов внедрения технологии в рамках Европейского регламента и поделился опытом практического применения технологии блокчейн.

После вступительного доклада обсуждение проходило в рамках двух сессий: «Регуляторные аспекты технологии блокчейн» и «Практическая реализация проектов».

РЕГУЛЯТОРНЫЕ АСПЕКТЫ

На первой сессии особенно интересным и полезным было выступление представителя ФСБ России Андрея Елистратова, представившего подводные камни сертификации блокчейн-решений, которые в разрезе классификации регулятора относятся к средствам криптографической защиты информации.

Елена Гульгяева, представитель правового комитета РАКИБ, познакомила слушателей с нормотворческой работой, касающейся использования блокчейн/DLT, и обозначила вопро-

сы, которые остались за рамками проектируемых законопроектов: легальность рынка цифровых активов, статус сделок, последствия совершения сделок с криптовалютами/токенами и др.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ

Докладчики практической сессии рассказали о возможностях и подводных камнях при применении технологии блокчейн. К примеру, в сфере семеноводства пользователям распределённой базы данных удаётся получать актуальные сведения в режиме реального времени, обеспечивать контроль достоверности предоставленной информации. Кроме того, применение распределённого реестра помогает предотвратить фальсификацию сведений и повысить уровень прозрачности взаимодействия с госорганами. В то же время существуют и сложности, среди которых — необходимость создания сборки, поддерживающей реализацию алгоритмов ГОСТ шифрования, и ее сопровождение, хранение конфиденциальной информации, нехватка квалифицированных специалистов на рынке.

Участники конференции DLTReg 2019 пришли к выводу, что технология блокчейн способна глобально преобразить бизнес, поэтому предпринимателям важно подготовиться к новой реальности, иначе можно оказаться за бортом быстро меняющегося рынка. Конференция позволила не только обозначить или прояснить вопросы регулирования технологии распределённых реестров, в частности, вопросы стандартизации и применения смарт-контрактов, но и увидеть реальную картину применения технологии в России, познакомиться с кейсами из сферы финансов, энергетики, ритейла, логистики и др.



Йорн Эрбгут, консультант по юридическим технологиям, блокчейну, смарт-контрактам и защите данных, преподаватель Женевского университета

ITSEF

XIII ЦИФРОВОЙ ФОРУМ

29-31 мая 2019

г. Казань

БОЛЬШИЕ ДАННЫЕ
КИБЕРБЕЗОПАСНОСТЬ
ЗАКОНОДАТЕЛЬСТВО

itsecurityforum.ru

ОРГАНИЗАТОР:

ICL СИСТЕМНЫЕ
ТЕХНОЛОГИИ



facebook

HI-HUME — HI-TECH: ВЫЗОВ ПРИНЯТ

КАК И ПОЧЕМУ ГУМАНИТАРНЫЕ АСПЕКТЫ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
СТАЛИ АКТУАЛЬНЫМИ

Информационная безопасность вообще и финансовой сферы в частности имеет не только технические, но и гуманитарные аспекты. До поры до времени гуманитарные аспекты оставались на втором плане, служили фоном для организационно-технических решений. В наши дни гуманитарные вопросы приобретают особенно большое значение. Без их решения невозможно полноценно обеспечить информационную безопасность: ни гражданина страны, ни финансовой отрасли, ни в национальном масштабе.

БЕСКУЛЬТУРЬЕ УЯЗВИМО

Чистая техника — абстракция. Даже природу мы воспринимаем в той степени, в какой её практически изменяет человек. Что уж говорить про чудеса научно-технического прогресса: их придумывают, создают и используют люди, исходя из своих интересов. С другой стороны, преобразование самого человека неотделимо от внешних инструментов. Среди которых есть разные и технические средства, и гуманитарные (информирование, обучение, воспитание и т.п., прямое физическое воздействие).

Поэтому информационная безопасность стала входить во все сферы повседневной жизни. Такая необходимость возникла по мере распространения высокотехнологичных сервисов, создаваемых на базе компьютеров и телекоммуникаций. В нашей отрасли — дистанционных финансовых услуг.

Примерно с середины 1990-х в центре внимания находились технические аспекты информационной безопасности. Однако программно-аппаратные решения, а тем более организационные меры не работают сами по себе. Для их применения нужны нормативно-правовая база, обучение и повышение квалификации специалистов, выработка общих подходов на деловых мероприятиях и в отраслевых изданиях. Эти гуманитарные по своему характеру направления поначалу выглядели вспомогательными для технических аспектов информационной безопасности, их инфраструктурой.

В 2010-е годы высокие технологии начали обширно применяться практически во всех гуманитарных сферах. На качественно новый уровень вышли сервисы государственного управления, политические, культурные, научные процессы, СМИ, образование и здравоохранение. Именно здесь наиболее ярко проявились гуманитарные аспекты информационной безопасности.

На первый план вышла угроза манипуляций человеком и общественным сознанием. Дистанционного, трансграничного управления, неявно-



**Павел
БЫЛЕВСКИЙ**

кандидат
философских наук,
шеф-редактор
BIS Journal

го — анонимного или замаскированного под дружественное воздействие. Аудиторию сознательно вводят в заблуждение, противопоставляя одних людей другим, чтобы побудить действовать в чуждых интересах, против собственных.

Скрытыми кукловодами могут выступать спецслужбы других стран, международные террористы, доморощенные экстремисты и мошенники, даже просто неуравновешенные, безответственные граждане. Под угрозой оказываются все интересы граждан: политические, культурные, экономические, социальные, вплоть до права на жизнь.

УГРОЖАЮЩЕ ГУМАНИТАРНОЕ

Спектр гуманитарных угроз информационной безопасности оказался широк. Начиная с хищения денег с банковской карты, вовлечения ребёнка в деструктивное сообщество в социальной сети и заканчивая распадом страны, гражданской войной в результате инспирированной извне «цветной революции». Именно такое видение проблемы сформулировано в актуальной «Доктрине информационной безопасности Российской Федерации», утверждённой 5 декабря 2016 года Указом № 646 Президента РФ.

Создание системы противодействия высокотехнологичным гуманитарным угрозам уже ведётся на федеральном, региональном и корпоративном уровнях. Банк России организует противодействие «социальной инженерии» в системах электронных платежей. Начат автоматизированный мониторинг деструктивных групп в социальных сетях, готовится пересмотр школьного курса безопасности жизни. Начинаний много, но им только предстоит выстроиться в единую систему.

Особенность гуманитарных угроз в том, что от них невозможно защитить человека извне, помимо его желания и сознательного активного участия. Единственный способ обезопасить общество и личность от гуманитарных угроз информационной безопасности — грамотное информирование граждан. Чтобы они знали об опасностях, которые сопутствуют таким удобным цифровым сервисам, умели их вовремя распознавать и противодействовать.

Широкая кампания формирования и повышения культуры информационной безопасности для всего населения нашей страны только начинает развёртываться. На этом фоне выпукло проявились гуманитарные аспекты собственно технического обеспечения информационной безопасности в отношении профессионалов.

Прояснилась важность не только профессиональных компетенций как таковых, но и личностных качеств специалиста. Зачастую именно последние играют решающую роль в том, выполнит

сотрудник задачу во что бы то ни стало или окажется слабым звеном «периметра». Став лёгкой жертвой манипуляций со стороны «социальных инженеров» или вообще оказавшись инсайдером.

Средства противодействия гуманитарным угрозам информационной безопасности при работе с персоналом также обширны. Начиная с преимущественно организационно-технических вопросов — обучения с особым вниманием к его воспитательным аспектам.

Внимание на всех уровнях к формированию как профессиональной, так и массовой культуры информационной безопасности будет только возрастать.

В этой сфере огромное количество важнейших вопросов, решения которых ещё только вызревают. Вопрос о соотношении технических и гуманитарных аспектов информационной безопасности решается в более широком контексте. Дело в важнейшей и острой проблеме современности, которая носит глобальный характер.

КРИТИЧЕСКИЙ ДИСБАЛАНС

Речь о критическом дисбалансе стремительного развития наукоёмких исследований, разработок и промышленных решений в двух сферах: с одной стороны в технической, с другой — в гуманитарной. В hi-tech ряд НИОКР прошли путь от «гаражных разработок», «стартапов» до глобальных компаний за кратчайшие исторические сроки. К 2019 году рыночная стоимость корпораций Microsoft, Google, Apple и Facebook превысила полтриллиона долларов США. Компания Стива Джобса была основана в 1976 году, а Марка Цукерберга — в 2004-м году.

Рынок инвестиций в hi-tech (только в информационные компьютерные технологии ИКТ) с 2013 года вырос с \$3,5 трлн до \$4 трлн (данные TAdviser). Для сравнения, рынок инвестиций в отрасли hi-hume за это же время, хоть и увеличивался рекордными темпами, достиг всего лишь \$800 млн (данные CB Insights Research).

Что такое hi-tech, знают все; но о том, что такое hi-hume — высокие гуманитарные технологии — до сих пор идут споры. К этой области относят исследования в области радикального преобразования человека: радикального омоложения, оздоровления, продления жизни, развития сверхспособностей. Такие разработки ведутся, их небезопасность также важна, но мы пока оставим этот вопрос в стороне.

Одни исследователи считают, что hi-hume — это просто традиционные гуманитарные дисциплины, только в век высоких технологий, с использованием компьютерных средств и телекоммуникаций. Другие отмечают: высокие



технологии сами по себе не могут сделать гуманитарные исследования наукоёмкими; однако открывают возможность для получения качественно новых результатов и продуктов.

С такой точкой зрения трудно не согласиться, учитывая колоссальный потенциал «больших данных» для мониторинга, сбора и анализа информации о человеке. На основании чего неизмеримо возрастает мощь адресного массового воздействия на аудиторию через электронную прессу и социальные сети.

ПРОТИВОСТОЯТЬ БЕСЧЕЛОВЕЧНОСТИ

Технические новинки в гуманитарной сфере, созданные на базе наукоёмких технологий, способствуют новой «культурной революции». Практические для всех и повсеместно доступными стали достижения науки, произведения искусства — книги, музыка, живопись, скульптура, архитектура, театр, кино, живое исполнительское мастерство, в том числе в прямой трансляции, новости и аналитика.

Появились колоссальные возможности культурного развития личности и общества. Но, учитывая особенности современного мира, эти новые возможности используются также для изощрённого манипулирования общественным сознанием в политических и коммерческих целях. Для провоцирования так называемых «цветных революций» и маркетинга малополезной, а то и вредной продукции, для вовлечения людей в деструктивные объединения, для совершения преступлений.

Водораздел именно здесь: речь идёт уже не о формальном отношении высоких технологий к гуманитарным сферам и дисциплинам. Дело в таком ключевом для определения гуманитарного понятия, как гуманизм. В его не отвлечённом, а конкретно-историческом смысле. Без решения этого вопроса, при его ошибочном или сознательном затушёвывании, высокие гуманитарные технологии легко приобретают антигуманный, бесчеловечный характер.

Ярких и наглядных примеров вставших проблем хоть отбавляй, даже непосредственно в финансовой отрасли. Это и развитие социального инжиниринга в системах электронных платежей. И практическое отсутствие полноценной воспитательной составляющей в средних и высших учебных заведениях, которые лишь «оказывают образовательные услуги». Это и распространение мошенничеств и деструктивных объединений в социальных сетях...

Указанные проблемы, как и другие вопросы безопасности наукоёмких технологий, не решать нельзя. Многие в этом направлении уже делается, но сделать предстоит гораздо больше. Для информирования об актуальной проблематике в этой области, ведения дискуссий, выработки решений и знакомства с передовым опытом мы открываем новый раздел Hi-Hume. Посвящённый гуманитарным аспектам обеспечения безопасности высоких технологий.

АНАТОМИЯ ДЕСТРУКЦИИ

«ЦИФРОВАЯ ГИГИЕНА» В СОЦСЕТЯХ — ЗАБОТА ОБЩАЯ



**Наталья
КАСПЕРСКАЯ**
Президент
ГК InfoWatch



**Игорь
АШМАНОВ**
Президент
АО «Крибрум»

28 марта 2019 года прошёл первый форум «Цифровая гигиена. Молодёжь в сети», посвящённый информационным угрозам и мерам защиты детей и подростков в виртуальном пространстве. На мероприятии собрались представители органов власти, регулирующих, образовательных и общественных организаций, психологи и специалисты в области информационной безопасности.

ГРУППЫ РИСКА

Подростки чаще других пользователей находятся в социальных сетях, стараются следить за новостями и обновлениями ленты. Самые популярные у них сети — «ВКонтакте», «Инстаграмм», «Твиттер» и «Ютуб». Проводят в социальных сетях почти треть своего времени. Там они находят друзей, узнают о субкультурах, входят в разные группы.

В социальных сетях всё активнее развиваются группы деструктивного воздействия. Они предлагают подросткам самореализацию себя, вовлекая в разные виды антиобщественной активности: расстрелы в школах («скулшутинг»), криминальную «романтику» («а.у.е.» — «арестантский уклад един»), суициды, наркотики. Активной деструктивной «раскачке» подвергается каждый третий подросток.

Действуют более 10 000 групп, которые провоцируют подростков совершать действия криминального характера, вовлекают в экстремистские группировки, «фанатские» и мошеннические организации, протестные движения. В подобных сообществах состоит около 1 млн подростков. Ситуация в социальных сетях стремительно ухудшается и может стать взрывоопасной.

В марте 2018 года Президент России В.В. Путин на встрече с женщинами-предпринимателями в Самаре отметил необходимость более тесного взаимодействия государства, бизнеса и общества в решении проблем деструктивного воздействия на детей и подростков в интернете. Эту проблему помогает решить поисковик и аналитическая система «Крибрум».

«Крибрум» — инструмент мониторинга социальных сетей («Инстаграмм», «Фейсбук», «Твиттер», «ВКонтакте», «Одноклассники»), а также блогов, форумов и комментариев к публикациям в средствах массовой информации. Технология больших данных позволяет делать

глубокий анализ по разным срезам. Суицидальные группы сейчас блокируются, поэтому там роста нет. Зато прирост численности членов ультрас-движений с марта 2018 года составил 9 млн человек.

МАНИПУЛЯТОРЫ НЕЗРЕЛЫМ

Аналитика позволяет увидеть взаимосвязанность деструктивных групп, выявить центральные и производные, вторичные. Часто владелец нескольких групп смежной тематики — одна группа лиц или один человек. Если деструктивных групп около 10 000, то их владельцев на порядки меньше. При необходимости воздействовать на них легко.

Ещё уже круг организаторов радикальных групп. Чаще всего они взаимосвязаны, имеют пересекающиеся множества членов, занимаются «перекрестным опылением», друг друга рекламируют. Наркотики, самоубийства, расстрелы и т.п. оказываются смежными, взаимодополняющими темами. Группы развиваются и мутируют, блуждают по «смежной» тематике. Например, уличные бои и драки в лесах, что затрудняет оперативно-розыскную работу.

Способ воздействия, в основном, визуальный: картинки. Движения имеют свою символику. Самореклама деструктивных групп ведётся разными способами, в том числе через родительские сообщества. Родителей, переживающих за своих детей, как бы «предостерегая», провоцируют распространять пугающую информацию о самоубийствах и т.п.

Это иезуитский способ вовлечения, вызывающий панику и цепную реакцию некритического распространения. Так, старт информационной кампании самоубийств был дан статьёй Галины Мурсалиевой «Группы смерти (18+)» в «Новой газете» от 16 мая 2016 года. В статье значение этого явления было сильно преувеличено, что и способствовало его популяризации, расширению аудитории.

Выявлены усиливающиеся тенденции вовлечения подростков в деструктивную активность. Начиная с троллинга, групповой травли, «кибербуллинга», когда ребёнка обижают, оскорбляют. Это явление существовало и прежде, но сейчас переходит в онлайн и, к сожалению, принимает более массовый характер. Вовлекают в экстремизм, в радикально оппозиционные организации, «ультрас», вплоть до террористических группировок, в наркома-

нию («не укололся — не жил»), чтобы использовать как рабочую силу для транспортировки наркотиков.

Незрелым сознанием манипулируют: хочешь быть «не таким, как все», поступай плохо. Пропагандируют «эстетику» хаоса и террора как единственно правильный образ жизни. Утверждение привлекательности, «крутости» насилия свойственно практически всем деструктивным группам.

Какие уязвимости подростковой психологии используют? С одной стороны, неприятие авторитетов, стремление разрушать, свойственные переходному возрасту 13–14 лет. С другой стороны, склонность действовать по шаблону. Эксплуатируют подростковые симпатии к героям или антигероям, завуалировано навязываются «образцы для подражания». Фальсифицируют критический пересмотр ценностей, «что такое хорошо и что такое плохо», некритически усвоенных в детстве. В этот важный момент подростку подсовывается ложная повестка.

СИТУАЦИЯ ОБОСТРЕТСЯ

Вовлечение начинается с того момента, когда подросток проявил своё отношение к группе: поставил «лайк», сделал комментарий, вступил в неё. Это ещё не полное погружение, а только первые «витки» «воронки вовлечённости». «Воронка вовлечения» выглядит так. Вначале идут группы «широкого охвата», чтобы просто вызвать интерес к теме, переключив с чего-то популярного.

Негатив вначале очень трудно уловить, на него переводят постепенно. Прощупывают «слабину» подростка, и начинают «двигать» в этом направлении: наркотики, самоубийства, «зацеперы», избиения... Вовлекают в специализированные группы. Там уже все «свои». Новичкам раздают роли, «чины» и «звания», предлагают «карьерный рост».

Следующий этап — переход в закрытые группы. Приглашают участвовать в опасных играх, формируют у подростков готовность быстро, не задумываясь, выполнить приказ. Действует методика выдачи заданий детям: куда-то пойти, что-то сделать. Не выполнил — из сообщества исключают, ребёнок превращается в изгоя.

Сложность заданий и глубина вовлечённости постепенно, пошагово увеличиваются. Вовлечённых подростков готовят к реальным действиям. В «наркотических» группах — пробовать, распространять. Так исподволь, скрытно ведётся дрессировка живых людей, несовершеннолетних. Манипуляция, отбор наиболее внушаемых, и «перепрошивка» их

сознания. Общечеловеческие ценности обнуляются, взамен формируются нужные «кукловодам».

Деструкторам важно «накручивать» общее ощущение неблагополучия, нестабильности. Вне зависимости от того, как на самом деле обстоят дела. Подросток может жить в очень благополучном месте, лично с ним, в его семье и у близких всё может быть очень хорошо. И у такого можно развить недовольство, дискомфорт: всё могло бы быть намного лучше!.. Всё начинает не нравиться, нужны перемены!.. Это подготовка к конкретным деструктивным действиям для социально-политической дестабилизации, вплоть до «пойди и убей».

Анализируя отношение участников деструктивных групп к политике, об искусственной «политизации» следует сказать особо. Шокирующему контенту присовокупляются политические оценки. Даже в «наркоманских» группах, казалось бы, далёких от политики, таких публикаций около 20%. Характерно, что носители радикальных политических идей часто являются членами деструктивных сообществ.

Анализ информационного поля в социальных сетях вокруг «керченского стрелка» показывает искусственную политизацию. Чуть ли не «кровавый режим расстреливает детей», совершенно нелепые «конспирологические» версии про «роль спецназа». Потому что «всё равно государство виновато». Политизация бывает стихийная, со стороны пользователей, а бывает целенаправленная. Последняя проявляется в призывах к деструктивным действиям в реальности. Деструктивные движения, существующие онлайн, всё больше двигаются в сторону оффлайна.

Ситуация за год резко обострилась. Каждый третий подросток находится «в обработке» у профессиональных манипуляторов. Они разрушают базовые ценности и переориентируют неокрепшее сознание на деструктивные действия. Сами подростки этого не осознают. Увидеть это, понять и сознательно действовать могут взрослые... которые, увы, для подростков «не авторитеты».

Для противодействия этим деструктивным тенденциям нужно объединение усилий. Обязательно вести мониторинг, законодательно обеспечить ограничение распространения деструктивного контента и, главное, замена позитивной повесткой, конструктивным контентом.

ПРОФЕССИОНАЛИЗМ: ПО ТУ СТОРОНУ ДОБРА И ЗЛА?

«РОДИНУ ЛЮБИТЬ НЕ ОБЯЗАН», ИБО НЕТ ТАКОГО ТРЕБОВАНИЯ К СПЕЦИАЛИСТУ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, НИ В ОБРАЗОВАТЕЛЬНЫХ, НИ В ПРОФЕССИОНАЛЬНЫХ СТАНДАРТАХ



Виталий ГРИГОРЬЕВ
заведующий кафедрой
«Информационное
противоборство»
Института
комплексной
безопасности
и специального
приборостроения
РТУ МИРЭА, к.т.н.

Современное профессиональное образование у нас проводится в формате «оказания образовательных услуг». Образовательная система будто самоустранилась от решения воспитательных задач. Запоздалые попытки компенсировать эти упущения «кодексом профессиональной этики специалиста по информационной безопасности» напоминают народную мудрость о том, что «поздно пить «боржоми»... На самом деле чётко артикулированный целенаправленный воспитательный процесс должен быть нераздельно связан с обучением. Только так можно обеспечить полноценную подготовку настоящего профессионала.

БЕЗРАЗЛИЧИЕ К НЕВОСПИТАННОСТИ

В настоящее время на вузы, как и на школы, государством не возложены воспитательные задачи. Что связано с отсутствием официальной государственной идеологии и внятно сформулированной «национальной идеи». Некогда был «учебно-воспитательный процесс», а сейчас воспитательная функция не входит в задачи обучения. Сейчас воспитание отдаётся на откуп только семье, «в факультативном формате», на усмотрение родителей.

Современные родители формировались как личности в конце 1980–1990-х годов, поэтому у многих из них самих размыты представления о важности воспитания и о целевых функциях суверенного государства. У них зачастую нет чётких ориентиров о предназначении России как духовного светоча для всего мира, представлений о прошлом нашей Родины в потоке исторического процесса. Родители готовы

кормить-поить детей, платить за их обучение, но хотят, чтобы их хорошо воспитывал кто-то другой, начиная с детского сада.

Местами действуют разные молодёжные организации, клубы по интересам. В июле 2003 года Президент России В. В. Путин заявил на совещании по проблемам развития малых городов, что объединяющей идеологией должен быть патриотизм. После этого начали развиваться историко-патриотические организации. Но и они полноценно не могут заменить бывшие комсомол и пионерию. Дети и молодёжь остаются предоставлены, как правило, сами себе. Реальная дружба уходит в виртуальный мир смайликов, фейков, репостов и лайков.

Образовательные и профессиональные стандарты подробно описывают различные компетенции. Однако ни один не указывает, что специалист, прежде всего, независимо от получаемой профессии, изначально должен любить Родину, быть достойным её гражданином. Не предъявляется и требований культурного, этического характера, необязательно знать историю своей страны, быть социально активным. Те, кто попал в армию по призыву или сознательно избрал себе профессию «Родину защищать», дают торжественную присягу «на верность своему Отечеству — Российской Федерации». Но надо признать, что большинство молодёжи учится именно в гражданских вузах. И именно они потом придут трудиться в государственные или коммерческие структуры. Вопрос, а что для них есть «верность своему Отечеству»? Культивируемый фетиш «рынка труда без границ» подавляет чувство гражданственности и своих обязательств перед воспитавшей их Родиной.



КОМИТЕТ
ОБЩЕСТВЕННЫХ СВЯЗЕЙ
И МОЛОДЁЖНОЙ ПОЛИТИКИ
ГОРОДА МОСКВЫ

Публикация подготовлена в рамках проекта «Безопасность цифровой экономики Москвы: Новое поколение», поддержанного грантом Мэра Москвы №085-МГ/18



Более того, определённые круги навязывают моду непременно находиться в оппозиции к общественным ценностям. Если и любить Отчизну, то только «странною любовью». Любить Родину, оказывается, можно и с двойным гражданством. Такая «оригинальная» гражданская позиция соблазнительно проста для студентов. Так же, например, как манера неряшливо одеваться, публично общаться, в том числе, и в общественных местах с помощью нецензурной лексики. Выпускнику высшей школы достаточно стать таким «образованцем», чтобы формально быть причисленным к интеллигенции. Но «образованцы» и интеллигенты суть разные по смыслу и содержанию понятия. К сожалению, мир наполняют в большей части «образованцы» с высшим образованием, к которым, к сожалению, малоприменимо понятие истинной интеллигентности, в основе которой всегда лежал, прежде всего, высокий уровень культу-

ры, как бытовой, так и построенной на высших достижениях отечественной и мировой мысли о духовных ценностях, свойственных именно Человеку.

В этом плане в нашем Университете практически для всех студентов, независимо от формы обучения и профессиональной ориентации читается курс «Национальная система информационной безопасности», в рамках которого студенты знакомятся не только с законодательными актами в этой сфере, начиная с Конституции РФ и Доктрины информационной безопасности РФ, и получают знания об исторической миссии России как центра духовности и гуманности. Меняются информационные технологии, меняются и сами люди. Но не должны меняться главные духовные ценности, которые и составляли основу социокультурного кода России, независимо от общественно-политического устройства государства. Именно чувство веко-

вой справедливости и духовного единства, чувство национального патриотизма позволяло нашим пращурам отстаивать независимость нашей Родины на протяжении веков. До студентов доводится основная мысль, что Национальная система информационной безопасности современной России строится на глубоком понимании угроз информационной безопасности и её суверенитету, появившихся не сейчас, а имеющих многовековую предысторию. Умение разобраться в реальной информационной обстановке за шелухой словес электронных СМИ, понять истоки и риски реальных угроз для России за шторой отвлекающих ложных информационных образов и фейков, вот какой компетенцией, как нам представляется, должен обладать выпускник нашего вуза.

ДОКТРИНА О ГУМАНИТАРНОМ

Непродуктивно понимать профессиональные навыки только как набор знаний, умений, навыков, компетенций, необходимых для успешного выполнения служебных обязанностей. Вырастив прекрасного специалиста в области информационной безопасности, нужно быть уверенными, что он будет работать на благо страны и общества в этой сфере. Важно помнить, что есть и иные пути профессиональной самореализации, успешной карьеры, которые идут вразрез с этими ценностями.

Вузы, особенно государственные, готовят специалистов с высшим образованием на средства, выделяемые из бюджета страны. Высшая школа должна работать, учитывая долгосрочные интересы общества в информационной сфере, и не только. Для этого есть базовые официальные документы. Такие, как «Доктрина информационной безопасности Российской Федерации», которая была утверждена 5 декабря 2016 года Указом № 646 Президента России. Также «Стратегия национальной безопасности Российской Федерации», утверждённая 31 декабря 2015 года Указом № 683 Президента России.

Эти программные документы должны быть основополагающими при формировании профильными вузами учебных предметов, курсов и планов. В них информационная безопасность

не сводится к чисто техническим аспектам, тому, что называют «кибербезопасностью». Наравне с этим широко рассматриваются её гуманитарные, социально-психологические аспекты.

Забвение гуманитарных аспектов информационной безопасности при подготовке профессионалов чревато в дальнейшем серьёзными инцидентами. Получается, мы готовим профессионала «по ту сторону добра и зла», в духе названия известного труда реакционного философа Фридриха Ницше. Но кем станет после окончания вуза такой выпускник, пусть и заслуживавший самые высокие оценки в процессе учёбы? На какой ниве он начнёт делать профессиональную карьеру, как и где будет пытаться снискать свой жизненный успех?

БОРЬБА ЗА УМЫ И ДУШИ

Хорошо ли будет, если лучшие выпускники, подготовленные за государственный счёт, уедут работать за рубеж? Не секрет, что самым способным специалистам там могут предложить намного лучшие условия труда и оплаты, чем у нас в стране. Там специалист-эмигрант будет работать, как минимум, не в интересах своей Родины. В лучшем случае. В худшем — ему могут поручить работу, направленную против неё, во вред. В таком случае получается, что вузы на деньги государственного бюджета подготовили прекрасного специалиста... для недружественной страны.

Есть и другое «поприще» для молодых специалистов по информационной безопасности. Это сфера «хакерства», часто на грани закона, а порою откровенно криминального. Особенно в сфере электронных финансов, например, в области майнинга криптовалют. Шансы на быстрый, лёгкий и большой заработок могут вскружить головы высокопрофессиональным недорослям.

Матёрые злоумышленники-рецидивисты пытаются рекрутировать в кибербанды именно таких «спецов». Эксплуатируя гражданскую незрелость юных дарований, прельщая их ложной «романтикой» риска, в том числе тюремной (например, АУЭ). Это может работать, и время от времени срабатывает, ломая человеческие жизни. Но откуда у студента взяться серьёзному жизненному опыту, если и в вузах сегодня не «воспитывают», не учат различать добро со злом?

Зато этому по-своему «учат», известно, в чьих интересах, голливудские фильмы «про хакеров». Такие триллеры как «Газонокосильщик», «Враг государства» и «Матрица» формируют безнадежный образ кибер-антиутопии, лишая воли к жизни и сопротивлению. В СССР была своя

Забвение гуманитарных аспектов информационной безопасности при подготовке профессионалов чревато в дальнейшем серьёзными инцидентами

культура, которая должным воспитательным образом воздействовала не только на молодёжь, но и на взрослых людей. «Золотой запас» фильмов, музыки, песен, книг, картин, скульптур, памятников архитектуры тех лет и сейчас широко популярен. Их потенциал добра, красоты и патриотизма по-прежнему высок. В новой России шедевры подобного воспитательного накала пока находить нелегко.

Некоторое время у части российского студенчества наблюдались низкопоклоннические настроения, стремление «свалить» за границу в поисках «лучшей доли». Эта дешёвенькая «мода» начала сходить на нет лишь в последние годы, после воссоединения Крыма с Россией. Положительную роль в этом нравственном очищении сыграло чувство естественного протеста против публичного унижения наших спортсменов на Олимпийских Играх 2018 года, поводом которого послужил сфабрикованный «допинговый скандал». Это не показной, «балалаечно-матрёшечный» патриотизм, а глубокое чувство, особое состояние души — вдохновения на великие свершения.

ДЕСТРУКЦИЯ ЧЕЛОВЕЧНОСТИ

Дело в том, что высокие технологии в гуманитарной сфере зачастую используются не на пользу, а во вред человеку. Точнее, одни люди используют их против других как информационное оружие, техническое и гуманитарное. Чтобы ими можно было управлять в своих интересах, эксплуатировать к собственной выгоде.

Ведётся злонамеренная спекуляция на реальных успехах высоких технологий, которые действительно улучшают повседневную жизнь человека. Автоматизированные системы управления технологическими процессами многократно повышают производительность труда, высвобождая людей для решения творческих задач. Много хорошего и полезного высокие информационные технологии приносят и в гуманитарную сферу, поэтому люди склонны им доверять, не ожидая подвоха.

Возьмём, для примера, дистанционное обучение. Которое открывает перед жителями регионов огромные возможности. В том числе для получения трансграничного образования, «не вставая со стула». Вместе с тем значительно сокращается живой личностный контакт студента с педагогом. Обрывается последняя ниточка, сохранявшаяся после «освобождения» школы и вузов от «непрофильных» воспитательных функций.

Пока в образовании и в обществе в целом наблюдается «воспитательный вакуум», его заполняют весьма сомнительные, а зачастую

Закулисные специалисты и их публичные представители посредством глобальных информационных социальных ресурсов целенаправленно и адресно воспитывают российскую молодёжь в деструктивном ключе

и, несомненно, вредные «источники». Это, как повелось с пресловутой «перестройки» во второй половине 1980-х годов, «чернушные» кинофильмы, «рэп-культура», терпимость к «лёгким наркотикам», к половой неразборчивости, «европейская» мода на «унисекс». В компьютерном мире это социал-дарвинистские компьютерные игры-«стрелялки» и сектантские группы в социальных сетях.

Закулисные специалисты и их публичные представители посредством глобальных информационных социальных ресурсов, по сути, контролируя и управляя ими, целенаправленно и адресно воспитывают российскую молодёжь в деструктивном ключе. Разрабатывают и реализуют «увлекательные» методики, специально рассчитанные их «педагогами» и «психологами» для незрелых умов и бурлящих чувств. Социотехнологии антигуманного характера оттачиваются на участниках молодёжных «клубов самоубийц» в социальных сетях. Таким образом, отрабатываются инструменты «расчеловечивания» молодого поколения, превращения его в слепое орудие чужой воли.

ПРОИЗВОДСТВО ВИРТУАЛЬНЫХ ЗОМБИ

Механизм манипулирования молодыми умами таков. Реальность подменяется виртуальным миром, в ней производится деструкция сознания, совершается культурное «перекодирование». В таком виде молодой «зомби» воспринимает уже реальную жизнь как что-то виртуальное, как на мониторе компьютера. Потому и готов делать уже в жизни что угодно и с другими людьми, и с собой.

Инциденты, подобные массовому расстрелу в школе, совершённого «керченским стрелком», являются закономерными эксцессами подобных манипуляций с сознанием молодёжи. Авторам и исполнителям людоедских «гуманитарных технологий» такая цена, по всей видимости, представляется приемлемой. Неизбежной издержкой массового производства одномерных людей-атомов, «заточенных» на успех без труда, на потребление и гедонизм, послушных «внешнему управлению» и манипуляциям.

Потому что на кону — огромный бизнес и большая политика. Ставки на рынке «научно-технологических гуманитарных технологий» быстро растут. Отточенные высокотехнологичные инструменты, позволяющие успешно манипулировать общественным сознанием, в большой цене. Ведь они помогают бизнесу успешно продвигать рекламу, наращивать продажи ненужных и даже вредных товаров. В политике бесчеловечные, антигуманные «гуманитарные технологии» являются инструментами превращения молодёжи в пушечное мясо «цветных революций», в таран для демонтажа «неудобных режимов».

Чтобы эффективно противодействовать этой деструктивной работе, необходимо вести мониторинг и аналитику повседневной поведенческой активности студентов, молодёжи в целом. В социальных сетях его вести ещё легче, даже чем живущим в одном общежитии невольно наблюдать друг за другом. Чаще всего человек бывает виден как на ладони. Тогда легко вовремя прийти на помощь товарищу, предостеречь его от явно ошибочных поступков. Депрессия, готовность убивать, как правило, проявляются в аккаунте в социальной сети задолго до трагедии. Так было и с «керченским стрелком», но никто своевременно не отреагировал, не предотвратил непоправимое.

Сейчас, при отсутствии комсомола, опекаемого парткомом, трудно представить, кто бы мог успешно выполнять эту важную функцию. Сомнительно, чтобы студенческие профсоюзы и советы могли бы заинтересованно и успешно вести такую нужную работу. Очевидно, что нужны новые прогрессивные формы работы с молодёжью, ориентированные на использование технологий информационных инструментов «формирования душ», которые понятны и близки им. Так, например, сегодня говорится о создании «кибердружин». Они могли бы бороться не только со злоумышленниками — «техническими» хакерами, но и отслеживать попытки «гуманитарных» злоупотреблений высокими технологиями. Этот вопрос требует самой серьёзной многосторонней проработки, включая внесения изменений в нормативно-правовую базу.

ПОБЕЖДАЕТ ДОБРО, А НЕ «БАБЛО»

Суть образования — в единстве обучения и воспитания, которое, в то же время является и самовоспитанием. Нельзя научиться чему-то серьёзному, не изменив самого себя. Образование нужно для познания окружающего мира и своего места в нём. Чтобы своим трудом менять к лучшему жизнь, других людей и свою. Стать продолжателем дел своих предшественников, в свою очередь, заложить фундамент для сле-

дующих поколений. Этой цели служат научные школы. Невозможно успешно выполнить эти задачи, не зная истории своей страны, игнорируя судьбы и заботы других людей.

Во встрече с учителями — наставниками выпускных классов, которая состоялась в преддверии Всероссийского дня выпускника 21 июня 2017 года, Президент РФ В. В. Путин отметил: «Получить знания — это непросто, современные особенно, широкие знания, но это всё-таки вторичное по сравнению с воспитанием человека, с тем чтобы он должным образом относился и к себе самому, и к своим друзьям, и к семье, и к Родине. Это абсолютно фундаментальные вещи». Можно с полной уверенностью сказать, что эти слова можно отнести и к студенческой молодёжи, тем более, что ею становятся вчерашние выпускники школ.

С этой точки зрения в вузах, особенно готовящих специалистов в области информационной безопасности, важны исторические традиции. Музеи, размещение в публичных местах портретов выдающихся отраслевых учёных и специалистов, информационных стендов. Наглядный «исторический дискурс» нужен на разных уровнях: как вуза, так и ведущих подразделений, кафедр. Как, например, это сделано в МГТУ им. Н. Э. Баумана, которому уже почти два века.

Эффективным элементом воспитательной работы в вузах выступают «галереи героев» — собственных сотрудников, выпускников разных эпох: Российской Империи, лауреатов Сталинских и Ленинских премий, Героев Социалистического труда, а также «живых легенд» современной России. В нашем Университете такие галереи выдающихся учёных, работавших и преподававших в МИРЭА, МГУПИ и МИТХТ, есть в каждом кампусе. В то же время, есть потенциал развития у наших студентов исторической памяти о родоначальниках и великих достижениях отечественных учёных в выбранной ими профессии. Важны исторические экскурсии наподобие истории отечественной криптографии «в лицах». В том числе, о только открывающейся «воюющей криптографии», о вкладе советских шифровальщиков в Победу в Великой Отечественной войне. Вот где кладезь сюжетов для самых увлекательных кинофильмов-триллеров!

Свежие, увлекательно поданные исторические примеры помогут молодым специалистам понять, «делать жизнь с кого», и наоборот, знать, кто такие «антигерои», «плохиши», уметь распознавать их в жизни. Через проекцию на личности студенты лучше будут понимать, что такое хорошо и что такое плохо, усва-



ивать разницу между добром и злом. Приходя к выводу: зло может быть побеждено только добром, а не «баблом».

СКВОЗНОЕ ВОСПИТАНИЕ

Большое воспитательное воздействие оказывают яркие запоминающиеся ритуалы. Такие как посвящение вчерашних абитуриентов в студенты, в РТУ МИРЭА их в этот день приветствует ректор С.А. Кудж и Президент РТУ академик РАН А.С. Сигов. Завершающим ритуалом является посвящение выпускников в профессию. Здесь уместны обычаи типа Гиппократовой клятвы у медиков. Студент, аспирант, молодой специалист должны ощущать эмоциональную сопричастность живой исторической традиции, а себя — её продолжателями.

Большое значение для профессиональной ориентации и выявления лучших и перспективных ребят имеет целевая работа со старшеклассниками. Среди самых эффективных мероприятий — Межрегиональная олимпиада школьников по математике и криптографии, другие профильные олимпиады. Незабываемо эффектно, в значимых местах проходят церемонии награждения победителей. На площадке РТУ МИРЭА проводятся соревнования «Кибербиатлон», аналогичные — специализированными школами, как, например, «Кибертон» ГБОУ г. Москвы «Школа № 1770». Это важный этап «сквозного» учебно-воспитательного процесса подготовки молодых специалистов.

Молодёжью востребованы увлекательные форматы состязаний, которые одновременно несут воспитательную «нагрузку». РТУ МИРЭА выступил «запевалой» такого популярного направления, как командные соревнования по информационной безопасности формата CTF (capture the flag, захвати «флаг» у соперника). Преподаватели и студенты нашего вуза вносят

большой организационный вклад в их проведение, а потом наша команда, соревнуясь с представителями других вузов, занимает призовые места.

Большую роль в подготовке студентов играет производственная практика, которую они проходят в лучших организациях и компаниях отрасли. Чуткое руководство практикой со стороны состоявшегося специалиста, пример его личности дают заметный положительный воспитательный эффект. Практика может играть решающую роль в дальнейшем трудоустройстве выпускника, играть роль старта его профессиональной карьеры. В этом плане у нас есть хороший отечественный исторический опыт: учебно-научно-производственные комплексы, в которые входили вузы, исследовательские организации и промышленные предприятия. Такого рода структуры, но в новом прочтении, в виде учебно-научно-производственных кластеров, создаются уже в настоящее время в РТУ МИРЭА. Очевидно, что за ними будущее!

Хороший специалист должен не только мастерски, во всех тонкостях овладеть секретами своей профессии, но и сформировать себя как целостную личность. Быть патриотом своей Родины, иметь чёткие нравственные ориентиры, обладать убеждённой в своей правоте и несгибаемой волей к великим свершениям. Слова великого Н.А. Некрасова «поэтом можешь ты не быть, но гражданином быть обязан» в полной мере относятся и к специалистам по информационной безопасности. Эти человеческие качества будущего профессионала должны интенсивно развиваться со школьной парты, со студенческой скамьи.

Отборочный этап соревнований по информационной безопасности — «Кибербиатлон 2019» на базе МИРЭА — Российского технологического университета (фото: www.mirea.ru)



**Марина
БРОДСКАЯ**
обозреватель
BIS Journal

СТФ — ИСТОЧНИК КАДРОВ

НО КАК ПРЕВРАТИТЬ ИГРАЮЩИХ ШКОЛЬНИКОВ В ПРОФЕССИОНАЛОВ ИБ?

Где искать кадровый резерв, как не в школе, подумали крупные игроки на рынке ИБ, и на крупном столе всероссийских соревнований по защите информации RuCTF поставили вопрос о переходе турниров на пятиуровневую систему. Теперь низший уровень соревнований проводится в школах и университетах, а победители первого уровня встречаются в международных финалах.

ОТ ШКОЛЫ ДО МАГИСТРАТУРЫ

Школьные соревнования по ИБ в формате учебного СТФ уже проходят во многих школах. Например, в декабре 2018 г. для московских школьников прошёл турнир «Кибербезопасник». Четыре часа ученики противостояли киберугрозам, обезвреживали вирусы, находили уязвимости web-приложений и пр. Принять участие в этих соревнованиях могли ученики с первым или нулевым уровнем владения программированием.

Для более продвинутых и уже организованных в команды старшеклассников проходят региональные соревнования в формате настоящего СТФ. По традиции, принять участие в отборочном онлайн-этапе могут все зарегистрировавшиеся команды, а победа в первом заочном туре даёт право участвовать в очном этапе. Например, открытые соревнования для школьников и студентов Уральского ФО ежегодно

проходят в октябре. В отдельных зачётах выявляется сильнейшая команда региона среди студентов, школьников и команд ПОО (колледжей). Принять участие в очном (для жителей Тюмени) или онлайн турнире могут все желающие.

Осенью 2018 г. в инновационном центре Сколково состоялся II Кубок СТФ России, собравший команды школьников и студентов (колледжей и вузов), занявших первые места в региональных соревнованиях. Такой крупный турнир (143 участника в составе 21 команды из 14 городов РФ) позволил выявить действительно достойных. Победителем стала команда VoidHack из Уральского федерального университета.

В ЭТОМ ГОДУ

Только завершаются соревнования одного года, сразу начинаются турниры следующего. Так, в марте состоялся отборочный тур международных открытых соревнований VOLGA CTF, которые собирают более 1000 команд со всего мира. Финал соревнований пройдёт в сентябре в Самаре при участии и поддержке СГУ и Департамента информационных технологий Самарской области.

В этом году в числе организаторов VOLGA CTF появился и «Ростелеком-Solar», который заключил соглашение о стратегическом партнёрстве, нацеленном на кадровое развитие Са-

марской области в сфере кибербезопасности, с Самарским национальным исследовательским университетом им. С.П. Королёва.

Также в марте состоялись и IV Региональные соревнования Altay-SchoolCTF-2019. Турнир проводился среди старшеклассников Алтайского края. Занявшие призовые места, получили приглашения на Межрегиональные межвузовские соревнования AltayCTF-2019, которые пройдут в июне в Барнауле в рамках международного форума «Электронная неделя на Алтае».

В апреле 2019 г. в Институте космических и информационных технологий Сибирского федерального университета пройдут KrasCTF — открытые межвузовские соревнования, проводимые университетом при поддержке МОО «Ассоциация руководителей служб информационной безопасности» (АРСИБ) и спонсоров.

Соревнования СТФ пройдут и в рамках Международной недели кибербезопасности (Global Cyber Week), которая впервые состоится в Москве в июне и объединит техническую конференцию OFFZONE-2019 и II Международный конгресс по кибербезопасности. Организатором Недели выступает ПАО Сбербанк.

ПРО RUCTF ОТДЕЛЬНО

Победители многих региональных турниров могут принять участие в старейших в стране соревнованиях RuCTF.



КОМИТЕТ
ОБЩЕСТВЕННЫХ СВЯЗЕЙ
И МОЛОДЕЖНОЙ ПОЛИТИКИ
ГОРОДА МОСКВЫ

Публикация подготовлена в рамках проекта «Безопасность цифровой экономики Москвы: Новое поколение», поддержанного грантом Мэра Москвы №085-МГ/18

В конце апреля в Екатеринбурге они пройдут в тринадцатый раз. В 2008 г. в RuCTF приняли участие всего восемь команд, в 2015 г. турнир вышел на международный уровень, а в прошлом году только в финале участвовали команды из восьми стран.

Сегодня RuCTF — самый масштабный турнир в области спортивного хакинга в России. К участию в финале приглашаются топ-50 команд из 54 стран. Соревнования проводятся по международным правилам Attack/Defence Capture The Flag. Победа в RuCTF даёт право участвовать в очном финале международного турнира DEF CON CTF, который ежегодно проходит в Лас-Вегасе и собирает сильнейшие команды мира.

ИГРА ПО-ВЗРОСЛОМУ

Многочисленные CTF проходят не только для новичков — школьников или студентов. Так, 8–11 апреля в Сингапуре, на конференции Kaspersky Security Analyst Summit (SAS), прошёл финал IV Международного турнира по индустриальной кибербезопасности Capture the Flag (CTF). Там специалисты без скидок на возраст и образование проверили защищённость умных устройств и промышленных систем.

Программа большинства крупных межрегиональных соревнований в формате CTF сегодня включает не только встречи команд, но и конференции с участием звёзд информационной безопасности, и олимпиады по защите информации, которые нередко входят в список Всероссийских Студенческих Олимпиад, дающих право на поступление без экзамена в магистратуру нескольких университетов.

Соревнования серии CTF поддерживают Минобороны РФ, Минкомсвязи РФ, Минобрнауки РФ, ФСТЭК России, ИПИ РАН, Федеральное Учебно-методическое объединение по образованию в области ИБ... В числе организаторов и спонсоров соревнований выступают МОО АРСИБ и Центр инновационных технологий «Сколково», ведущие международные компании в сфере ИБ, разработчики телекоммуникационного оборудования, платёжные системы и пр. Например, в пла-

«Этот CTF развеял все сомнения насчёт моих навыков. Я знаю, что мне ещё многое предстоит узнать, но я также знаю, что не притворяюсь»

нах АРСИБ на 2019 г. — порядка 40 школьных и студенческих соревнований CTF.

ПОИГРАЛИ, ПРОИГРАЛИ И... ВЫИГРАЛИ

Что такое CTF для участников? Для школьников — это первая проба сил, для студентов — понимание на практике того, чему учат в теории, для профессионалов в области ИБ — возможность проверить свои силы, тренинг роста.

В немногочисленных отчётах об участии в соревнованиях разного уровня специалисты рассказывают, как разгадали хитроумный шифр, проанализировали логи, дампы и файлы, нашли вирус в системе и многое другое. Вот, например, один из отзывов на ресурсе «Библиотека программиста» (proglib.io): «Это был хороший старт для новичка, он помог мне почувствовать свою принадлежность к сфере. Временами, особенно в технической специальности, легко стать жертвой синдрома самозванца. Этот CTF развеял все сомнения насчёт моих навыков. Я знаю, что мне ещё многое предстоит узнать, но я также знаю, что не притворяюсь. Также это было хорошей тренировкой для ума и помогло мне расширить знания по информационной безопасности. Несмотря на то что мои фундаментальные знания увеличились незначительно, я многому научилась, решая задачи, о которых не знала раньше или знала, но не знала, как их решить. Чтобы изучить новые технологии, разработчики создают приложения, с этой же целью специалисты по безопасности конкурируют друг с другом и занимаются взломами».

КАДРОВЫЙ РЕЗЕРВ ЗА ШКОЛЬНОЙ ПАРТОЙ. ОПЫТ «РОСТЕЛЕКОМА»

Цитирую статью на портале HR-tv.ru: «Ростелеком» за короткий срок сформировал кадровый резерв из 1500 ло-

яльных и компетентных школьников IT-профиля. Для этого был проведён «Кибервызов». Что это такое? Онлайн-олимпиада по информационной безопасности в формате CTF, образовательный курс для 60 лучших участников на базе «Сириуса», финальный квест со спецоперацией в ракетном хранилище, аудитом безопасности настоящей Tesla S и спасением планеты».

Руководитель проекта Юлия Кукина рассказала, что компания «Ростелеком» поставила задачу резко увеличить лояльность школьной аудитории, вовлечь ребят в деятельность компании, заинтересовать проектами и обеспечить хорошее погружение в теорию и практику. Всё это для того, чтобы сформировать верхушку рынка молодых IT-специалистов через 4–5 лет.

Онлайн-олимпиада обеспечила максимальный охват аудитории, в ней могли принять участие все желающие. Отборочная игра в формате CTF проходила в сентябре 2018 г. и длилась пять дней. Многочисленные задания делились по темам: реверс-инжиниринг, веб-безопасность, криптография, форензика, стеганография и программирование подсистем безопасности. Рейтинг конкурсантов был доступен онлайн. Знания 150 лидеров рейтинга перепроверили посредством интервью по скайпу. 60 финалистов олимпиады прошли очное интенсивное обучение по ИБ в образовательном центре «Сириус» в Сочи.

Там же прошёл и финал: школьникам надо было расследовать хакерскую атаку на ракетное хранилище с боеголовкой, восстановить работу компьютерной системы и разработать модель защиты, исключающую повторный инцидент. А также удалённо открыть электромобиль Tesla S, брошенный по сценарию злоумышленниками, найти лог-файл, узнать из него маршрут перемещения преступников и спланировать операцию по их задержанию.

По итогам акции «Ростелеком» охватил более 3 млн человек, на треть повысил лояльность к компании и сформировал кадровый резерв из 1500 активных участников, принявших участие в онлайн-туре.

Победители «Кибервызова» получили от 5 до 10 дополнительных баллов при поступлении на профильные кафедры технических вузов. А в планах организаторов — включение олимпиады в пе-

речень олимпиад, которые дают 100 баллов за ЕГЭ по информатике, а также расширение образовательной программы на студентов.

* * *

Кадровые проблемы отрасли можно решать разными способами: традиционными, как принято в Универ-

ситетах с классическим подходом к образованию, или в духе времени, когда путём охвата массовой аудитории через сито конкурсов отбираются сильнейшие и заинтересованные в получении новых знаний студенты и школьники.

Вот только без получения ими классического образования всё же не обойтись...

КОД ВЕРЧЕНКО

МЕЖРЕГИОНАЛЬНОЙ ШКОЛЬНОЙ ОЛИМПИАДЕ ПО КРИПТОГРАФИИ, МАТЕМАТИКЕ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ПРИСВОЕНО ИМЯ И.Я.ВЕРЧЕНКО¹

В Математическом институте РАН имени В.А. Стеклова состоялось торжественное закрытие XXVIII Межрегиональной олимпиады имени И.Я.Верченко, проводимой по профилям «Криптография и математика» и «Компьютерная безопасность». На награждение были приглашены победители и призёры олимпиады, а также старшеклассники, учителя и руководители ряда школ столицы, преподаватели вузов, представители отечественных компаний, работающих в области ИБ.

Памятные дипломы и значки победителям вручил председатель оргкомитета, лауреат Государственной премии СССР, заслуженный деятель науки РФ, действительный член Академии криптографии РФ Владимир Николаевич Сачков.

Для старшеклассников провели ряд интересных мероприятий. Среди них — выступление эксперта по информационной безопасности Кирилла Ермакова и показ документального фильма «Код Верченко» о замечательном учёном Иване Яковлевиче Верченко, имя которого с этого года носит олимпиада. Кроме того, школьникам помог-

ли разобраться с особенностями заданий прошедшей олимпиады, провели экскурсию по «Лаборатории популяризации математики» и встречу с представителями компаний-разработчиков средств защиты информации. Особый интерес вызвал мастер-класс по отражению компьютерных атак на киберполигоне МИРЭА.

Параллельно представители преподавательского сообщества и специалисты в области ИБ приняли участие в круглом столе «Безопасность цифровой экономики Москвы: школа – вуз – работодатель». Его участники обсудили

новые проекты «Математическая вертикаль» и «Инженерный класс», реализуемые в московских школах, и предложили новые форматы профориентации старшеклассников.

Мероприятие организовано Фондом содействия развитию безопасных информационных технологий (ФСРБИТ) в рамках проекта «Безопасность цифровой экономики Москвы: новое поколение», поддержанного грантом Мэра Москвы. Партнёрами выступили компании «ИнфоТеКС», «Код Безопасности», «Перспективный мониторинг», «Линфо», а также Медиа Группа «Авангард».



Торжественное награждение участников из Московского региона

¹ О выдающемся советском ученом-криптографе И.Я.Верченко читайте в BIS Journal №2/2018 и на сайте <https://journal.ib-bank.ru/post/662>.

Здесь могла быть реклама банка,

но успешная DDoS-атака
«уронила» его рейтинг



Ваш бизнес не остановить

Технологии «Лаборатории Касперского» обеспечивают защиту
и непрерывную работу вашего бизнеса.

Благодаря инструментам защиты от DDoS-атак ваши онлайн-сервисы
всегда будут доступны клиентам и репутация организации не пострадает.

www.kaspersky.ru/ddos-protection

KASPERSKY

#ИстиннаяБезопасность

© АО «Лаборатория Касперского», 2017. Зарегистрированные товарные знаки и знаки обслуживания
являются собственностью их правообладателей.



Kaspersky®
DDoS Protection

Специализированный системный интегратор в области информационной безопасности



Адрес: Москва, Дербеневская набережная, д.11,
БЦ «Полларс», корп.В, 5 этаж, оф.502
Тел./факс +7 (495) 786-34-93, +7 (495) 781-64-12
Отдел продаж sales@itprotect.ru



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

«МЫ ВЕРНУЛИСЬ ДОМОЙ В СЕВАСТОПОЛЬ РОДНОЙ...»

75 ЛЕТ НАЗАД, 9 МАЯ 1944 ГОДА, СОВЕТСКИЕ ВОЙСКА
ОСВОБОДИЛИ СЕВАСТОПОЛЬ



**ФОНД
ПРЕЗИДЕНТСКИХ
ГРАНТОВ**

Публикация подготовлена с использованием средств гранта Президента Российской Федерации на развитие гражданского общества №18-2-012576, представленного Фондом президентских грантов.



75 лет назад, 9 мая 1944 года, был освобождён Севастополь. На следующий день, 10 мая, Москва салютовала его освободителям — доблестным черноморским морякам, лётчикам и воинам 4-го Украинского фронта. Великую радость от этой победы легко понять и нынешним гражданам России, ведь Севастополь всегда был и будет символом воинской славы для нашего Отечества. Символична и сама дата освобождения Севастополя, 9 мая, ровно за год до окончательной победы над врагом в Великой Отечественной войне.

В нашей благодарной памяти слились воедино героические события победного мая 1944 г. и двух оборон Севастополя: 1854–1855 гг. и 1941–1942 гг.

Среди множества исследований и публикаций об участниках обороны Севастополя в 1941–1942 гг. и его освободителях в мае 1944 г. присутствуют и документальные свидетельства самоотверженного труда радиоразведчиков, криптографов, связистов закрытой связи.

СРАЖЕНИЕ ЗА СОХРАННОСТЬ СВЯЗИ

Для Севастополя Великая Отечественная война началась 22 июня в 2.00. Тогда в Штабе Черноморского флота приняли донесение с поста, расположенного на мысе Тарханкут (самой западной точке Крымского полуострова) о шуме моторов самолётов в направлении Севастополя. Оперативный дежурный немедленно доложил обстановку командующему флотом вице-адмиралу Ф. С. Октябрьскому и по городской радиотрансляции прозвучали сигналы боевой тревоги. Днём 22 июня Штаб ЧФ перешёл в помещение подземной АТС, а после эвакуации Штаба на Кавказ там разместился Командный пункт командующего Севастопольским оборонительным районом Ф. С. Октябрьского.

Эта АТС располагалась глубоко в скалах Южной бухты и имела автономную электростанцию. Её подземные помещения, созданные ещё в 1935 г., специально предназначались для размещения в них Штаба ЧФ на период военной опасности.

Из скальных подземелий осуществлялась координация связи всего Севастопольского оборонительного района и Черноморского флота. Весьма своевременным оказалось обнаружение и возобновление работы подземного 200-парного телефонного кабеля, проложенного ещё в 1912–1916 гг., но позднее забытого. Так, в первой половине ноября 1941 г. в результате бомбардировок и прямых попаданий снарядов были разрушены основные кабельные выходы из АТС и тогда 200-парный кабель стал использоваться на особо важных направлениях, он очень выручил связистов.

2 декабря вышел из строя подводный кабель, соединявший центр города с Се-

верной стороной. Сразу нарушилась проводная связь командования с частями, защищавшими город на северном направлении. Связисты-моряки трое суток работали на барже под обстрелом и бомбёжкой. Разрывы двух снарядов, попавших в борт баржи, сразили нескольких связистов. Лишь к концу третьих суток связь с Северной стороной была восстановлена.

Нелегко было и в городе. Один из связистов, А. И. Буйлов, в последствии вспоминал: «Обычно на дне воронок, образовавшихся от разрыва вражеских авиабомб, а они, как правило, были большими, мы устанавливали палатку и там сращивали концы повреждённых кабелей. Когда мессера пикировали, мы прижимались ко дну воронки, твёрдо убеждённые в том, что дважды в одно место не попадает» [1].

ШИФРТЕЛЕГРАММЫ О ПОЛОЖЕНИИ ЗАЩИТНИКОВ СЕВАСТОПОЛЯ

С 28 мая 1942 г. начались постоянные массированные налёты вражеской авиации на Севастополь. Об обстановке того времени можно составить представление по опубликованным шифртелеграммам Особых отделов НКВД Приморской армии и Черноморского флота. Вот выдержки из нескольких телеграмм [2].

10 июня 1942 г.: «Продвижение противника, благодаря преимуществу в авиации, на переднем крае продолжается. Воздействовать нечем, отсутствуют зенитные боеприпасы... Нашей зенитной артиллерией и истребительной авиацией 7–8 июня сбито 37 самолётов противника, из них подбито 9...»; «В 9 час. 15 мин. авиацией противника потоплен транспорт «Абхазия», прибывший в Главную базу ночью. Выгрузить с транспорта успели только 54 т. боеприпасов. В 13 час. вражеской авиацией разбомблён и потоплен эсминец «Свободный», прибывший в Главную базу вместе с «Абхазией»...»

11 июня: «Продолжаются мощные артудары, действия авиации, в Главной базе — 187 налётов, на фронте — 359 налётов. Резко снизился зенитный огонь, имеется боевой запас на 15–20 минут боя...»

13 июня: «В первой половине дня противник атаковал наши позиции на Ба-



9 мая 1944 г. в Севастополе. Фото Е. Халдея

лаклавском направлении... Все атаки отбиты с незначительным отходом наших частей. В течение дня 24 орудия 76 мм нашей зенитной артиллерии огонь не вели из-за полного отсутствия снарядов. Утром в 4 час. вражеской авиацией потоплен прибывший в Главную базу транспорт «Грузия» с боевым запасом. В 11 час. 50 мин. в районе мыса Фиолент потоплены быстроходный тральщик № 2738 и катер «МО-92». В результате этого напряжённое положение с боевым запасом. На месте приняты меры к разгрузке затонувшего боевого запаса и усилению доставки боевыми кораблями...

21 июня: «Северная сторона в основном занята противником, бухта Матюшенко, Нордовый берег Северной бухты в его руках. Заняв Учкеевку немцы расстреляли 27 женщин и детей, укрывшихся в расщелинах. Маршевое пополнение идёт слабо, за 2 дня поступило до 700 человек. Доставка боезапаса не покрывает дневного расхода. Севастополь имеет до 35 тыс. мин при ежедневном расходе 5000. Активные действия авиации противника в течение

всего времени действуют на моральное состояние войск...»

28 июня: «На восточном участке велись ожесточённые бои, все атаки отбиты. На линию фронта и базы авиация противника совершила 765 самолётовывлетов...»

ФЛОТСКАЯ СВЯЗЬ СО СРАЖАЮЩИМСЯ ОТЕЧЕСТВОМ

В период обороны Севастополя важную роль в обеспечении связи с Москвой и Куйбышевом (резервной столицей СССР в то время), военно-морскими базами на Кавказе, с кораблями и подводными лодками, да и внутри города, сыграл узел связи Черноморского флота. Узел связи, включавший в себя радиоприёмный и радиопередающий центры, телефонную станцию и телеграф, возглавлял майор А. Н. Макаренко.

Передающий радицентр имел 18 передатчиков, а приёмный был рассчитан на обеспечение около 30 направлений радиосвязи [1]. Александр Никитич Макаренко был опытным команди-

ром, более года воевал в Испании. Он был прекрасным радистом-оператором, и дежуря по связи, передавал самые большие и ответственные телеграммы. Его подчинённые иногда сутками не покидали места своей вахты. С ноября 1941 г. радио стало единственным средством связи для защитников города с центром страны и кораблями флота.

Особенно тяжело было поддерживать связь с подводными лодками. Радист знал только волну, на которой должен был работать: «Сидишь и вращаешь ручкой настройки приемника плюс-минус 2 градуса от назначенной волны. А рядом стоит офицер оперативного отдела и время от времени напоминает, что корреспондент должен уже работать. Пот прошибает, не прохлопал ли. И уже не ограничиваешься интервалом плюс-минус 2 градуса, шарь по всему диапазону... И вдруг улавливаешь слабый-слабый шорох. Это ещё не передача, нет, только слабое дыхание эфира. Стрелка замирает на зафиксированном делении шкалы... Иногда это результат напряжённой работы и томительного

ожидания в течение нескольких вахт, а то и нескольких суток» [1].

Узел связи Черноморского флота оставался в Севастополе до самых последних дней обороны. В ночь на 28 июня 1942 г. наши войска под давлением превосходящих сил противника стали отходить к берегу моря. Бои шли уже в районе Братского кладбища. На рассвете 29 июня дежурный передающего радицентра донёс в штаб, что немцы переправляются через Северную бухту. Было приказано перенести оставшиеся средства связи на 35 батарею, развернуть там радиостанцию и к 18–19 часам установить связь со всеми возможными направлениями [1].

«ЕСЛИ БЫ НЕ БЫЛО РАЗВЕДКИ ЧЕРНОМОРСКОГО ФЛОТА...»

В ночь с 29 на 30 июня 1942 г. командующий Севастопольским оборонительным районом Ф. С. Октябрьский перешёл на 35 батарею в районе Херсонесского маяка. К этому моменту Макаренко со своими связистами установил радиосвязь с Москвой и Краснодаром.

Флотский криптограф Зайцев впоследствии вспоминал: «Устроились в недостроенном туннеле для аварийного спасения, пробитом между штольнями, отгородившись от внешнего мира брезентом; брезентовая же занавесь отделяла нас от Уманского, первоклассного специалиста, не пропустившего ни одного донесения в Генштаб командующего румынским горно-стрелковым корпусом, вместе с немцами штурмовавшим город» [3].

Криптографы и радиоразведчики ЧФ действовали слаженно, очень пригодился довоенный опыт. Их основные усилия были направлены на Румынию и Турцию. Самоотверженный труд вскоре был вознаграждён первыми успехами. 25 июня криптографы вскрыли новые шифры противника, введенные с началом боевых действий. Летом 1942 г. Верховный главнокомандующий И. В. Сталин так оценивал работу дешифровально-разведывательной службы ЧФ: «Если бы не было разведки Черноморского флота, я не знал бы обстановки на Юге» [3].

«30 июня бои шли уже в районе Малахова Кургана, на Куликовом поле,

вдоль Лабораторного шоссе. Гитлеровцы были на расстоянии одного километра от бывшего Командного пункта обороны, когда он был уничтожен защитниками» [1]. В последние дни обороны телеграммы в Москву шли с 35 батареи через Сталинград. Там до последнего момента поддерживали радиосвязь с Севастополем...

Ленинградская поэтесса Ольга Берггольц написала в 1942 г.:

*«Но мы не хотим и не будем прощаться
С тобой не смилившийся город-солдат:
Ты жив, ты в сердцах москвичей,*

сталинградцев,

Дыханье твоё бережёт Ленинград.

*Мы знаем, на всех пламенеющих тропах,
Со всеми, кто бьёт ненавистных врагов,
Идёт Севастополь, родной Севастополь,
И кровь и огонь от его берегов...»*

ПРИКАЗ ОБОРОНЯЮЩЕМУСЯ ПРОТИВНИКУ

Враги тоже прекрасно понимали, что значит Севастополь для России. Очень показателен приказ командующего 17 немецкой армией, оборонявшей Севастополь весной 1944 года. В своём приказе войскам от 3 мая он указал: «Я получил приказ защищать каждую пядь Севастопольского плацдарма. Его значение вы понимаете. Ни одно имя в России не произносится с большим благоговением, чем Севастополь... Я требую, чтобы все оборонялись в полном смысле этого слова, чтобы никто не отходил, удерживал бы каждую траншею, каждую воронку, каждый окоп. В случае прорыва танков противника пехота должна оставаться на своих позициях и уничтожать танки как на переднем крае, так и в глубине обороны мощным противотанковым оружием.

Если сильный огонь противника разрушит наши оборонительные сооружения, необходимо оставаться на месте и защищать остатки этих сооружений, воронки... Плацдарм на всю глубину сильно оборудован в инженерном отношении. Но никому из нас не должна даже и в голову прийти мысль об отходе на эти позиции, расположенные в глубине... Честь армии зависит от каждого метра полученной территории...» [4].

Этот приказ, как и многие другие документы германского командования, был перехвачен радиоразведкой 4-го

Украинского фронта, освободившего Севастополь от врага.

ДОСТИЖЕНИЯ ФЛОТСКИХ ДЕШИФРОВАЛЬЩИКОВ И РАЗВЕДЧИКОВ

Как изменились возможности радиоразведчиков за время, прошедшее с лета 1942 г.! Преодолевая все сложности, неуклонно росли их техническая оснащённость и боевые навыки. Особо стоит отметить дешифровально-разведывательную службу Черноморского флота. Даже базируясь только на Кавказе, она «постоянно добывала достоверную разведывательную информацию самого разнообразного содержания, в том числе и стратегического значения» [3].

Наиболее ценным источником сведений для неё явилась шифрпереписка румынского Генерального штаба со своей миссией связи при командующем группировкой германских вооружённых сил на юге СССР фельдмаршале Манштейне. Отметим, что чтение румынской шифрпереписки началось ещё раньше, даже до того момента, как Манштейн возглавил осаду Севастополя в 1941 г. [3].

Вот «примеры полученной информации:

- ◆ боевые приказы о штурме Одессы, Севастополя, Новороссийска;
- ◆ планировавшееся направление главного удара в районе Курска в летней кампании 1943 г.;
- ◆ подготовка покушения на глав правительств союзных держав во время предстоящей Тегеранской конференции;
- ◆ условия, при которых Турция вступит в войну с Советским Союзом;
- ◆ план увода (или уничтожения) румынского флота, разработанный немцами в связи с наступлением советских войск» [6].

НОВЫЕ ВОЗМОЖНОСТИ РАДИОРАЗВЕДКИ

Весной 1944 г. освободителей Севастополя поддерживали 361, 370 и 875 отдельные радиодивизионы Особого Назначения. Это были мощные подразделения, хорошо оснащённые новейшей техникой радиоперехвата сообщений противника. Не менее важно и то, что в этих радиодивизионах слу-

жили специалисты с богатым боевым опытом. Сведения из своевременно дешифрованных ими передач противника очень помогали нашим наступающим войскам.

Приведём пример дешифрованной переписки неприятеля, отступавшего в Крым с Кавказа в 1943 г. Это переписка подразделений 17-й немецкой армии от 9 октября 1943 г.:

«К положению на Таманском полуострове. Отвод остатков войск из предмостного укрепления будет осуществляться под видом отхода на новые рубежи с целью обмануть противника, однако эти позиции занимать не будут. Для того, чтобы заставить противника терять время на атаку ложных рубежей, отходящие части совершат марш с линии обороны непосредственно к переправочным рубежам. Как линия обороны, так и ложный промежуточный рубеж защищены проволочным заграждением, концы которого заминированы с таким расчётом, что

каждое прикосновение к проволоке вызывает взрыв мины. Перед последним оборонительным рубежом и на всей его глубине будут установлены новые шестиствольные деревянные минные аппараты, которые в момент стрельбы самовзрываются. Прекращение боевых действий будет осуществлено по всему фронту одновременно; войска будут направлены к местам переправы, где будут подготовлены все переправочные средства, которыми располагает понтонный полк полковника Генке, с таким расчётом, чтобы все войска были переправлены одним рейсом. Для противодействия авиации противника ожидается прибытие 100 истребителей и 50 бомбардировщиков. В с. Коломка, что в 6 км северо-восточнее г. Керчи, установлена тяжёлая артиллерия, которая будет прикрывать отход аррьергардов» [6].

Обратим внимание на упоминание «предмостного укрепления», здесь речь идёт о начатом немцами строитель-

стве железнодорожного моста через Керченский пролив. Отступление их войск с Кавказа прервало строительные работы. Надо сказать, что неприятелю удалось без существенных потерь переправиться в Крым через Керченский пролив, что было весьма непросто. 17 немецкая армия, которой предстояло оборонять Севастополь, была сильным и опытным противником для наших войск. До Крыма она в 1942–1943 годах с боями прошла Донбасс, Дон и Северный Кавказ.

КОГДА КАЖДЫЙ ВОИН ЗНАЕТ СВОЁ ДЕЛО

Стойко оборонявшемуся в Севастопольских укреплениях врагу наша армия противопоставила своё уже сложившееся превосходство в авиации и артиллерии. Только перед решающим штурмом, с 29 апреля по 5 мая, фронтовая, флотская и приданная Ставкой авиация дальнего действия совершила 8200 самолёто-вылетов на позиции противника. Эти позиции были детально выяснены радиоразведкой, которая контролировала весь радиозфир уже на дальних подступах к месту боёв.

Вот пример боевой работы 370 отдельного радиодивизиона ОсНаз накануне решающего штурма. 2 мая радист принёс в оперативное отделение только что перехваченную радиограмму военно-транспортного самолёта Ю-52, адресованную радиостанции немецкого аэродрома на мысе Херсонес. Старший лейтенант К. Бондаренко сумел быстро прочитать кодированное сообщение: «5 мая в 4 часа из Констанцы (в Румынии — авт.) на вашу посадочную площадку придут 30 бомбардировщиков ХЕ-11».

Из дивизиона немедленно пошли шифрованные сообщения в штабы 8-й воздушной армии и Особой приморской армии, усилилось наблюдение за Херсонесом. Рано утром 5 мая, перед началом штурма Севастополя, на аэродром Херсонеса зашли на посадку вражеские бомбардировщики. И сразу после их посадки с юго-востока от мыса показались наши штурмовики. Смертоносные бомбардировщики противника скоро превратились в груды горящего металла [5].



Освобождение Севастополя в 1944 г.



В 1944 г. в Севастополь вернулись дети

ГОСУДАРСТВЕННОЕ ПРИЗНАНИЕ ЗАСЛУГ РАДИОРАЗВЕДЧИКОВ

В ознаменование заслуг при освобождении Севастополя от сильного и упорного врага Приказом Верховного Главнокомандующего от 24 мая 1944 года 361 радиодивизион стал именоваться 361 отдельным Севастопольским радиодивизионом ОсНаз. Тем же приказом получил наименование Севастопольского 5 отдельный полк правительственной

связи НКВД. Наградами были отмечены и заслуги 370 и 875 отдельных радиодивизионов ОсНаз Особой приморской армии. Всем им предстоял ещё долгий путь по фронтам до самой Победы, а 875 радиодивизион обезвреживал врага и в войне с Японией.

Освобождённый Севастополь уже в мае 1944 начал постепенно возвращаться к жизни. Почти лишившийся в период оккупации гражданского населения, он принял как родных и вернув-

шихся, и новых своих жителей, взрослых и совсем юных. Для детских игр стали притягательным местом даже городские развалины.

Сплочённый и терпеливый труд взрослых и юных рук, незатейливые детские радости оживляли, день ото дня возрождали и, наконец, возродили из руин родной город, родной Севастополь!

ЛИТЕРАТУРА

1. Пересыпкин И. Т. Связь в Великой Отечественной войне. М., 1973.
2. Органы государственной безопасности СССР в Великой Отечественной войне 1941–1945. Сб. документов. М., 1995.
3. Куличенко В. Русские против «Энигмы» // Независимое военное обозрение. — 2004. — № 40.
4. ЦАМО, ф. 244, д. 6.
5. Шмырёв П. Часовые эфира (об истории радиоразведки) // Красная Звезда. — 2004. — 18 марта.
6. Бутырский Л. С., Ларин Д. А., Шанкин Г. П. Криптографический фронт Великой Отечественной. М., 2017.



Танк Т-34 «Родина» в Сталинграде

НА ВОЛГЕ ШИРОКОЙ

СТАЛИНГРАД. КОРЕННОЙ ПЕРЕЛОМ В ВОЙНЕ¹

Слово «Сталинград» хорошо знакомо всем нам ещё со школы, да и за пределами России оно широко известно. Именно в Сталинграде и на прилегающей к нему территории свершился решительный перелом не только в Великой Отечественной, но и во всей Второй мировой войне. Имея в виду мировую войну, следует сказать, что Сталинградская битва стала наиболее ярким и важным событием в переломный момент военного противостояния двух коалиций. И этот перелом был достигнут в значительной степени за счёт успехов информационного обеспечения сил антигитлеровской коалиции.¹

¹ Публикация подготовлена с использованием средств гранта Президента Российской Федерации на развитие гражданского общества №18-2-012576, представленного Фондом президентских грантов.

СОБЫТИЯ НА КРИПТОГРАФИЧЕСКОМ ФРОНТЕ

Основные события Сталинградской битвы происходили, как известно, с середины июля 1942 г. по начало февраля 1943 года. Первая половина 1942 г. внешне была в основном успешной для Германии и её союзников: Красная Армия с боями отступала; британские войска на севере Африки были оттеснены дивизиями Э. Роммеля уже в окрестности египетской Александрии; мощный флот Японии, дальновидно оснащённый авианосцами, господствовал в Тихом и Индийском океанах. Немецкий генерал К. Типпельскирх, бывший начальник главного разведывательного управления генштаба германских сухопутных сил, написал об этом времени: «В конце августа в ставке Гитлера можно было слышать о том, что победа над Советским Союзом для него стала

второстепенным делом... и что сейчас его больше всего интересуют широкие планы захвата Среднего Востока» (1).

Это теперь мы знаем, что британские криптографы тогда же сумели одолеть несколько модификаций немецкой шифрмашин «Энигма» и начали чтение шифрованных радиogramм Германии, прежде всего, её подводного флота и авиации. Насколько это было важно для Германии и для Великобритании и США, имеющих внешние экономические связи исключительно по морю, видно из следующих данных. Потери немецких подводных лодок составили в 1941, 1942 и 1943 годах, соответственно, 35, 85, 237 субмарин (2).

Приведённые данные весьма показательны, но осенью 1942 года они были ещё никому не известны, а сам успех британских криптографов являлся величайшей тайной. Летом 1942 г. и американцы в сотрудничестве с ан-

гличанами сумели наладить чтение зашифрованных японских радиogramм, в результате чего нанесли своему противнику два чувствительных удара. Сначала «американцы перехватили японское радиосообщение и, расшифровав его, узнали о планах своих противников в Коралловом море, близ берегов Австралии» (1). В результате десантный конвой японцев с солидным боевым охранением неожиданно нарвался на засаду американского флота и понёс большие потери. Чуть позже, японский флот серьёзно пострадал у острова Мидуэй при попытке нападения на базу подводных лодок США. «Американцы, благодаря перехваченным и расшифрованным радиосообщениям имели достоверные сведения о японских планах и заранее стянули в угрожаемый район три авианосца под защитой крейсеров» (1). В итоге этих морских боёв японцы потеряли все шесть своих авианосцев: четыре были уничтожены, а два сильно повреждены. Правда, стратегические планы Японии после таких потерь остались неизменными.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — ЗАБОТА ОБЩАЯ

Вот на таком внешнем фоне в середине июля 1942 г. началась Сталинградская битва, точнее, её первая часть — оборонительное сражение.

Завязалось сражение на подступах к городу, а затем, с 23 августа, произошло и в самом Сталинграде. Спустя четыре месяца, 19 ноября, советские войска перешли в контрнаступление, 23 ноября сомкнули кольцо окружения противника и завершили его разгром 2 февраля 1943 г.

В период подготовки контрнаступления по указанию Верховного Главнокомандования был проведён критический пересмотр опыта информационного взаимодействия в предыдущих военных операциях советских войск. Вопросы обеспечения информационной безопасности при планировании предстоящей операции, развёртывании сил и при организации управления войсками в боевой обстановке вышли на первый план. Ведь требовалось обеспечить скрытность развёртывания группировки численностью, гораздо превышав-

В период подготовки контрнаступления был проведён критический пересмотр опыта информационного взаимодействия в предыдущих военных операциях советских войск

шей миллион человек, со многими тысячами танков и автомобилей вблизи линии фронта длиной 400 км. Прежде всего были приняты меры по пресечению возможности утечки секретной информации по каналам связи.

Так, директива командующему Сталинградским фронтом гласила: «Ставка Верховного Главнокомандования категорически запрещает вам впредь пересылать шифром какие бы то ни было соображения по плану операции, издавать и рассылать приказы по предстоящим действиям. Все планы операции по требованию Ставки направлять лишь только написанными от руки и с ответственным исполнителем. Приказы на предстоящую операцию командующим армиями давать только лично по карте» (3).

Сокращению переписки и сохранению секретности действий командования способствовало также «пребывание на фронтах представителей Ставки Г. К. Жукова и А. М. Василевского. Они решали на местах без переписки не только вопросы организации взаимодействия между фронтами, но и другие принципиальные вопросы планирования и подготовки операции» (3).

Вот воспоминания участников контрнаступления: «С планом операции был ознакомлен лишь узкий круг офицеров и генералов, и только в необходимом объёме. Остальному командному составу конкретные задачи ставились лишь за сутки или двое до начала наступления... Переписка, телефонные и телеграфные переговоры о готовившемся наступлении запрещались». «Сосредоточение и перегруппировка войск проводились только ночью. Ставка незамедлительно и резко реагировала на любое нарушение скрытности подготовки контрнаступления» (3). Вся подготовка к наступлению велась под видом усиления оборонительных по-

зиций. Противнику навязывали идею о том, что советские войска не собираются наступать. С этой целью Ставка направила соединениям Сталинградского и соседних фронтов директивы о прекращении любых наступательных действий и переходе к жёсткой обороне. Эти директивы «были переданы Генеральным штабом по прямому проводу. Они не шифровались, поэтому вскоре стали известны немецкой разведке» (3).

В середине ноября было отмечено усиление воздушной разведки противника как на фронте, так и в нашем тылу. Одной из причин этой повышенной активности стали опасения германского командования относительно возможного наступления советских армий. Такие опасения были связаны и с начавшейся 8 ноября высадкой англо-американских войск в северной Африке, в Марокко и Алжире.

Типпельскирх, описавший историю Второй мировой войны с немецкой точки зрения, по его собственному признанию, отметил в 1951 г.: «Русские хотели быть полностью уверенными в том, что крупные силы немцев скованы войсками западных держав... Поэтому они медлили с наступлением, ожидая пока определится успех десантной операции в Северной Африке. Когда это произошло, русские войска перешли в наступление» (1).

А тогда, в середине ноября 1942 г., с немецких самолётов-разведчиков шёл на землю доклад обо всём, что было обнаружено в расположении советских войск: расположение частей, их передвижение, проведение инженерных работ. На земле наши «слухачи»-переводчики внимательно следили за этими докладами и советское командование узнавало, что известно противнику о войсках фронтов, так по докладам немецких лётчиков проверялось качество маскировки наших сил. Непосредственно перед контрнаступлением

ОПО Штаба 18
Вход № 094
5 101 1942
Подпись

СЕКРЕТНО
Экз. №....

ДАННЫЕ АВИАРАЗВЕДКИ ПРОТИВНИКА
(радиоперехват) 2.10.42 карта 100.000

1. Свой передний край проходит восточнее Раз.564.
В балке ГРАЧЕВАЯ стоят танки и большое количество арт-позиций.
2. В балка 3 км с.в. КУЗЬМИЧИ стоят, предположительно, свои танки.
3. Из ГРАЧИ на балка ГРАЧЕВАЯ - 13 танков, из них 5 танков достигли балка ГРАЧЕВАЯ.
4. В балке сев. перекрестка дорог, балка ГРАЧЕВАЯ скопление 250 автомашин.
5. 2 км вост. выс. 102,3 стоят 8 русских танков фронтом на юг.
6. 1 км вост. выс. 111,2 две батареи на ОП; 2 км с.в. выс. 139,5 одна батарея на ОП; 3 км с.з. выс. 139,5 две батареи на ОП
7. Свои бомбардировщики атакуют СПАРТАКОВКА, БАРРИКАДЫ.
8. Свои части на выс. 144,2 и 2 км с.в.
9. В ОРЛОВКА русских частей нет.
10. Свои части в двух км с.з. СПОРТАКОВКА.
(5 км с.в. КАЗЬМИЧИ)
11. 1,5 км зап. отм. 82,3 стоят русские танки, до 30 русских танков стоит в 5 км с.в. КУЗЬМИЧИ.
12. 1 км южн. ГРАЧИ 6 батарей на ОП.
13. 3 русских танка атакуют выс. 130,4, после обстрела повернули на север.
14. 1,5 км вост. выс. 102,3 30 русских танков ведут бой с нашими, два танка горят.

НАЧ. ИНФОРМОТДЕЛЕНИЯ РО ШТАБА
ДОНСКОГО ФРОНТА
ПОЛКОВНИК
ЛАВРЕНЧУК

Данные авиаразведки противника (радиоперехват) за 02.10.1942 г. Архив: ЦАМО, Фонд: 206, Опись: 262, Дело: 61.

ем была проведена перегруппировка войск, не обнаруженная авиаразведкой противника (4).

Даже командиры легендарной 62-й армии Василия Ивановича Чуйкова, дивизии которой поредело до нескольких сотен бойцов, но остановили гитлеровцев в уличных боях на развалинах Сталинграда, не знали о готовившемся контрнаступлении.

По воспоминаниям В.И. Чуйкова: «После 12 ноября Паулюс не прекратил

активных наступательных действий, затишья на фронте не было... В первую очередь перед нами встала задача оказать помощь дивизии Людникова, оторванной от главных сил армии. Её положение стало очень тяжёлым: она была зажата противником с севера, с запада и с юга, а с востока отрезана Волгой, по которой шёл сплошной лёд... Своими контратаками мы не дали противнику уничтожить дивизию Людникова. Не могу не сказать

о мужестве командования окружённой дивизии во главе с полковником Иваном Ильичом Людниковым. Несмотря на исключительно тяжёлое положение, там соблюдали спокойствие и уверенность. Телефонная связь, разумеется, была порвана. Работала только радиосвязь. Я лично несколько раз открытым текстом говорил по радио с Людниковым. Мы узнавали друг друга по голосу, не называя себя по имени и фамилии. Я не стеснялся открыто говорить ему, что помощь будет оказана, что скоро соединимся с ним. Я надеялся, что он понимает, почему разговор с ним ведётся открыто, и что скоро никакой помощи мы дать ему не можем. Он мне тоже говорил о надежде на скорое соединение. Мы старались таким образом ввести в заблуждение противника. Лишь в ночь на 16 ноября наши «ночные самолёты» на парашютах сбросили Людникову четыре тюка продовольствия и четыре тюка боеприпасов. А в ночь на 20 ноября четыре бронекатера наконец пробились в протоку Денежная Воложка, затем к берегу, где оборонялась дивизия. Катера доставили боеприпасы, медикаменты и вывезли 150 раненых. Вечером 18 ноября у меня в блиндаже обсуждали наши возможности для дальнейших активных действий, силы наши были на исходе. В этот час позвонили из штаба фронта и предупредили о скором получении приказа. Мы все переглянулись. «О чем может быть этот приказ? — подумал каждый из нас» (5).

РАДИОСВЯЗЬ ВСТРЕЧНОГО ВЗАИМОДЕЙСТВИЯ

При планировании контрнаступления пришлось предусмотреть много нового в организации связи и боевого управления войсками. И.Т. Пересыпкин, нарком связи и одновременно заместитель наркома обороны СССР в годы войны, вспоминал спустя 30 лет после Сталинградской битвы: «В начале ноября 1942 г. Ставка Верховного Главнокомандования командировала меня в район Сталинграда... В предстоящей операции «Уран», имевшей целью окружение группировки фашистских войск, в районе Калача должны были соединиться войска Юго-Западного и Сталин-

градского фронтов, которые должны были встретиться на поле боя, действуя навстречу друг другу. Мы отлично понимали, что в случае отказа связи в момент встречи могла возникнуть опасность их взаимного поражения. В штабы участвовавших в этой операции фронтов были высланы все отправные данные, необходимые для организации радиосвязи встречного взаимодействия, как мы её тогда называли. Основной особенностью этого, ещё не встречавшегося в нашей практике способа организации радиосвязи, явились выделение так называемой «волны встречи» и разработка системы позывных, позволившей быстро определять принадлежность радиостанции и устанавливать связь между передовыми частями и соединениями армий, завершавшими окружение противника.

Сущность организации такой радиосвязи заключалась в следующем: все соединения, действовавшие в операции навстречу друг другу, имели свои радиостанции или радиоприёмники, настроенные на одну волну — «волну встречи». Каждая армия получала один позывной, а соединения, входившие в её состав, имели тот же позывной, что и штаб армии, но к нему добавлялся цифровой индекс, предназначенный только для данного соединения.

Установление связи по этой радиосети осуществлялось путём вызова действовавшего навстречу соединения на «волне встречи» с указанием присвоенного позывного. Для взаимного опознавания вызываемая радиостанция другого соединения сообщала свой позывной. После взаимного опознавания и установления радиосвязи радиообмен, как правило, производился на дополнительно назначенных для этой цели рабочих радиоволнах.

Для переговоров по радиосети встречного взаимодействия Главное управление связи разработало и разослало в войска подробную инструкцию и специальную таблицу радиосигналов... Именно этот новый способ организации радиосвязи сыграл очень важную роль и способствовал достижению успеха в Сталинградской наступательной операции. Обеспечивать связь встречного взаимодействия, да ещё в таком огромном масштабе, нам ранее не при-

Из.....

П Е М Е Н Т НАЧАЛЬНИКУ 2 ОТДЕЛА УЗР

ВЕСЬМА СРОЧНО

ОП. Штаб 9 ф.

Вход. № 05947

31 XII 1942

Данные радиоразведки за 1.12.42

И т о г о в а я /

Карта 200.000.

1. Штаб Командования ФТА - СТАРОБЕЛЬСКИ.

Штаб 4 танковой Армии - РЕМОНТНАЯ

Штаб 6 Армии - ГИМРАК

Штаб 6 армии - МОРОЗОВСКИ

Штаб 3 армии румын - МОРОЗОВСКИ

2 эшелон 3 армии румын - ТАЛИНСКАЯ

Штаб 14 тк - Ферма /20 км. ю-в. Песковатка/

Штаб 24 тк - КУТОВИЧКОВ

Штаб 48 тк - ДОГЗМАНКИН /80 км. вост. Ремонтная/

Штаб 8 ак - свх. № 1 /14 км. ю-в. Вертячий/

Штаб 17 ак - ПАРАМОНОВ /8 км. ю-з. Чернышевская/

Штаб 29 ак - СЕТРАКОВСКИ

Штаб 51 ак - СТАЛИНГРАДСКИ

Штаб 51 ак - КУЛЬТСТАН

Штаб неустановленного ак - И. АСТАХОВ

Штаб неустановленного ак - ПОНОМАРЕВ

Штаб неустановленного ак - ДУВИНСКИ

Штаб 14 тк - НОВО-АЛЕКСАНДРОВСКИ /30.11 - Дмитриевка/

Штаб 16 тк - ГОРОДНИЦЕ

Штаб 24 тк - АЛЕКСАНДРОВКА

Штаб 3 мд - ДМИТРИЕВКА

Штаб 29 мд - Район МИРНОКЛЕБЕНА

Штаб 60 мд - ДЕРЕВЯННЫЙ ВАЛ

Штаб 76 пд - свх. № 1

Штаб 79 пд - ГОРОВОЙЕ

Штаб 113 пд - восточн. ПЕСКОВАТКА /данные за 28.11/

Штаб 385 пд - В. РОССОШКА

Штабы неустановленных пд - свх. № 1, Подсобное хозяйство

2. В В С. В связи с аэродромами отмечено 81 самолет. Из них: бомбардировщиков - 9, бомб. разведчиков - 3, транспортных - 61, неустановленного типа - 8.

ЗАПЕЧАТ

РАЗГЛАШЕВ.

Отпеч. 5 экз.

31.

Сводные данные радиоразведки за 01.12.1942 г. Архив: ЦАМО, Фонд: 206, Опись: 262, Дело: 61.

ходило. Опыт организации радиосвязи встречного взаимодействия, полученный под Сталинградом, был широко использован и в последующих операциях. В частности, с большим успехом он был применён на Донском фронте в операции «Кольцо» по разгрому окружённой сталинградской группировки немецких войск» (5).

Добавим, что изложенные здесь глубокие идеи специалистов по безопасности связи нашли своё применение

и в криптографии более позднего времени. В период подготовки к Сталинградской наступательной операции большое внимание было уделено и проводной связи. Войска связи обеспечили устойчивую телеграфную и высокочастотную (ВЧ) телефонную связь штабов всех трёх фронтов со штабами их армий. «Если на каком-то направлении бои принимали затяжной характер, проводная связь широко применялась уже во всех звеньях управления» (5).

СЕКРЕТНО.

Экз. №

16

РАСПИСАНИЕ

действия ключей к таблице „ДУБ“ на декабрь м-ц

№ п.п.	Срок действия	Горизонтальные Вертикальные к л ю ч и															
		Г	1	6	4	8	0	3	7	2	9	5					
1	1—3.12.42 г.	Г	1	6	4	8	0	3	7	2	9	5					
		В	77	55	10	18	35	90	47	25	41	85	73	70	51	00	96
2	4—6.12.42 г.	Г	5	3	6	7	2	4	1	9	0	8					
		В	19	28	32	63	58	79	88	94	38	83	03	16	30	81	60
3	7—9.12.42 г.	Г	7	9	1	0	4	8	3	6	5	2					
		В	61	13	24	78	86	93	50	44	39	33	05	11	53	67	62
4	10—12.12.42 г.	Г	8	2	7	6	5	0	9	3	1	4					
		В	22	29	92	45	36	17	09	54	65	71	99	80	26	15	01
5	13—15.12.42 г.	Г	0	8	5	1	7	9	6	4	2	3					
		В	66	14	21	31	40	49	98	89	82	75	69	57	06	34	43
6	16—18.12.42 г.	Г	2	4	9	3	1	5	0	7	8	6					
		В	97	76	56	02	84	42	95	74	12	23	37	46	87	72	64
7	19—21.12.42 г.	Г	4	7	0	9	8	6	2	5	3	1					
		В	59	08	52	04	68	91	48	07	20	27	72	25	60	99	41
8	22—24.12.42 г.	Г	3	1	8	2	6	9	5	0	4	7					
		В	33	78	31	20	66	12	57	70	85	91	96	36	62	13	04
9	25—27.12.42 г.	Г	6	0	2	5	3	1	4	8	7	9					
		В	10	26	79	38	90	45	50	73	54	15	23	29	87	98	42
10	28—31.12.42 г.	Г	9	5	3	2	4	7	8	1	6	0					
		В	95	40	34	76	69	63	16	08	55	01	52	27	21	43	49

ПРИМЕЧАНИЕ: Смена ключей 24.00

Начальник 8 отдела штаба Сталинградского фронта
полковник КИРЧЕНКО.

Старший помощник начальника 8 отдела штаба Сталинградского фронта
майор КОНИН.

Расписание действия ключей к таблице «дуб» на декабрь. Архив: ЦАМО, Фонд: 303, Опись: 4005, Дело: 8.

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОПЕРАЦИИ «КОЛЬЦО»

В операции «Кольцо» Донского фронта по уничтожению группировки фашистских войск в районе Сталинграда связь тоже имела свою специфику. В ходе этой операции «проводная связь штаба Донского фронта была организована по замкнутому кольцу. Основой сети проводной связи являлись постоянные линии связи, построенные частями связи в декабре 1942 г. По мере

сокращения фронта окружения линии непрерывно наращивались, и к решающему периоду операции создавалась сеть проводной связи, состоявшая из многих линий, на концах которых было создано несколько вспомогательных узлов связи. Только за время с 1 по 15 января телеграфная станция фронта произвела обмен телеграммами в количестве 41 312» (5).

Под Сталинградом связисты получили первый опыт организации связи для представителя Ставки Верховно-

го Главнокомандования. И. Т. Пересыпкин отметил: «Представителем Ставки в то время был генерал А. М. Василевский. Я входил в состав его группы. После завершения окружения сталинградской группировки противника группа А. М. Василевского переехала в штаб Донского фронта в Запорово. Туда же прибыл из Москвы подвижный узел связи представителя Ставки. В его составе имелись 8 телеграфных аппаратов Бодо и другая телеграфная аппаратура, несколько телефонных коммутаторов для внутренней связи, две автомобильные радиостанции РАТ, другие радиостанции и радиоприёмники. Вся основная аппаратура узла связи была смонтирована в кузовах автомобилей. Узел связи обеспечивал обмен телеграммами с Москвой, соседними фронтами, иногда непосредственно с армиями. Пошёл поток телеграмм и в обратном направлении. Кроме телеграфного обмена по проводам и по радиогенералам, входившие в состав группы, имели возможность систематически вести прямые переговоры по Бодо с Генеральным штабом, с Юго-Западным и Сталинградским фронтами, нередко и с армиями. Кроме радио и проводной связи группа генерала А. М. Василевского широко использовала и авиацию связи. Между Москвой и Запорово регулярно курсировали самолёты, доставлявшие генералов и офицеров Генерального штаба и центральных управлений Наркомата обороны, фельдъегерей с различными документами» (5).

ДОЛГОЖДАННЫЙ ПЕРЕЛОМ В ВОЙНЕ

Усилия по защите информации в каналах связи и обеспечению безопасного управления войсками внесли весомый вклад в достижение общей победы над врагом в переломном сражении войны. Общие потери немцев и их союзников в Сталинградской битве составили около 1,5 млн человек, из них погибших — около 500 тысяч. Потери в танках и автомобилях равнялись полугодовому их производству в Германии и оккупированных странах, артиллерии — трёхмесячному.

Типпельскирх констатировал: «Результат наступления оказался потрясающим: одна немецкая и три союзные

армии были уничтожены, три другие немецкие армии понесли тяжёлые потери. По меньшей мере пятидесяти немецких и союзных дивизий больше не существовало. Остальные потери составляли в общей сложности ещё двадцать пять дивизий... Надежда на общую победу рухнула. Моральный дух русских высоко поднялся» (1).

Геббельс в конце января 1943 г. заявил: «Германия сможет выдержать атаки русских лишь в том случае, если ей удастся мобилизовать свои последние людские резервы». Из донесения службы безопасности СС от 17 февраля 1943 г.: «трагическое положение 6-й армии до глубины души потрясло весь народ»; «в обществе господствует убеждение, что Сталинград стал переломным моментом в войне»; «широкие круги населения пребывают в глубоком пессимизме»; «теперь спрашивают: сколько мы сумеем продержаться, чтобы исход войны оказался более-менее благоприятным для нас?» (7).

Р. Гелен, создатель и руководитель разведки ФРГ, а в период Сталинградской битвы глава оперативной армейской разведки Германии на восточном фронте, 10 февраля 1943 г. сформулировал для начальника генштаба некоторые выводы, которые уже в послевоенное время привёл в своей книге: «Русское военное командование, в частности маршал Жуков, пользуется полной свободой действий в рамках выполнения поставленных перед ним задач; принципы ведения боевых действий русские строят теперь на основе немецких методов и оперативных взглядов. Мы же, напротив, в значительной степени переняли русские методы жёсткого регули-



Всё закончилось, дали прикурить

рования сверху всех вопросов, вплоть до мелочей, чем отчасти объясняются наши поражения. Командный состав ныне избегает принятий самостоятельных решений и действий из опасения предстать перед военно-полевым судом. В результате теряется одна из важнейших предпосылок успешного ведения маневренных боевых действий» (6).

Вот такой перелом заметил германский разведчик. Добавим здесь, что 9 октября 1942 г. в Красной Армии было введено единоначалие и не стало комиссаров, с 6 января 1943 г. началось переобмундирование военнослужащих в новую форму, на которую вернулись погоны.

Д. Слейтон, будущий американский астронавт, а в 1943 г. пилот бомбардировщика, вспоминал о тех чувствах, которые он испытал после известия о по-

беде русских под Сталинградом: «Когда гитлеровцы капитулировали, ликование нашему не было предела. Все понимали, что это поворот в войне, это начало конца фашизма».

Раскаты Сталинградской бури эхом отозвались на африканском континенте. 12 мая 1943 г. в Тунисе сдались нашим союзникам последние окружённые части итало-германских войск. У. Черчилль не переоценивал значение победы в Африке и, выступая в британском парламенте 21 сентября 1943 г., заявил: «Я называю фронт, который мы открыли сначала в Африке, затем в Сицилии, а теперь в Италии, третьим фронтом. Второй фронт... ещё не открыт» (1).

Бои в Африке прекратились, этим подтвердив окончательность перелома в войне, свершившегося под Сталинградом.

ЛИТЕРАТУРА

1. Типпельскирх К. История Второй мировой войны. М., 1956.
2. Бутырский Л. С., Ларин Д. А., Шанкин Г. П. Криптографический фронт Великой Отечественной. М., 2017.
3. Барятинский М. Битва за Сталинград. М., 2007.
4. Болтунов М. Е. «Золотое ухо» военной разведки. М., 2011.
5. Связь в Сталинграде в годы Великой Отечественной. СПб.: Центральный музей связи имени А. С. Попова, 2012.
6. Гелен Р. Война разведок. М., 2003.
7. Вторая мировая война. Дискуссии. Основные тенденции. Результаты исследований. Пер. с нем. М., 1997.

УШЁЛ ЛИ ПОЕЗД?

ПРО АППАРАТНЫЕ ПЛАТФОРМЫ ДЛЯ «ДОВЕРЕННЫХ ВЫЧИСЛЕНИЙ»

Регуляторы планомерно по-нуждают общество и бизнес задумываться о защите от угроз, возникающих вследствие несовершенства программного обеспечения ИТ-инфраструктур. При этом педалируется мысль, что «мы опоздали вскочить на поезд» в том, что касается разработки «железа» для ИТ.

ЭФФЕКТ MELTDOWN&SPECTRE

В начале 2018 года было официально признано наличие уязвимостей в ряде «штатных» процессоров, используемых в ИТ-системах по всему миру. Оказалось, что «дыра» Meltdown в микросхемах от Intel и уязвимость Spectre в микросхемах от Intel и AMD (по некоторым данным и в процессорах с архитектурой ARM) позволяют вредоносу из заражённого приложения получить разрешение на использование «защищённого режима» и считывать данные из закрытых областей вычислительной платформы.

В конце 2018 года израильская компания CTS Labs выпустила отчёт об обнаружении более десятка уязвимостей в процессорах AMD. И хотя это заявление было воспринято рынком с недоверием, информации о Meltdown и Spectre оказалось достаточно, чтобы привлечь внимание к проблемам ИБ на аппаратном уровне.

В США после выявления «эффекта Meltdown&Spectre» резко повысился градус дискуссий о необходимости переосмыслить подходы к построению аппаратной компоненты. Эксперты утверждают, что источники поступления микросхем для критической инфраструктуры США скомпрометированы, и правительству необходимо позаботиться о запуске нового витка развития микроэлектроники. Обновлением должны быть охвачены как системы критически важной инфраструктуры

(оборонной, промышленной, финансовой), так и оборудование потребительского уровня.

Одновременно ставится вопрос о тотальной ревизии всех аппаратных ИТ-платформ в контексте выявления угроз, похожих на Meltdown и Spectre. Причин две — обеспечение национальной безопасности и обеспечение устойчивости прогресса в сфере безопасности в целом.

«Пришло время ответственно заняться обеспечением безопасности аппаратной компоненты критической инфраструктуры и, в частности, разработать национальную стратегию закупок безопасного «железа» для нужд нашей военной и критически важной инфраструктуры», — это одна из цитат в докладе аналитиков, представляющих руководство Центра по изучению проблем критической инфраструктуры, технологий и логистики (Vital Infrastructure, Technology and Logistics (VITAL) Center) и Института политических исследований «Потомак» (Potomac Institute for Policy Studies).

Любопытно, как авторы доклада подчеркнули важность государственной поддержки. По их мнению, промышленность США сегодня не может самостоятельно решить эти сложные проблемы безопасности. Хотя уместно заметить, что по некоторым данным, в оборонном ведомстве США на обеспечение ИБ на уровне микросхем уходит около 10% всего бюджета, выделяемого на приобретение изделий микроэлектроники или до полумиллиарда долларов.

Несмотря на непрерывный полувек прогресс в области микроэлектроники, Агентство по перспективным НИОКР Министерства обороны США (DARPA) сочло необходимым инициировать ещё и «Проект по возрождению электроники» (Electronics Resurgence Initiative). Это означает, что

общее число перспективных программ по микроэлектронике (новые материалы, новые средства проектирования микросхем, новые системные архитектуры...) в ближайшие годы дополнится дюжиной новых проектов. В том числе и в рамках т.н. аппаратной киберинициативы.

АППАРАТНЫЕ СРЕДСТВА ИБ

В теории и практике ИБ существуют такие понятия, как trusted computing (доверенные вычисления) и trustworthy computing (надёжные вычисления).

В этих «сущностях» много общего, но есть и разница:

- ♦ «доверенные вычисления» обеспечивают защиту вычислений от непрогнозируемого и/или несанкционированного влияния при реализации политик безопасности, предлагаемых поставщиком «доверенной» вычислительной платформы;

- ♦ а концепция «надёжных вычислений» основана на подходе, в рамках которого пользователь, применяя «доверенные» аппаратные и программные компоненты для создания вычислительной платформы, реализует собственные представления об ИБ.

И «надёжные» и «доверенные» вычисления опираются на такие базовые технологии, как шифрование (симметричный и асимметричный алгоритмы), вычисления хэш-функций, использование криптографических контрольных сумм сообщений (Message Authentication Codes или Message Authentication Checksums / (MACs)).

Дополнительно к этим базовым технологиям используются и другие приёмы и механизмы. При этом до сих пор не удалось создать платформы, где «надёжность» или «доверенность» вычислений была бы гарантирована исключительно программными средствами на том же уровне, что обеспечивается совместным применением программ-

ных и аппаратных средств. Считается, что лишь аппаратные средства гарантированно защищают вычислительную платформу от вмешательства со стороны хакера, получившего к этой платформе физический доступ. Поэтому в состав процессорных микросхем, как правило, встраиваются специализированные аппаратные блоки для защиты всей микросхемы от различных типов атак.

Наиболее известными является т.н. «x86_64 архитектура процессоров Intel». Но в критических ИТ-инфраструктурах часто используются процессоры с архитектурой POWER (IBM) и UltraSPARC (Sun/Oracle), а в последнее время и с архитектурой ARM, превращающейся в открытый стандарт де-факто для широкого круга процессоров — от микроконтроллеров до серверных микросхем.

ПОРА ТРЕБОВАТЬ ОТДЕЛЬНУЮ СТРАТЕГИЮ

Стандартом популяризации выше-названных архитектур является упоминание о реализации в процессорах механизмов trusted- и trustworthy computing. Это, например, т.н. «технологии» Software Guard Extensions (SGX); Secure Encrypted Virtualization (SEV); SecureBlue++; TrustZone и некоторые другие.

Тем неприятнее оказались предположения уже упомянутой израильской CTS Labs о том, что найденные её специалистами «дыры» позволяют получить контроль над подсистемой обеспечения безопасности AMD Secure Processor (уязвимости класса RyzenFall); вмешиваться в работу механизмов обеспечения безопасности Secure Encrypted Virtualization (SEV) или Firmware Trusted Platform Module (FTPM) (из-за ошибок в прошивках процессоров EYUC и Ryzen); считывать информацию из защищённых областей памяти («бреши» Fallout).

Т.е. налицо все основания предполагать, что существенная часть т.н. «бюджетных» реализаций аппаратных платформ отечественной ИТ-инфраструктуры, в т.ч. и «критической», потенциально небезопасна. И есть все основания потребовать (хотя бы в рамках программ

«Импортозамещение» и «Цифровая экономика») отдельной стратегии — стратегии обеспечения аппаратной кибербезопасности отечественной ИТ-инфраструктуры. Стратегии, сформулированной в явном виде, детально, начиная с уровня микросхем и вплоть до продуктов для сетевой инфраструктуры государства.

ОПЫТ ЕСТЬ

Определённый задел в этой области в нашей стране есть. Например, результат совместных усилий отечественных компаний — подсистема обеспечения «доверенных» вычислений на базе отечественных процессоров Мультикор (рисунок 1).

Несколькими отечественными компаниями накоплен определённый опыт, и в коалиции с естественными партнёрами нашей страны (будет на то политическая воля прорабов «цифровой экономики») вполне возможно создание фундамента критической ИТ-инфраструктуры без общеизвестных ныне аппаратных мин и подкопов в виде «технологии» Intel vPro и цензурирования устанавливаемого ПО.

Приведённые факты указывают на безотлагательную необходимость создания отечественных систем «надёжных вычислений». И тут без отечественной программы по возрождению электроники не обойтись.

ОТСТАВАНИЕ НЕ ТАК УЖ И ВЕЛИКО

Реализация подобных программ требует денег, ресурсов, идей, людей и технологий. Из этого набора в нашей стране две первые составляющие в избытке. Проблемы Meltdown&Spectre и исчерпание потенциала «Закона Мура» указывают на то, что ресурс привычных идей выработан до основания, и разработчикам всего мира придётся искать новые подходы с нуля — практически на равных.

Таким образом, реальное отставание от лидеров, представляющих опасность для отечественной микроэлектроники, лежит в плоскости технологий и кадров. Приходится признать, что тут возникли заметные бреши. Но эти бреши всё ещё могут быть за-



Рисунок 1. Блок-схема процессора Мультикор

крыты. В стране продолжают работать ряд компаний, разрабатывающих SoC-конструкции процессоров на основе собственных разработок и процессоры с открытыми архитектурами ARM и MIPS. На их основе изготавливаются (к сожалению, на зарубежных фабриках) реальные процессорные микросхемы.

В России есть компании, которые продуктивно работают в области технологий систем шифрования конфиденциальной информации и создания систем управления шифрованием на основе аппаратных архитектур. Ими предлагается оборудование как «бюджетного» класса, так и предполагающее несколько уровней обслуживания.

Официально признаваемый авторитет отечественных разработчиков ПО позволяет активизировать разработки «доверенного» системного ПО для поддержки механизмов обеспечения безопасности аппаратных платформ.

* * *

Менталитет класса «не успели» в принципе неприменим к нашей стране, имеющей за плечами богатый опыт навёрстывания упущенного. Как бы гуманитарно и эмоционально, на первый взгляд, ни выглядело это утверждение. Тем более что в рамках союзного государства сохранена база для возрождения микроэлектроники.

**Александр БОДРИК**

вице-президент по ИБ московского отделения ISACA, экс-руководитель направления ИБ-экспертизы THK-BP, экс-исполнительный директор MSSP (SOC), ITIL Expert

SEX QUESTIONS

О ЦИФРОВОЙ БЕЗОПАСНОСТИ ДЛЯ ЦИФРОВЫХ БИЗНЕС-МОДЕЛЕЙ

«**Ц**ифровая трансформация — это не про технологии, но про изменения», — утверждает одна из самых признанных книг Питера Уэйлла и Стефани Уорнер (1). Соответственно «в процессе изменений бизнес становится уязвимым, и наша задача — измениться самим, чтобы адекватно и актуально поддерживать и защищать его ключевые элементы» (2).

Ключевой задачей цифровой трансформации, по мнению авторов, становится изменение способа мышления — центрирование портфеля продуктов и услуг вокруг жизненных ситуаций клиента. Жизненные ситуации знакомы: все мы когда-то шли первый раз в первый класс, и наши родители были озадачены расходами на школу, все мы заводили семью и приобретали жильё, теряли работу и брали кредиты до лучших времён.

Плохая новость: переосмысление и органичная перестройка портфеля продуктов делает наши организации более понятными и для злоумышленников. Теперь старый принцип security by obscurity («безопасность через неизвестность») не работает от слова «совсем». Внешние и внутренние злоумышленники больше не будут введены в затруднение сложностью наших организаций, они будут понимать для чего создаются те или иные продукты или услуги, какие примерно корпоративные ресурсы выделяют организации — просто примерив на себя жизненную ситуацию и прикинув количество клиентов.

ЦИФРОВЫЕ БИЗНЕС-МОДЕЛИ

Согласно книге (1) все компании подразделяются на четыре типа — Поставщики, Омни-канальный сервис, Экосистемы и Специализированные сервисы.

Поставщики — традиционные компании: страховые, управляющие, медиа... Они производят продукты сами, но продают их через других, например, агентов и брокеров. Конкурентоспособность Поставщиков зависит от управления себестоимостью, а значит, в таких компаниях будет востребована функция защиты и контроля от мошеннических действий (Fraud Management), которые по различным оценкам приводят к потерям от 5 % до 50 % от выручки компании (данные опросов глобальной Ассоциации сертифицированных специалистов по борьбе с хищениями (ACFE) и российского отделения Ассоциации менеджеров по безопасности (ASIS)).

Низкая себестоимость достигается бизнесом и через увеличение масштаба бизнеса («эффект масштаба»), а значит, на счётах растущих компаний всегда накоплен большой оборотный капитал, нуждающийся в защите (атаки Business Email Compromise, традиционные банковские трояны).

Омни-канальные сервисы — банки, ритейл, телеком — производят продукты, а также контактируют с клиентами напрямую, а значит, знают о клиентах много и соответственно должны защищать базы данных, внедрять развитые системы управления приватностью

(privacy), например, на основе стандарта BS 10012. Системы управления приватностью дают клиентам чувство уверенности в компании и снижают риски интервенций со стороны государства.

Их точки контакта с миром («поверхность атаки» в терминологии Microsoft) могут составлять сотни единиц, и с точки зрения защиты от внешнего нарушителя именно на них стоит фокусироваться при разработке стратегического плана ИБ.

В силу значительного присутствия компании в цифровых каналах важна и защита бренда — негатив от действий мошенников неизбежно докатится до владельца бренда.

Экосистемы — маркетплейсы (Amazon, Uber) — полная противоположность Поставщикам. Они не производят продукты, но оперируют на перекрестке интересов конечных клиентов и поставщиков, используя максимум данных и о тех и о других. Защита точек контакта, полученных и собранных данных является для экосистем приоритетом, важно им и доверие клиентов и партнёров, поэтому для них необходимо внедрение системы управления информационной безопасностью (СУИБ) на основе общепринятых стандартов (ISO 2700x).

Специализированные сервисы — PayPal, Kabbage — не разрабатывают продукты для конечного клиента, но делают возможным рост экосистем. Как и Поставщикам им необходимо управлять себестоимостью, в том числе с помощью Fraud Management, а как



элементам большой экосистемы — продемонстрировать прозрачность и эффективное управление безопасностью путём внедрения СУИБ.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СЛУЖБЫ ИБ

Многие компании пытаются изменить свою цифровую бизнес-модель. Например, страховые компании Альфа-страхование и Ингосстрах запустили продажу полисов через Интернет, Яндекс запустил маркетплейс Яндекс.Такси, а Сбербанк и Mail.ru — свои маркетплейсы товаров.

В такой ситуации важно донести до руководителя компании, что изменение бизнес-модели потребует существенного изменения бюджета, структуры, компетенций и технологий в подразделении ИБ. К примеру, нефтегазовая компания, решившая торговать бензином через интернет (как стартап Benzuber), должна на порядок усилить процесс обеспечения безопасности Интернет-ресурсов. Теперь при вводе системы в эксплуатацию недостаточно делать её пентест и прогонять по чек-листу безопасности. Нужно проверять все обновления в части дизайна безопасности, организовать цикл безопасной разработки и постоянно проверять безопасность доступных из Интернета сервисов. Нужна отдельная программа проектов, новые внутренние сервисы безопасности и новая система управления ИБ. Зачем? Чтобы понять, как и когда на-

чинать применять все корпоративные требования к новым бизнесам, бизнес-экспериментам и постоянно растущему количеству общих предприятий.

НОВЫЕ КЛЮЧЕВЫЕ КОМПЕТЕНЦИИ СЛУЖБЫ ИБ

Отдельная проблема: руководитель службы ИБ не знает в точности, какие компетенции и ресурсы потребуются в будущем для поддержки цифровой трансформации бизнеса. Однако совершенно точно понадобятся три новых направления:

- ◆ Бизнес-партнеры, которые смогут наладить и сохранить отношения с ключевыми игроками бизнес-подразделений, несмотря на стресс и все изменения. Такие специалисты должны обладать пониманием бизнеса, чувством такта и способностью держать удар в любых обстоятельствах.

- ◆ Менеджеры внутренних продуктов ИБ как гаранты соответствия ключевых продуктов ИБ новым бизнесам, особенно тем, что совсем непохожи на традиционные виды деятельности организации. Такие специалисты должны обладать продуктовым мышлением,

определённой коммерческой жилкой и переговорными навыками.

- ◆ Проектный офис для поддержания скорости изменений внутри службы ИБ.

ОПАСНОСТЬ — ЭТО ВОЗМОЖНОСТИ

Цифровая трансформация на первый взгляд несёт большой карьерный риск для руководства службы ИБ. Много изменений и стрессов — и всё это без очевидного изменения компенсации или полномочий.

* * *

Однако в любой опасности содержится возможность. В цифровой трансформации — это возможность лучше узнать новых игроков в бизнес-подразделениях, наладить связи с бизнес-лидерами, для которых ИБ теперь — не «ещё одна навязанная статья затрат», а необходимость для успешного бизнеса. Таким образом, можно создать новые опоры внутри организации и перестать зависеть исключительно от воли непосредственного руководителя.

ЛИТЕРАТУРА

1. What is your business model? Six questions to build the next-gen enterprise. Peter Weill & Stephanie Woerner. 2018, Harvard Business Press.
2. Business model for information security. 2009, ISACA.



Первое интеллектуальное шоу по информационной безопасности

*Смотри новые выпуски
и становись участником игры:
igra.ib-bank.ru*





Форум
Россия 2019

**XVII международная конференция по проблематике
инфраструктуры открытых ключей и электронной подписи**

**г. Санкт-Петербург
17–19 сентября 2019 года**

www.pki-forum.ru



**Встречаемся
в Питере!**

АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Образование
и карьера

ib-bank.ru