



20> Дмитрий СКОБЕЛКИН
Банк России
Стратегические приоритеты

37> Екатерина РАЧКОВА
(КАЛАШНИКОВА)
Банк ВТБ (ПАО)
Вредные советы

42> Денис КОРЯКОВСКИЙ,
Алексей ТЕРЕНИН
Сбербанк
ИИ на страже данных

67> Татьяна СТАНКЕВИЧ
Код безопасности
ЗДОРОВО-е питание в облаке



112> «Он видит будущее»
К 75-летию
В.Г.Матюхина

БЕЗОПАСНОСТЬ В ИСКУССТВЕ БАЛАНСА



15–17
сентября



📍 AZIMUT Отель Санкт-Петербург

3 МЕРОПРИЯТИЯ

ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОБЪЕДИНЯТСЯ В ОДНОМ МЕСТЕ

ПОДРОБНОСТИ НА САЙТЕ



Форум
Россия 2020



КОМПЛЕКСНАЯ
ЗАЩИТА
ИНФОРМАЦИИ

kzi.su

pki-forum.ru

ctcrypt.ru



**Игорь
НЕКРАСОВ**
главный редактор

Посидеть месяц дома неплохо. Обозреть в неспешной динамике необозримые поля социальных сетей и прийти к старому доброму выводу: кто-то становится умнее, кто-то глупее, а тысячи прочих ни в чём не меняются... Но любопытных ассоциаций много, в том числе и для информационной сферы. Большинство из самых интересных посвящены банальному, но иррационально тревожащему постулату: мир после коронавируса не будет прежним.

Вот, например, один писатель в своем посте заявляет, что несомненным признаком средневековья является фантастическая шаткость мнений о реальности, и приводит в качестве примера выступление главного инфекциониста страны, который «будто тувинский шаман 13 века говорит о мистической странности ковида». Я посмотрел по ссылке, и да, действительно, выступление доктора наук, профессора Никифорова очень неоднозначное, но суть не в нем, и даже не в выводе писателя, утверждающем на основании этого и, видимо, других разных высказываний, что мы вступили «в эпоху убийственно мрачного разброда мнений и мракобесной научной неопределенности во всем — от вирусов до цифровых сфер».

Интересное в ответах на этот пост.

«Выходом из Темных веков стал Ренессанс — взрыв творчества. У тысяч людей возникла потребность творить!» Это приятная, потому что оптимистическая, трактовка нашего постулата.

Другой ответ: «Всё просто: увеличилась скорость распространения информации. Мы её получаем мгновенно, в необработанном виде. Быстрая коммуникативность — враг устойчивых концепций».

И именно тут, на этой мысли, посещает откровение: как хорошо, что BIS Journal выходит по старинке — в своей бумажной версии. Не умаляя, конечно, стремительных достижений его электронной версии в контексте роста масштабов и популярности портала ib-bank.ru. Портал давно стал главным оперативным ресурсом отрасли ИБ. А вот в бумажной версии журнала мы не можем похвастать быстрой коммуникативностью, о чём ничуть не жалею. Потому что мнения, которые мы в ней представляем, готовятся долго, обстоятельно. Например, тема номера — «Смена парадигмы ИБ» и большинство других были сформулированы задолго до апреля — нашего маленького средневековья, а выйдут к читателю гораздо позже — в эпоху, будем надеяться, большого (или хотя бы малого) Ренессанса.

Отличное время для смены концепций.

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

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Былевский П. Г. — шеф-редактор, кандидат философских наук
Велигура А. Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А. Ю. — специалист Службы информационной безопасности КБ Максима (ООО)
Вихорев С. В. — советник генерального директора по информационной безопасности IT Expertise
Воробьева А. А. — руководитель интернет-проектов
Дзержинский Ф. Я. — главный эксперт — координатор системной экспертизы ООО «ТехноСофт»
Зубков А. Н. — генеральный директор ООО «Медиа Групп» «Авангард», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Курило А. П. — президент компании «Реальная безопасность», кандидат технических наук
Левиев Д. О. — председатель Совета НП «Партнерство специалистов по информационной безопасности»
Мельников С. Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», кандидат физико-математических наук
Некрасов И. В. — главный редактор журнала
Одувалов М. В. — руководитель службы Управления по обеспечению ИБ Банка ВТБ (ПАО)
Окулесский В. А. — заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук
Пазизин С. В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО), кандидат физико-математических наук
Рачкова (Калашникова) Е. В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО)
Филипчук А. А. — технический директор ГК ЦРТ
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

Баранов А. П. — заведующий кафедрой ИБ НИУ ВШЭ, доктор физико-математических наук, академик Академии криптографии РФ
Батранков Д. В. — консультант по информационной безопасности Palo Alto Networks
Гадарь Д. А. — вице-президент — директор департамента информационной безопасности, Tinkoff.ru
Калемберг Д. А. — генеральный директор ООО «СэйфТек»
Лукацкий А. В. — бизнес-консультант по безопасности Cisco Systems
Сабанов А. Г. — заместитель генерального директора ЗАО «Аладдин РД»
Сумманен К. Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук
Хайретдинов Р. Н. — заместитель генерального директора АО «Инфовотч»

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И. В.**
Шеф-редактор: **Былевский П. Г.**
Директор по развитию: **Минаков А. В.**
Арт-директор: **Мельников Н. С.**
Руководитель интернет-проектов: **Воробьева А. А.**
Руководитель спецпроектов: **Седов О. В.**
Обозреватели, корреспонденты: **Куликов В. А., Бродская М. А., к. т. н.**
Иллюстрация на 1-й обложке: **Виктор Миллер Гауса**
Фото в номере: **фотобанк DepositPhotos, Салаватова Я. М., wikipedia.org, ramyat-naroda.ru**
Цветокорректор: **Науменко М. Б.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Групп» «Авангард»
Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д. 21
Тел.: +7 499 271-70-85
Интернет-версия: ib-bank.ru/bisjournal
E-mail: bis@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).
Свидетельство ПИ № ФС 77-61378 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 20.04.2020. Тираж 7000 экз.
Заказ №242020. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS Journal, 2020



НОВОСТИ

- 5 **Технологии, в мире, в России, криминал**

ТЕМА НОМЕРА

- 10 **Смена парадигмы ИБ**
Андрей Курило (Реальная безопасность)
Информационная безопасность. Остановиться, оглянуться...
- 17 Алексей Лукацкий (эксперт BIS Journal)
«Верхи не могут, а низы не хотят»
- 18 Карл Сумманен (эксперт BIS Journal)
«Главная проблема — отсутствие в стране единого института, ответственного за развитие системы ИБ в целом»

РЕГУЛЯТОРЫ

- 20 **Стратегия**
Дмитрий Скобелкин (Банк России)
Стратегические приоритеты
- 26 **Взаимодействие**
Вадим Уваров (Банк России)
«Если кто-то кое-где у нас порой...»
- 31 **Нормативы и надзор**
Андрей Выборнов (Банк России)
Проверка боем



БАНКИ

- 34 **Обзор**
Денис Середенко (ПАО «Плюс Банк»)
ИТ и ИБ — конъюнкция или дизъюнкция?
- 37 **Новая рубрика**
Екатерина Рачкова (Калашникова)
(Банк ВТБ (ПАО))
Вредные советы
- 40 **SOC**
Дмитрий Гадарь, Игорь Кубышко (Tinkoff.ru)
Эффективный SOC — это сложно, но недорого
- 42 **Технологии**
Денис Коряковский, Алексей Теренин
(Сбербанк)
ИИ на страже банковских данных
- 49 **Антифрод**
Алексей Войлуков (Ассоциация банков России), Сергей Вельц (Кибертоника)
Третий путь
- 52 **ДБО**
Евгений Карпов (АО КБ «Хлынов»)
Разумный компромисс



УГРОЗЫ И РЕШЕНИЯ

- 58 Контроль действий**
Дмитрий Михеев (АйТи БАСТИОН)
Сотрудники «на удалёнке»
- 60 Автоматизация**
Екатерина Степанова, Илья Кондратьев (АМТ-ГРУП)
ГОСТ оправдывает средства?!
- 64 Файловый обмен**
Дмитрий Сушков (АО «МСП Банк»)
Цель достигнута!
- 65 Виртуализация**
Владимир Верещагин (Код Безопасности)
Пять вопросов
- 67 Облака**
Татьяна Станкевич (Код Безопасности)
ЗДОРОВО-е питание в облаке
- 70 SIEM**
Иван Лопатин (ДиалогНаука)
Система под контролем

ИНФРАСТРУКТУРА

- 73 Деловые мероприятия**
XII Уральский форум «Информационная безопасность финансовой сферы»
- 78 Деловые мероприятия**
Корней Реут (BIS Journal)
iFin-2020
- 79 Деловые мероприятия**
Марк Новодачный (BIS Journal)
Made in Russia 2020
- 80 Деловые мероприятия**
Николай Кольский (BIS Journal)
Регулятор и пустота
- 80 Деловые мероприятия**
Николай Кольский (BIS Journal)
«Корпоративная безопасность» 2020
- 83 Денежное обращение**
Елена Меланич, Сергей Касьян (Ассоциация организаций в сфере наличного денежного обращения, инкассации и перевозки ценностей)
АНДО. Наличные. Надолго!

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 85 Юридические лица**
Артем Прохоров (эксперт ИБ)
Кто под маской?
- 87 Инсайд**
Ольга Лимонова, Андрей Жаркевич
(Антифишинг)
Выученный инсайд
- 93 Инсайд**
Александр Пальцев (АО Русагротранс)
Борьба с инсайдом в страховании
- 95 Инсайд**
Лев Матвеев (СёрчИнформ)
«Предотвращать инсайдерские инциденты — задача непростая. Но и не фантастическая»
- 98 Обзор**
Сергей Мельников
(Лингвистические и информационные технологии)
Определяем автора

ОБРАЗОВАНИЕ И КАРЬЕРА

- 100 Нормативная база**
Василий Окулесский
(Банк «Возрождение»)
«Прочитал с пристрастием, и кое-что нашел...»
- 102 Нормативная база**
Сергей Вихорев (ООО «ИТ-Экспертиза»)
«Мы все учились понемногу...»
- 104 Обзор**
Марина Бродская (BIS Journal)
Точки отсчёта множатся
- 107 За рубежом**
Валерия Мещерякова (студентка факультета журналистики Университета Сорбонны)
Как там во Франции?



СУБЪЕКТЫ

- 112 Юбилей**
Слово о настоящем руководителе. К 75-летию В. Г. Матюхина
- 113** Виктор Пярин (лауреат Государственной премии Российской Федерации в области науки и техники)
«Он видит будущее»
- 115** Борис Гиричев (лауреат Государственной премии Российской Федерации в области науки и техники)
Прародитель идей
- 117** Андрей Галдин (АО «НИИАС»)
Человек с большой буквы
- 119** Александр Шабунин (АО «НИИАС»)
Колоссальный сдвиг в отрасли
- 120** Артем Зубков (Медиа Группа «Авангард»)
«Вы — это ваш масштаб!»
- 121 История**
Борис Столпаков (историк криптографии)
Криптографический фронт
- 124 История**
Борис Столпаков (историк криптографии)
Слушают или нет?
- 128 Неделовые мероприятия**
Екатерина Коденцева (BIS Journal)
Разожгли в сердце огонёк

КОШЕЛЬКИ PAYPAL И VENMO В ОПАСНОСТИ!

В нескольких онлайн-проектах (в том числе PayPal и Venmo) найдена уязвимость, дающая контроль над аккаунтами. Для успешной атаки нужно знать только номер телефона жертвы.

Уязвимость обнаружили специалисты Принстонского университета — они сообщили о 17 компаниях, которые находятся под угрозой (среди них Amazon, PayPal, Venmo, Blizzard, Adobe, eBay, Snapchat и Yahoo). Их сервисы позволяют сбрасывать пароль с помощью текстовых сообщений, доставляемых на телефон, а значит, хакеры могут провести атаку SIM swapping и получить контроль над нужным аккаунтом.

После оперативного уведомления всех компаний, специалисты проверили, кто из них устранил уязвимость. Adobe, Blizzard, Ebay, Microsoft и Snapchat — да. PayPal и Venmo — пока нет. Эти сервисы могут привязаться к бан-

ковским картам и счетам, поэтому наличие этой уязвимости для них критично.



ВЗЯЛИСЬ ЗА РОУТЕРЫ

Хакеры взламывают роутеры, перенаправляя людей на сайты, посвященные новому коронавирусу. Попад на такой сайт, пользователь рискует «сдать» хакерам свои пароли и учётные данные от криптовалютных кошельков. Специалисты из Bitdefender сообщили, что преступники атакуют маршрутизаторы Linksys. По другой информации —

D-Link. ИБ-исследователи пока не вполне понимают, как именно взламываются маршрутизаторы.

По одной из версий, хакеры угадывают пароли, защищающие консоль удалённого управления роутеров. Также они могут зайти через облачные аккаунты пользователей устройств от Linksys. Проникнув в систему роутера, операторы переназначают серверы DNS.

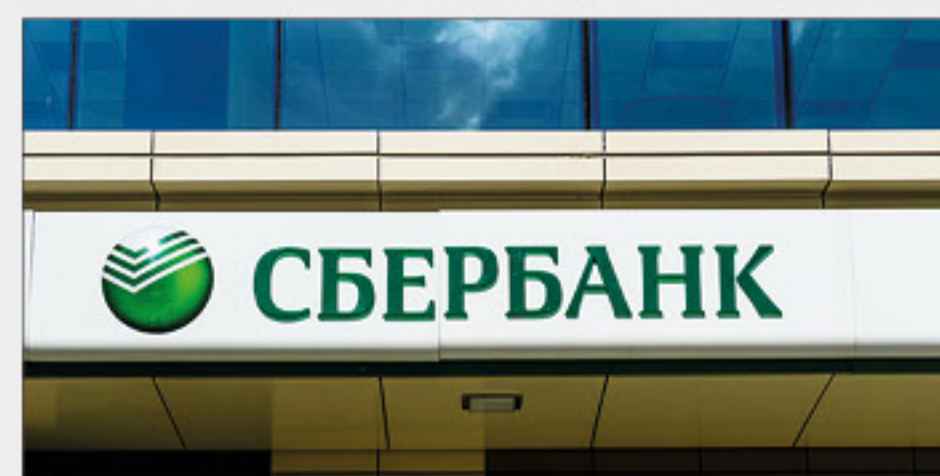


СБЕРБАНК ПОДКЛЮЧИЛСЯ К СБП

31 марта «Сбербанк» подключился к Системе быстрых платежей. Сейчас тестируются переводы на некоторых клиентах.

«После того, как мы убедимся, что сервис работает стабильно, переводы через СБП начнут постепенно появляться в «Сбербанк Онлайн», — объяснили представители кредитной организации.

Ранее Герман Греф выступал против обязательного подключения к СБП. Мотивация: у «Сбербанка» уже есть собственная система переводов по номеру телефона и QR-платежей.



РОСКОМНАДЗОР ПРОТИВ VPN-СЕРВИСОВ

В этом году Роскомнадзор запустит автоматизированную систему мониторинга поисковых систем, прокси и VPN-сервисов, позволяющих обходить блокировки ресурсов в РФ. Она уже находится в стадии тестирования.

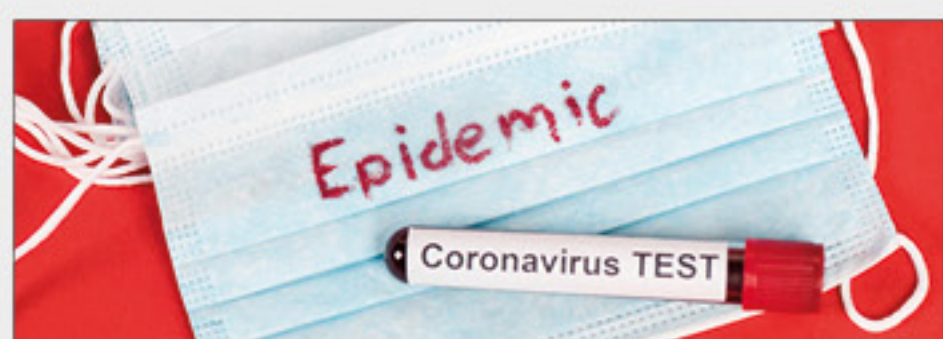
В апреле 2019 года прошёл конкурс по выбору подрядчика, в котором победил ФИЦ «Информатика и управление» РАН. Согласно сайту госзакупок, стоимость системы мониторинга составляла 25 млн руб., но в итоге цена снизилась до 19,92 млн руб. Акт приёма-передачи был подписан 24 декабря, и сейчас система функционирует в режиме опытной эксплуатации.

 **РОСКОМНАДЗОР**

УГРОЖАЮТ КОРОНАВИРУСОМ

Мошенники активизировали уже знакомый вид вымогательства sextortion, однако на этот раз несколько иначе. Ранее этот способ выглядел так: пользователю приходило письмо, в котором мошенники утверждали, что владеют записью с веб-камеры жертвы, на которой запечатлён процесс посещения порносайта, и угрожали разослать эту запись его знакомым.

Теперь кибервымогатели обещают заразить жертву, если та не пожелает откупиться, и всю её семью новой коронавирусной инфекцией. Некоторые в панике переводят деньги преступникам. ИБ-специалисты отмечают, что вымогатели могут не остановиться на первой сумме.



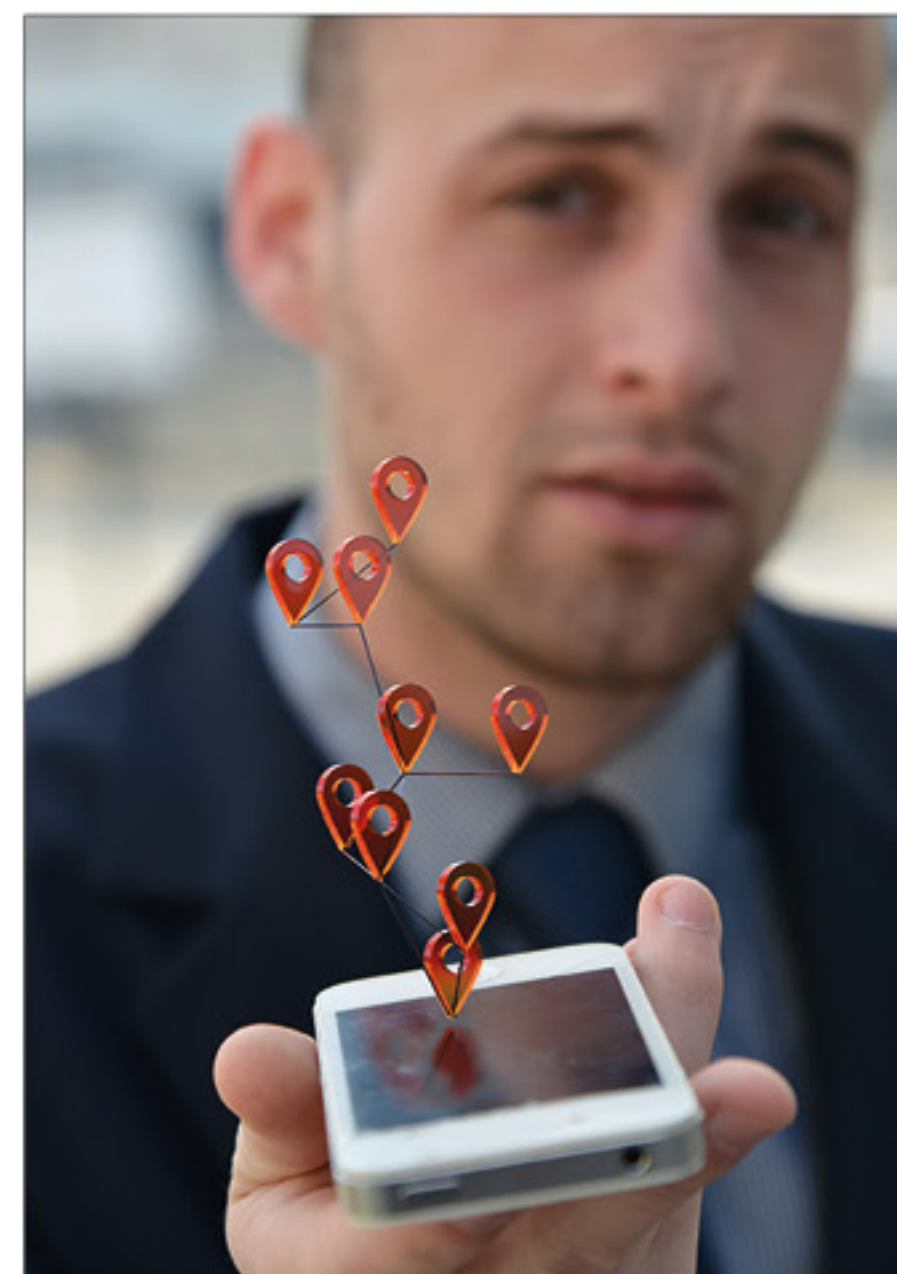
ПАНДЕМИЯ — НЕ ПОВОД ДЛЯ СЛЕЖКИ

Учёные и исследователи из 25 стран опубликовали открытое письмо, в котором призвали правительства не злоупотреблять приложениями для отслеживания случаев заражения новым коронавирусом с целью слежения за гражданами.

К подобной реакции привела ситуация с некоммерческой организацией Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) — её критикуют за намерения централизовать данные о заражённых. Организация вызвала волну критики в связи со слабой прозрачностью и начала терять поддержку. Профессор Федеральной политехнической школы Лозанны Марсель Салате покинул инициативу. За ним последовали и другие.

Критики PEPP-PT поддерживают использование децентрализованного протокола отслеживания больных под названием DP-3T, сохраняющего

данные на гаджетах, а не отправляющего их в централизованную базу данных (управляемую, например, Минздравом).



26-я Международная выставка
технических средств охраны
и оборудования для обеспечения
безопасности и противопожарной защиты



Москва

11-14
августа
2020

МВЦ «КРОКУС-ЭКСПО»

Бесплатный билет
по промо-коду:

sec20BIS

securika-moscow.ru



Видеонаблюдение



Контроль
доступа



Охрана
периметра



Противопожарная
защита



Сигнализация
и оповещение



Автоматизация
зданий



НОВЫЕ ВОЗМОЖНОСТИ ДЛЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Пресс-службы ВТБ, Сбербанка и Росбанка сообщили о новых способах социальной инженерии в период пандемии коронавируса. Например, злоумышленники стали прикрываться банками, чтобы «помочь» клиентам оформить QR-коды, необходимые для перемещения по Москве и области.

«Да, появились новые сценарии атак на клиентов банков, особенно в контексте социальной инженерии. Мошенники эксплуатируют темы компенсаций от государства, штрафов за нарушение самоизоляции и другие. Очевидно, что по итогу периода будет зафиксирован рост числа киберпреступлений и убытков от них», — отметил эксперт BIS Journal Денис Калемберг.

Официальной статистики в России на эту тему пока нет, но, например, в Малайзии, по отчётам национального агентства кибербезопасности, за



период с 18 марта по 7 апреля количество инцидентов выросло на 82,5 % к аналогичному периоду прошлого года. По мнению Дениса Калемберга, это общемировой тренд и нам его не избежать.

БУМ НА РЫНКЕ ФИШИНГ-КИТОВ

По данным Group-IB, в 2019 г. число активных продавцов фишинговых наборов увеличилось на 120 % по сравнению с 2018 г. Брендами-фаворитами, от имени которых создавались фальшивые страницы, были Amazon, Google и Office 365. Количество уникальных объявлений, размещённых на этих ресурсах, также возросло больше, чем в два раза.

Вдвое выросли и цены. Так, в среднем один фишинг-кит стоит \$304 (в 2018 году — \$122). Как правило,

стоимость фишинговых наборов зависит от их сложности, а именно от качества и количества фишинговых страниц, а также наличия дополнительных сервисов, таких как, например, техническая поддержка со стороны разработчика. В то же время на форумах попадались и бесплатные варианты. Однако, это объясняется отнюдь не щедростью продавцов, а вероятным наличием в них бэкдоров, которые позволяют их авторам получать доступ к скомпрометированным данным.

Для привлечения покупателей разработчики наборов используют в них известные бренды, что в теории должно облегчить реализацию мошеннических схем для владельцев таких наборов. В 2019 г. наиболее часто используемыми брендами были Amazon, Google, Instagram, Office 365 и PayPal, а Топ-3 интернет-площадок для торговли фишинговыми наборами был представлен Exploit, OGUsers и Crimenetwork.



ФЕЙКОВЫЙ РАЗГУЛ НА ФОНЕ COVID-19

Компания ESET обнаружила новые виды мошенничества, появившиеся во время перехода предприятий на режим удалённой работы. Мошенники распространяют фейковые сообщения «с актуальной и достоверной информацией о COVID-19».

Одна из таких рассылок распространяет троян, похищающий данные. Вредоносный файл находится в приложении под видом документа, содержащем секретные сведения, как избежать заражения.

Цель следующего вида атак — компании, оказавшиеся в сложной финансовой ситуации в результате экономического кризиса на фоне пандемии. Ссылаясь на то, что работа финансовых учреждений замедлена, мошенники отправляют вредоносный файл под видом «гарантии оплаты» (например, выписки с банковского счета), вынуждая пользователя открыть его.

ЗНАНИЯ ПРОТИВ ВИРУСОВ

В рамках программы Kaspersky Security Awareness разработан бесплатный онлайн-курс «Безопасность во время пандемии в жизни и бизнесе».

Курс состоит из двух модулей. Первый полностью посвящён физической безопасности во время пандемии. Он помогает изучить, какую угрозу несёт COVID-19, как следует себя вести, чтобы минимизировать риск заболеть самому или заразить коллег.

Второй модуль помогает адаптироваться к удалённой работе и в целом повысить киберграмотность в условиях оторванности от офиса и привычной помощи системного администратора. Урок сконструирован так, что даже пользователи с невысокой цифровой грамотностью, смогут по его итогам организовать себе максимально безопасную работу из дома.

Курс разработан на базе адаптивной системы обучения. Он содержит теоретический материал и тесты.

ОТСРОЧКА НА ПОЛГОДА

Госдума на шесть месяцев отложила вступление в силу закона, который обязывает производителей предустанавливать на гаджеты и компьютеры российский софт.

Планировалось, что «антияблочный» закон вступит в силу 1 июля 2020 года. Отсрочка связана с пандемией коронавируса и общим экономическим спадом. Также за перенос даты высказались производители электроники и бытовой техники.

Норма начнёт действовать с 1 января следующего года, решила ГД РФ.

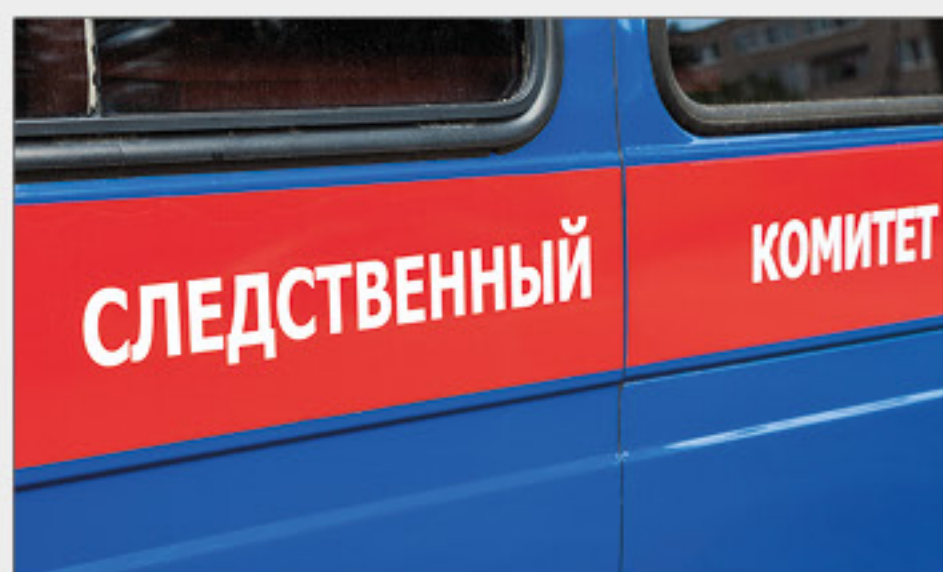


В СКР ПОЯВИЛСЯ КИБЕРОТДЕЛ

Следственный комитет России сформировал отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий.

Приказ о создании подразделения был подписан в декабре 2019 года председателем СКР Александром Бастрыкиным. Следователи нового отдела специализируются на расследовании преступлений, отличающихся «особой спецификой».

Инициатива продиктована увеличением количества киберпреступлений на территории России в последние годы.



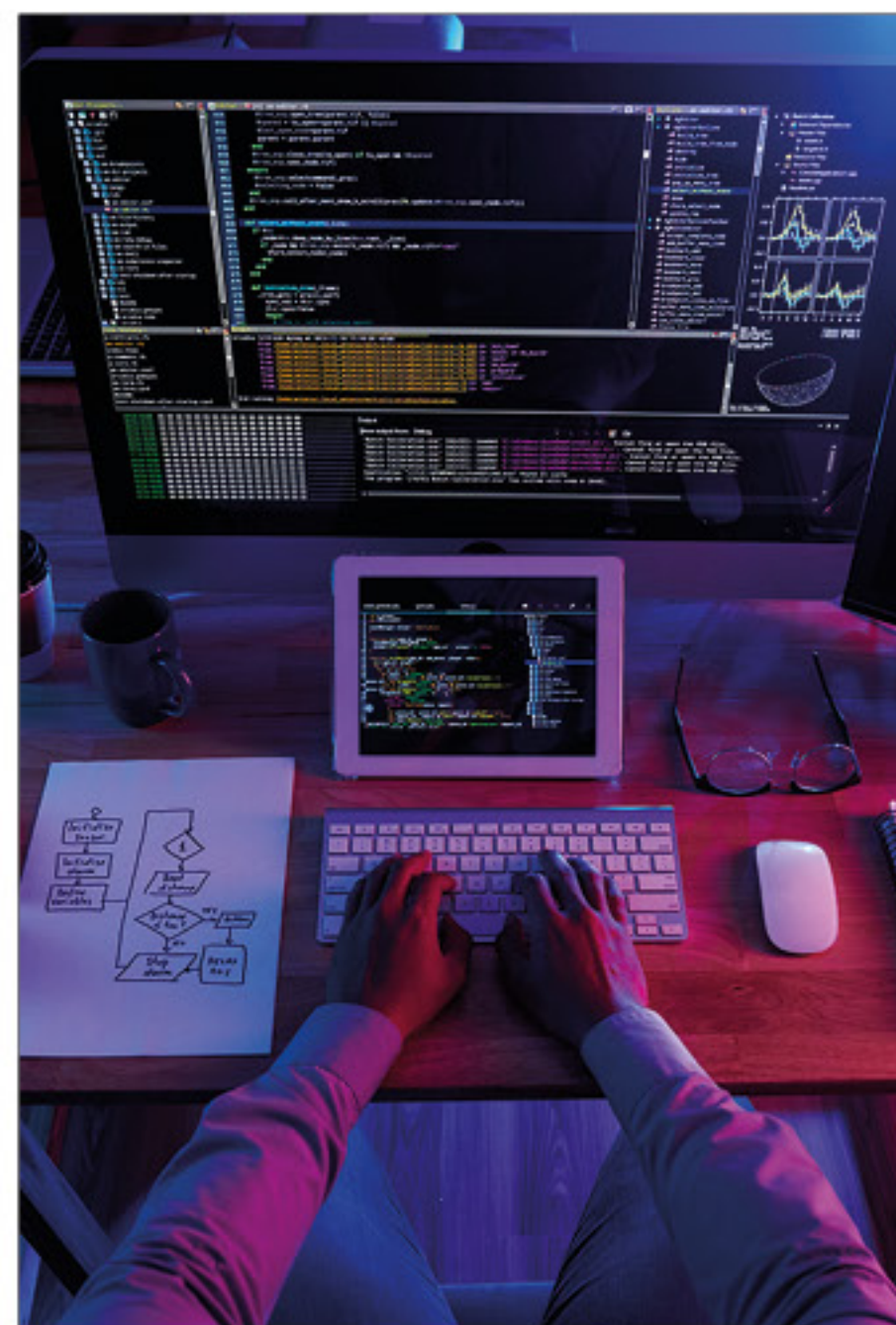
ФСТЭК ОБНОВИЛ МЕТОДИКУ МОДЕЛИРОВАНИЯ УГРОЗ

Федеральная служба по техническому и экспортному контролю России обнародовала новый вариант методики моделирования угроз, примечательный коррекцией самого подхода к моделированию.

Необходимо определить те негативные последствия, которые организация считает недопустимыми. Далее вычислить, что и как может привести к таким последствиям. И в итоге построить киллчейны, с помощью которых в теории можно это осуществить.

Согласно новой итерации методики, больше нельзя просто отбиться изолированностью сети и неактуальностью кибератак. Придётся продемонстрировать, что хакер не сможет добраться до вашей сети. Кроме того, при моделировании угроз теперь нужно учитывать меры защиты и возможные проблемы в применении

этих средств — меры защиты как таковые не являются панацеей от реализации угроз.



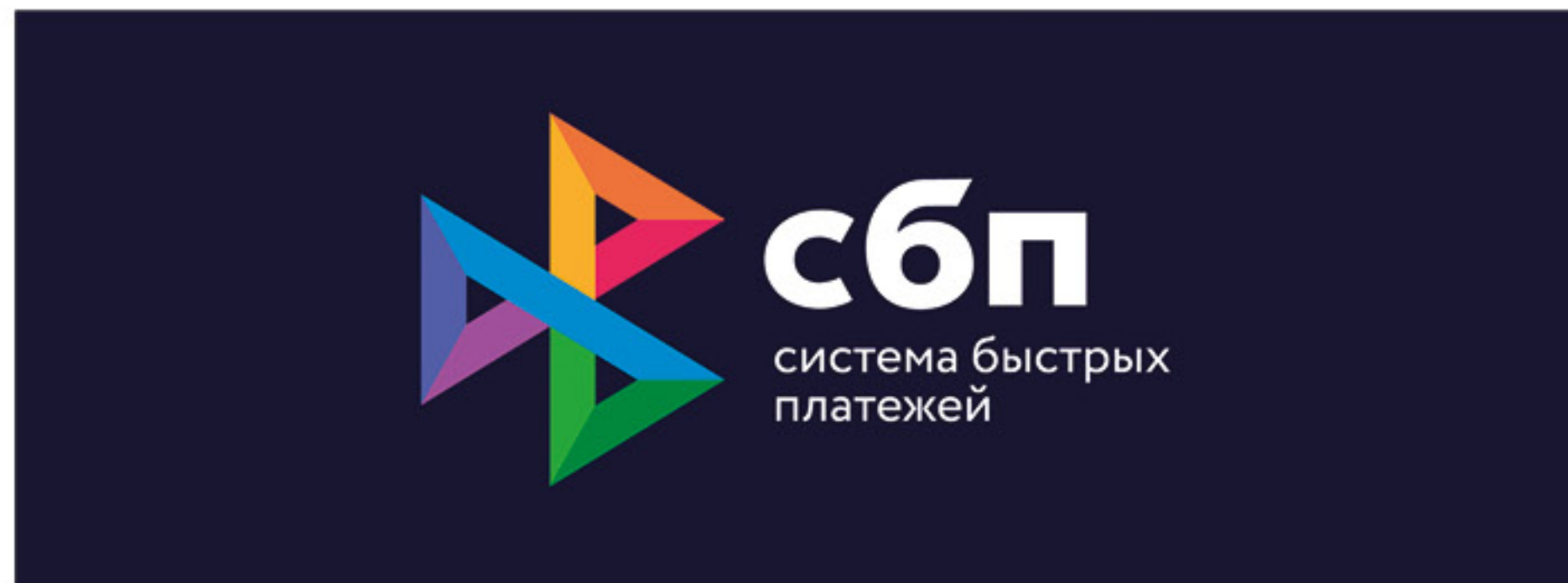
СБП ИЗМЕНИТ ПРОЦЕДУРУ ВОЗВРАТА СРЕДСТВ

С 1 июня будут изменены стандарты возврата средств, уплаченных через Систему быстрых платежей физлицом юрлицу.

В операционном бюллетене от 31 марта «Об операциях СБП в b2c (бизнес — потребителю)» сказано, что процедура возврата ранее уплаченных через СБП средств торгово-сервисным предприятиям (ТСП) меняется.

Эти платежи стали возможны с осени 2019 года. Они проводятся с

помощью QR-кодов и для ТСП стоят дешевле, чем стандартный эквайринг по банковским картам. С 1 июня потенциальное обналичивание станет невозможным — по новым стандартам возвраты можно будет осуществить только на оригинальную транзакцию. Также все юрлица, использующие Систему, должны будут зарегистрироваться в ОКЦП СПБ и получить единый идентификатор юрлиц (ИД ЮЛ).





ЗООМ СЛИЛИ В ОТКРЫТЫЙ ДОСТУП

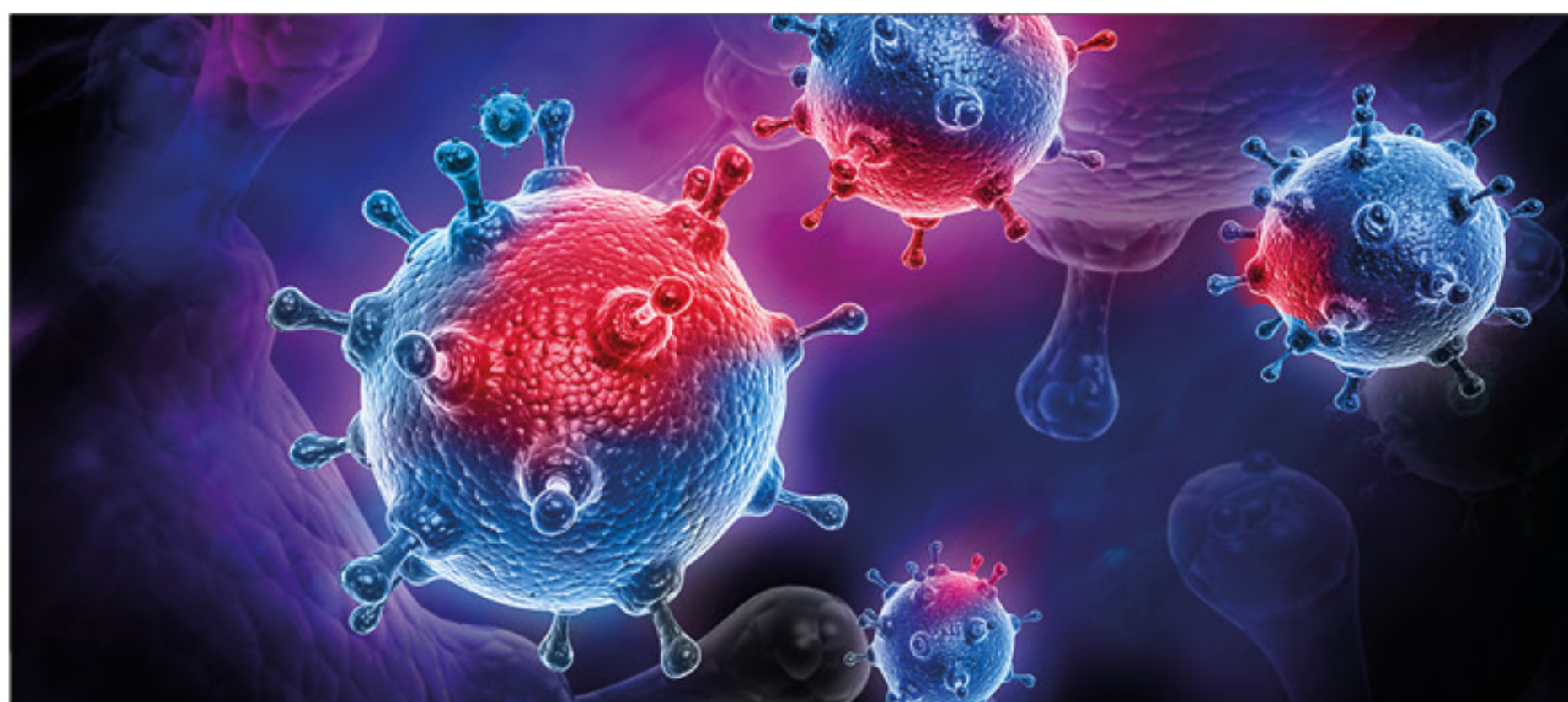
Записи «тысяч» видеозвонков, сделанных через Zoom, оказались опубликованы на YouTube и Vimeo: сеансы психотерапии, школьные занятия, медконсультации, а также совещания компаний, на которых обсуждали финансовые отчёты. Многие из коллов содержат персональные данные (имена и номера телефонов).

Zoom не ведёт запись по умолчанию, однако организаторы могут начать её — в этом случае все участники получат соответствующее уведомление. Есть мнение, что записи оказа-

лись в открытом доступе, так как были сохранены в отдельном незащищённом онлайн-хранилище.

Видеоколлам в Zoom присваиваются открытые идентификаторы, поэтому их легко найти через поиск. Таким способом было найдено более 15 тысяч записей.

Популярность сервиса значительно выросла из-за пандемии, потому что многим компаниям и людям пришлось переносить общение в онлайн. С декабря 2019 года аудитория Zoom выросла в 20 раз.



COVID-19 НА СЛУЖБЕ ФИШЕРОВ

Новые фишинговые письма приходят якобы от локальных медучреждений и гласят: получатель какое-то время находился рядом с источником нового коронавируса.

Преступники пытаются убедить сотрудников организаций в том, что у их домашних, коллег и друзей диагностировали коронавирус, вызывающий COVID-19. Далее послание рекомендует получателю провериться самому, скачав и распечатав прикреплённый

файл EmergencyContact.xlsm, а после отнеся его в ближайшую клинику.

При открытии файла пользователь должен будет разрешить выполнение определённого контента, после чего установится зловред.

Сам вредонос внедряет множество процессов в легитимные потоки вроде msixes.exe, что помогает ему уходить от обнаружения антивирусом. После этого ПО похищает цифровую валюту жертвы.

ЛИКВИДИРОВАНО ВОСЕМЬ МАЙНИНГОВЫХ ФЕРМ

Ущерб для энергоснабжающих компаний ежемесячно составлял порядка 15 миллионов рублей, такую же сумму злоумышленники получали в качестве незаконного дохода.

Майнеры добывали криптовалюту на восьми объектах в Ленобласти: в заброшенном здании птицефабрики в деревне Лесколово Всеволожского района, в здании базы отдыха в поселке Рощино, в ряде жилых помещений. Было проведено 20 обысков, в ходе которых было обнаружено 1500 спецустройств, более 2 млн руб., 100 модифицированных электросчетчиков, запрограммированных на занижение показаний расхода энергии с ДУ-пультами. Также было изъято 150 пломб и голографических этикеток, 5 пломбираторов, 10 устройств для вскрытия и модификации сертифицированных счетчиков учета расхода энергии.

ВИРУС АКТИВИЗИРОВАЛ МОШЕННИКОВ

ЦБ РФ предупредил о финансовых махинациях на фоне распространения в стране вируса SARS-CoV-2. Регулятор сообщил, что гражданам поступают звонки от мошенников, обещающих отсрочки по кредитам, пособия, компенсации за авиабилеты, услуги по диагностике заражения коронавирусной инфекцией, волонтерскую помощь и т.д.

Жертву просят сообщить реквизиты банковской карты, пароль из СМС или осуществить платёж самолично. Например, 5 апреля лжесотрудник банка позвонил московской пенсионерке и неустановленным способом похитил с её карты 963 тыс. рублей.

Авторы фишинговых рассылок поддельывают фирстиль сайтов известных организаций: Минздрава РФ, Роспотребнадзора, Банка России, ВОЗ и других.



Андрей КУРИЛО
глава компании
«Реальная
безопасность»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ОСТАНОВИТЬСЯ, ОГЛЯНУТЬСЯ...

ВГЛЯДИМСЯ В ПРОШЛОЕ, ЧТОБЫ
РАЗГЛЯДЕТЬ БУДУЩЕЕ

Наступает новое десятилетие — двадцатые годы XXI века. Смутные очертания будущего частично проглядывают, частично угадываются. Каким оно будет? Какие новости преподнесёт нам стремительно ускоряющийся научно-технический прогресс на фоне разворачивающихся в мире событий, какие новые проблемы, задачи, трудности, успехи и разочарования придётся нам пережить? Какие цели сформулировать и поставить перед собой, как их достичь и можно ли их будет достичь?

Контуры будущего сейчас в деталях рассмотреть невозможно, но уже вполне различимы общие тренды. И некоторые вещи выглядят, скажем мягко, недружественными.

Вполне очевидна перспектива утраты нами того самого «прайвеси», ради чего поднималась и разрабатывалась проблема персональных данных. С одной стороны, понятно наше желание ограничить круг собираемых данных о нас, с другой — становится очевидным, что без массового сбора и обработки ПД государство не в состоянии справляться с вызовами преступности, терроризма, а сейчас и массовых заболеваний.

При нынешнем качестве образования и поголовном использовании с пелёнок современных «гаджетов» — впереди массовое перестроение сознания и мышления, вместе с деградацией у новых поколений способности к длительному целенаправленному восприятию и анализу информации. Следствие этого — потеря квалифицированных кадров, утрата гуманитарных завоеваний, изменение и деградация общественного и индивидуального сознания.

Непонятно, куда нас заведёт «цифровая» гонка. Не потеряем ли мы реальную экономику, которая является фундаментом жизни?

Очевиден растущий разрыв между внедряемыми всё в возрастающей степени на бизнес-уровне прикладными технологиями и обеспечением их безопасности. И так далее.

Всё это означает, что, решая задачу развития проблематики информационной безопасности, просто жизненно необходимо понимать, что мы делаем, иметь ясную, понятную стратегию действий и активно её реализовывать, настойчиво «формировать будущее» в благоприятном для нас направлении, иначе это будущее будет сформировано кем-то другим и не в наших интересах.

НАЗАД В БУДУЩЕЕ

Весьма полезно, для примера, взглянуть на методологию, используемую военной наукой, которая предполагает постоянное изучение опыта прошлых войн одновременно с активным поиском тактики и стратегии в условиях ускоряющегося научно-технического прогресса. При появлении новых видов оружия такая методология часто приводит к качественному изменению тактики ведения боевых действий.

Очевидно, что тут крайне важна роль опережающих исследований на стратегическом уровне, чем занимается, например, Управление перспективных исследовательских проектов Министерства обороны США DARPA.

Попробуем и мы использовать старый и надёжный приём — вспомнить, понять и оценить прошлое, а через него — будущее. Вспомнить те мотивы, которые двигали нами, цели, которые мы ставили, и беспристрастно оценить результаты, которых мы достигли.

К тому же приближается ещё один славный юбилей — тридцатилетие начала работ по проблематике информационной безопасности в том её понимании, которое доминирует сегодня в нашем профессиональном сообществе.

1980–90-Е ГОДЫ

Итак. 90-е годы, если рассматривать их через призму информатизации информационной безопасности и права, выглядят совершенно не в негативном свете, не так, как мы привыкли рассматривать их в экономической, социальной и политической сферах. В зарождавшейся сфере информационной безопасности они были поступательными и крайне позитивными.

Во всём мире, включая нашу страну, в 80-е и 90-е годы шёл масштабный процесс внедрения «цифры» в практические сферы деятельности общества, включая науку, военное дело, промышленность, финансовую сферу. Коротко обозначим вехи: суперкомпьютеры, СУБД, всевозможные АСУ, персональные ЭВМ, Интернет, электронные платёжные и расчётные системы, кредитные карты, гражданская криптография + электронная цифровая подпись, система SWIFT.

Так совпало, что в это время в нашей стране происходила смена парадигмы государственного регулирования: осуществлялся переход от административно-командных способов управления к правовым, базирующимся на верховенстве закона. В экономике стала доминировать концепция рыночного саморегулирования. При этом выбраны были не лучшие модели управления, а накопленный ранее опыт оказался не востребуемым и был проигнорирован. В результате были утрачены в том числе целые отрасли промышленности, например, станкостроение и электронная промышленность, разрушена система стандартизации. Государственные стандарты утратили статус закона, что несомненно было существенным шагом назад, в архаику и дикие рыночные отношения. Как-то незаметно и тихо ушли корифеи, у которых мы учились.

В НАШЕЙ ПРОФЕССИОНАЛЬНОЙ СФЕРЕ

А что происходило в нашей профессиональной сфере? Вопросы информационной безопасности (тогда защиты информации АСУ, ЭВМ и ТСПИ) носили сугубо прикладной, закрытый характер и фактически были недоступны широкому кругу специалистов. Но работы велись, и они были адекватны реалиям. Приоритет отдавался вопросам защиты от утечки информации по радиотехническим каналам. Проблема-

Решая задачу развития проблематики информационной безопасности, просто жизненно необходимо понимать, что мы делаем, иметь ясную, понятную стратегию действий и активно её реализовывать

тика защиты от несанкционированного доступа была проработана недостаточно. Что касается моделирования угроз, то этот подход был в зачаточном состоянии, а такой класс нарушителей, как внутренний, тем более инсайдер, практически вообще не рассматривался в нашей стране, и что интересно — за рубежом тоже.

Именно в это время появилось само понятие «информационная безопасность», в которое разными специалистами вкладывался разный смысл: технические специалисты считали его родственным ранее возникшему понятию «защита информации» и определяли его как «деятельность», в отличие от «состояния».

Вторая группа специалистов рассматривала это понятие более широко, ставя во главу угла социально-политические и психологические аспекты существования и развития государства и общества. Собственно, это противопоставление существует и до сих пор, хотя в последнее время среди технических специалистов всё шире начинает использоваться понятие «кибербезопасность», которое ограничивает сферу рассмотрения и более точно отображает сущность феномена, с которым мы имеем дело.

ПРО ТУЛЬСКОГО ЛЕВШУ

Компьютерной преступности, то есть собственно основного противника, в стране практически не существовало (пожалуй, за исключением единичного случая махинации с платёжными базами данных в ВЭБ в начале 1980-х годов), поэтому специалисты в области защиты информации, формулируя концепции развития и планы работ, были вынуждены пользоваться либо моделированием будущих угроз, либо примерами из зарубежных источников, к чему руководство министерств и ведомств, от которых зависело принятие решений, относилось с серьёзной долей скепсиса.

Но тем не менее, мы получили гигантскую фору и могли самым серьёзным образом подготовиться к будущему.

Впрочем, плохое прогнозирование, реагирование на негативный результат только тогда, когда отклонение от желаемого становится

заметным и раздражающим (в теории автоматического управления этот метод «управления по отклонениям» классифицирован как самый простой и неэффективный) — наша национальная забава. Вспомним знаменитого тульского Левшу, за много лет до Крымской войны кричавшего о серьёзном отставании России в создании современного нарезного огнестрельного оружия. Смотрели на него как на чудака. Да кому он был нужен, зануда, — в результате его на всякий случай споили. Ну, он и умер от белой горячки. А ведь неправильное конструирование угроз стало одной из причин, если не поражения, то крайне высоких потерь русской армии в Крымской компании в середине XIX века.

В конце XX века созданная в стране по отраслевому принципу система защиты информации начала умирать вместе с отраслями промышленности, в первую очередь, из-за недостатка финансирования, пока не умерла вместе с ними в начале 90-х годов. В результате катастрофически сжалась научно-методологическая база. В созданных на месте почивших министерств бизнес-корпорациях эта тема должного развития не получила. Как следствие страну стала накрывать волна зарубежных стандартов и последовавших за ними продуктов и решений, прежде всего в IT- сфере, а потом и в безопасности. Собственно, сильнейшая зависимость от импорта не преодолена до сих пор.

ПЕРЕКОС В ДОКТРИНЕ

В этих условиях, усилиями специалистов и руководителей Гостехкомиссии СССР (России), Совета Безопасности России, КГБ СССР (МГБ, ФАПСИ, а впоследствии ФСБ России) были разработаны первые документы, регламентирующие вопросы защиты информации от несанкционированного доступа, а также, с участием специалистов Академии наук, сформированы первые концептуальные взгляды на направления развития проблематики информационной безопасности, впоследствии нашедшие своё отражение в первой Доктрине информационной безопасности Россий-

ской Федерации, утверждённой Президентом Российской Федерации 9 сентября 2000 г. (N Пр-1895).

В этой Доктрине были сформулированы национальные интересы Российской Федерации в информационной сфере, а под информационной безопасностью понималось состояние защищённости и баланс интересов личности, общества и государства, что в определённой степени перекосило понимание и развитие проблематики информационной безопасности.

НЕОПТИМАЛЬНАЯ КОНСТРУКЦИЯ

Законодательства в области информатизации и информационной безопасности в начале 90-х годов не было вообще. Но складывающаяся обстановка диктовала необходимость быстрого создания основополагающих законов, регулирующих отрасль информационной безопасности.

В результате удалось сформировать стратегию действий, заложить и в целом реализовать приоритетные направления работ, что и определило на длительный срок направления развития проблематики информационной безопасности.

К ним относятся:

1. Создание Государственной системы защиты информации.
2. Развитие законодательства в области:
 - ◆ информатизации, информационной безопасности и защиты информации;
 - ◆ административного законодательства и уголовного права в части установления ответственности за совершение компьютерных преступлений;
 - ◆ персональных данных;
 - ◆ использования электронной цифровой подписи.
3. Развитие необходимой нормативной базы по технической защите, с последующим выходом на систему стандартизации.
4. Развитие государственной системы лицензирования, аттестации и сертификации.
5. Создание системы подготовки кадров в области информационной безопасности.

Следует отметить, что традиционно регулированием вопросов, связанных с проблематикой информационной безопасности, у нас занимались два известных ведомства, строго соблюдая баланс интересов друг друга.

Известно также из теории и практики управления, что система управления, имеющая два центра управления, — конструкция не оптимальная и требует наличия арбитра (суверена), коим во времена СССР являлись ВПК при СМ СССР и по отдельным вопросам — ЦК КПСС. Эта схема была вполне работоспособной и эф-

Система управления, имеющая два центра управления, — конструкция не оптимальная и требует наличия арбитра (суверена), коим во времена СССР являлись ВПК при СМ СССР и по отдельным вопросам — ЦК КПСС

фективной. В новые времена все попытки реформировать систему безопасности государства оказались неудачными и снова привели к прежней конструкции, только место арбитра занял совещательный орган — СБ РФ.

ПРОМЕЖУТОЧНЫЕ ИТОГИ

Каковы итоги этой деятельности? Многое удалось сделать.

1. Создана Государственная система защиты информации.

Однако приоритеты системы оказались сдвинуты в сторону обеспечения интересов государства. Да по-другому и не могло быть.

Сдвиг приоритетов привёл к необходимости создания сильных отраслевых систем безопасности (ЦБ РФ), ориентированных на иные модели угроз и на решение практических задач, возникающих в банковском бизнесе. Одновременно началась дефрагментация системы управления, в результате чего число регуляторов по направлениям работ достигло пяти (вместе с Минюстом, утверждающим проекты НПА — шести), и это, не считая традиционно стоящих особняком отраслевых систем безопасности силовиков.

Последствия такого подхода просто бросаются в глаза — управление по сложившейся схеме, при слабой вертикали управления, через нормативное регулирование, становится всё более сложным, запутанным, управленческий цикл (от возникновения проблемы до появления нормативного акта) растягивается на годы, вызывая отставание от реальных потребностей. Возник и совершенствуется новый казуистический юридический язык, которым излагаются документы по информационной безопасности. В сообществе специалистов по безопасности появился новый термин — «бумажная безопасность». А на практике, между «бумажной» и практической, реальной безопасностью бывает очень большой разрыв, в который и пролезает преступность.

Хрестоматийный пример подобной практики регулирования — сначала аккредитация 500 удостоверяющих центров в России, потом осознание полной потери управления и контроля за их деятельностью и попытки резкого сокращения их числа. В результате резать уже придётся по живому.

2. В период с 1994 года (выход I части ГК РФ) по 2006 год (ФЗ «О персональных данных») сформирована в первом приближении необходимая законодательная база.

В более поздние времена шло интенсивное внесение изменений в ранее упомянутые ФЗ и Кодексы, а также был принят ФЗ «О безопас-

Управление по сложившейся схеме, при слабой вертикали управления, через нормативное регулирование, становится всё более сложным, запутанным, управленческий цикл растягивается на годы, вызывая отставание от реальных потребностей

ности КИИ РФ». Вместе с тем, нельзя считать этот процесс завершённым, так как ещё не нашли своего практического решения вопросы архивного хранения электронных документов и оборота юридически значимых электронных документов, присутствуют целые терминологические ямы, не покрытые НПА.

Возникло новое направление «цифровое право», в котором, правда, ученых-юристов гораздо меньше, чем IT-шников, а следовательно и правового осмысления происходящего. Но всё уже было, как говорил мудрый Экклезиаст. И проходило. Достаточно вспомнить императора Клавдия, который после того, как преданные подданные накормили его блюдом из бледных поганок, тут же написал Указ о том, чтобы эти грибы всегда подавали к царскому столу. И умер в муках. Вывод простой — не всегда следует сразу заниматься законотворчеством, особенно в неизвестном деле. Нужно помнить историю. Без этого двигаться вперёд, конечно, можно, но результат будет далеко не тот, на который мы рассчитываем.

3. В целом сформирована необходимая нормативная база по технической защите и стандартизации, определены регламенты и процедуры разработки и приёмки в эксплуатацию систем информационной безопасности.

Работы по совершенствованию нормативной базы ведутся с нарастающей интенсивностью.

Однако, есть вопросы к методикам оценки защищённости системы, иногда сливающимся с весьма древними методиками аттестации объекта. На этом фоне наиболее продвинутыми выглядят взаимоувязанные ГОСТы (57580.1 и 57580.2), разработанные Банком России, однако они распространяются только на финансовую сферу и только начинают применяться.

К сожалению, на фоне практически полной обеспеченности нормативными требованиями, остаётся невнятной ситуация со стандартизацией. Законодательный, то есть обязательный к исполнению, статус стандартов отменён вместе с распадом СССР. С этих пор стандарты приоб-

рели статус рекомендательных, то есть необязательных к исполнению документов. Процедура придания им обязательности через включение ссылок на них в НПА организации вызывала жёсткое сопротивление юридических служб на всех уровнях. Это надолго остановило процесс использования стандартов в сфере информационной безопасности.

Потребовалось разработать и утвердить в июне 2015 года ФЗ «О стандартизации в Российской Федерации», чтобы на основании ст. 27 этого Закона стало возможным включение в НПА ссылок на национальные стандарты и (или) информационно-технические справочники (однако только в том случае, если Правительство Российской Федерации, заинтересованные федеральные органы исполнительной власти, Государственная корпорация по атомной энергии «Росатом», иные заинтересованные государственные корпорации уполномочены на установление соответствующих требований). Чтобы решить эту проблему ЦБ РФ потребовалось включить в Закон о ЦБ отдельную статью, предоставляющую ему такое право.

То есть мы видим, что при соблюдении принципа добровольности применения стандартов реализуется не общее, а избирательное предоставление такой возможности отдельным ФОИВ (только через внесение изменений в права органа, как правило определёнными Законом). Процесс внесения поправок в ФЗ сложен и неоднозначен, а уж времени занимает — годы! Это не работа, это бюрократия в чистом виде.

В результате, в России вроде есть основные аутентичные международным стандарты, но нет правил, по которым ими можно пользоваться (не приняты и не введены системы оценки по этим стандартам, результаты оценок официально не признаются, сами оценки делаются по нормативным документам Банка России, ФСБ и ФСТЭК). При этом все банки, параллельно с реализацией отечественных требований по безопасности, проводят оценки по стандартам PSI DCC, отчитываются по ним перед уважаемой международной организацией PSI Council со штаб-квартирой в г. Нью-Йорке.

По факту в стране действуют две как бы не замечающих друг друга системы регулирования в банковской сфере. Список можно продолжить и расширить.

4. Анализируя эффективность функционирования Государственной системы лицензирования, аттестации и сертификации, следует отметить, что огромными усилиями регуляторов в лице ФСБ и ФСТЭК несомненно достигнут положительный резуль-



тат, что позволило не потерять управление отраслью. Ну, а слабости системы известны и заслуживают отдельного анализа.

5. Что касается системы подготовки кадров, то формально вроде она действует, десятки, если не сотни вузов готовят специалистов по утверждённым образовательным программам и специальностям.

При ежегодном выпуске сотен дипломированных специалистов по информационной безопасности на рынке ощущается всё боль-



ший дефицит кадров. Специалистов, знающих современные продукты и имеющих практический опыт работы, становится всё меньше. Очевиден перекос в сторону формального знания, все готовы быть аудиторами и контролёрами, а на практике ощущается острый дефицит по техническим специальностям, не хватает программистов, инженеров, архитекторов, аналитиков, способных работать на рабочих местах операторов SOC и SIEM. Молодых специалистов приходится доучивать на рабочем месте, и при этом

практически сразу терять, потому что они, немного освоившись в жизни и профессии, находят работу с более высокими окладами и уходят. Небольшие и средние коммерческие фирмы не заинтересованы в таком исходе. Отсюда и дефицит. Что-то в этой системе не так.

А ТЕМ ВРЕМЕНЕМ...

Радикально выросла и изменилась за прошедшие годы компьютерная преступность. Соответственно состав и содержание угроз и рисков,



составляющий основу модели нарушителей и угроз, претерпели существенные изменения. В целом с начала 2000-х мы наблюдаем возникновение новых форм, общее развитие, консолидацию и взлёт уровня технической подготовки киберпреступности.

Изменяются источники угроз. В качестве таковых для систем бизнес-уровня нам теперь приходится рассматривать не только криминальную среду, многократно нарастившую силу и квалификацию за счёт похищенных средств, но и соответствующие правительственные структуры ведущих государств, а это совершенно иная квалификация и возможности.

Приобрёл особую актуальность фактор «инсайдера», доля которого, по некоторым источникам, доходит уже чуть не до 90 % в общем объёме киберпреступлений.

Да и сами информационные системы усложнились настолько, что уследить за их настрой-

ками и администрированием становится всё более сложно. Это привело к созданию новой идеологии управления безопасностью — с использованием SOC и SIEM. Субъекты защиты тратят значительные средства на их приобретение и внедрение с учётом дефицита специалистов. Однако пока незаметно, что стало легче.

ПО-ПРЕЖНЕМУ...

По-прежнему вопрос практической реализации требований безопасности и выполнения норм ФЗ находятся под вопросом. Рекомендательные механизмы действуют плохо, механизмы принуждения к исполнению требований толком не работают. Ответственность за некачественное исполнение требований по безопасности должным образом не определена.

Механизмы ответственности за искажение или сокрытие информации об инцидентах не установлены. А их много, достаточно вспомнить о частых отказах платёжных сервисов наших крупнейших банков.

КАК ОЦЕНИВАТЬ?

Задаюсь ещё одним вопросом. Эффективность работы системы должна быть оценена. А каковы критерии оценки состояния информационной безопасности? Что используется в качестве показателей, метрик и индикаторов эффективности? Какова методика измерений и расчёта? Насколько она публична и доступна обществу. Вопрос не простой.

Паспортом национальной программы «Цифровая экономика Российской Федерации» установлен единственный целевой показатель эффективности системы информационной безопасности: средний срок простоя ГИС в результате компьютерных атак (раздел 2, п. 2.5).

Но по этому частному показателю невозможно оценить уровень информационной безопасности в целом. Очевиден перекоп в приоритетах, о чём уже было сказано. Не оценивается ни объём преступных действий, ни хищений денежных средств у граждан, ни потери и хищения информации, в том числе ПД, ни простои платёжных систем, негативно влияющие на деловую активность того самого малого бизнеса, ни соответствие негосударственных систем требованиям по безопасности.

Не заданы и не описаны ни соответствующие индикаторы, ни критерии. Таким образом, оценить уровень информационной безопасности ни в общем, ни в частном случае невозможно.

А как же тогда квалифицировать крупнейший прокол системы защиты в последние не-

сколько лет — поголовное хищение баз данных из банков и операторов сотовой связи? Ведь похищенные базы данных, содержащие весьма значительные объёмы сведений о нас (персональные данные, кстати) стали источником ценной и точной информации для мошенников, в массовом порядке начавших обманывать граждан и совершать хищения денежных средств у них и юридических лиц с применением методов социальной инженерии. Рост объёма хищений составил за 2 года свыше 30%. А до этого были АРТ-атаки. А до этого вирусы. А до этого хакеры. И т.д.

Пока дела у нас в целом выглядят довольно неплохо и обращать внимание на истерики в стиле «Шеф, всё пропало» не нужно и вредно, система защиты борется, но постепенно ситуация становится более тревожной.

Вывод

Вывод напрашивается сам собой.

Времена изменились, назрела проблема системного порядка, её нужно решать. Киберпреступность — вещь гибкая, подвижная и агрессивная.

Мировое окружение тоже не сахар. Почти у всех окружающих нас стран есть и действуют кибервойска.

Новые информационные технологии меняют подходы к работе и изменяют сознание и психологию людей.

Противостояние этим угрозам — задача сложная и требует адекватной модификации системы защиты. А лучше — работа на опережение. Иначе нельзя.

На классический вопрос «Что делать?» постараемся ответить в следующей статье.

BIS-КОММЕНТАРИЙ

«ВЕРХИ НЕ МОГУТ, А НИЗЫ НЕ ХОТЯТ»

Андрей Петрович во многом прав в своём историческом экскурсе, посвящённом становлению отрасли информационной безопасности в России. Однако, учитывая его прошлое место службы и работы, он всё-таки видит это становление немного не так, как оно видится мне, человеку, который никогда не работал внутри регулятора.

Я начинал свою карьеру в области ИБ в московском «ящике», работавшем на оборонку, потом были госкорпорация и крупный банк, затем разработчик средств защиты информации и т.п. И могу сказать, что мы оказались в нашем текущем не самом лучшем положении во многом благодаря нашим регуляторам, которые как страусы засовывали голову в песок на протяжении двух десятков лет и не предпринимали никаких действий по развитию отрасли ИБ.

Все благие начинания, а они были и в Гостехкомиссии России, и в других организациях, которые могли изменить и ситуацию с кадрами, и ситуацию с законодательством, и ситуацию с рынком средств защиты, гнобились на корню, что и привело в итоге к тому, что все начинания регуляторов сегодня воспринимаются в штыки. Самого регулятора (это касается и ФСТЭК, и

ФСБ, и ЦБ, и РКН, и др.) рассматривают как ничего не понимающего в современных технологиях «старпёра», а большинство российских игроков рынка ИБ выглядят как «прихвостники» регуляторов, занимающихся получением бумажек, а не удовлетворением реальных потребностей рынка. А тут ещё и Крым, внезапно возжелавший вернуться в объятия России, и последовавшие за ним санкции, которые поставили отрасль ИТ и ИБ на грань выживания.

Мы потеряли очень много времени на следование в кильватере у регуляторов, которые продемонстрировали, что они не способны оперативно реагировать на возникающие вызовы, но и отпускать вожжи регулирования тоже не готовы. В итоге мы пришли к ситуации, которая сложилась в Российской империи более ста лет назад — «верхи не могут, а низы не хотят». И мы помним, к чему эта ситуация привела. Поэтому изучение истории — дело, безусловно, полезное, но уроки истории надо не только изучать, но и делать выводы, которые наши регуляторы почему-то делать не хотят!



**Алексей
ЛУКАЦКИЙ**
эксперт
BIS Journal



Карл СУММАНЕН
эксперт BIS Journal

BIS-КОММЕНТАРИЙ

«ГЛАВНАЯ ПРОБЛЕМА — ОТСУТСТВИЕ В СТРАНЕ ЕДИНОГО ИНСТИТУТА, ОТВЕТСТВЕННОГО ЗА РАЗВИТИЕ СИСТЕМЫ ИБ В ЦЕЛОМ»

Статья представляет развёрнутый анализ истории формирования, текущего состояния, проблем и перспектив развития системы информационной безопасности (ИБ) России. Материал тем более интересный, что его автором является один из наиболее авторитетных специалистов в этой области, внёсший большой личный вклад в формирование существующей сегодня системы ИБ. Основной вывод автора, тем не менее, — развитие системы ИБ в России сейчас сопровождается целым рядом проблем.

Важность вопросов, поднятых в статье, обусловлена тем, что, хотя автор прямо об этом не говорит, в случае цифровой экономики, тотально зависящей от информационных систем, неэффективность ИБ может приводить к нарушению или полной остановке критичных экономических процессов, вплоть до разрушения экономики, что превращает ИБ в геополитический фактор, влияющий на жизнеспособность страны.

Существенно также, что вопросы, поднятые в статье, отражают озабоченность профессионала, видящего фундаментальные проблемы и связанные с этим фундаментальные риски. Уже только поэтому статья заслуживает серьёзного внимания не только узких специалистов в ИБ, но и руководителей всех уровней, в зону ответ-

ственности которых прямо или косвенно входят вопросы управления развитием национальной стратегии ИБ.

С заключением автора о наличии проблем нельзя не согласиться. Все перечисленные в статье проблемы действительно есть и требуют решения, однако, на наш взгляд, важно, следуя известной максиме «зри в корень», выделить первичную проблему, без опережающего решения которой невозможно устранить порождённые ей более частные проблемы. Представляется, что таковой является несовершенство организации процесса развития ИБ, а более конкретно — отсутствие в стране единого института, ответственного за развитие системы ИБ в целом.

Сегодня развитие системы ИБ в России происходит на основе «ведомственной» модели управления, когда комплексная сложная задача раздроблена на несколько частных подзадач, каждой из которых по отдельности и в значительной степени независимо занимается отдельное ведомство, действуя соответственно своим корпоративным целям и интересам.

Как следствие, в России сегодня отсутствует единый мозговой центр стратегического анализа в области ИБ, наделённый необходимыми полномочиями и обеспеченный ресурсами, способный компетентно сформулировать долгосрочные цели создания ИБ, определить оптимальную стратегию их достижения и обеспечить системный процесс комплексного проектирования и внедрения национальной системы ИБ.

Свято место пусто не бывает и в отсутствие системного процесса проектирования системы ИБ его место занимает какой-нибудь суррогатный. В нашей стране роль такого суррогатного

Все перечисленные в статье проблемы действительно есть и требуют решения, однако, на наш взгляд, важно, следуя известной максиме «зри в корень», выделить первичную проблему

процесса играет законодательный. Нельзя сказать, что управление ИБ через законодательство не даёт вообще никаких результатов, вопрос в их качестве. Проблема в том, что при таком подходе конечные содержательные решения в сложной предметной области уполномочены принимать непрофессионалы, а специалисты широкого профиля, представленные в соответствующем законодательном институте, тогда как при правильной организации управления развитием ИБ законодательный процесс должен был бы лишь обеспечивать нормативно-правовое оформление профессиональных решений, принятых профильными специалистами.

Заслуживает внимания также тезис автора о важности опережающих исследований и необходимости «настойчиво формулировать будущее в благоприятном для нас направлении». Подчеркнём, что опережающее проактивное проектирование целевой архитектуры системы ИБ важно в первую очередь с геополитической точки зрения.

Особенность ситуации сегодня в том, что экономика России, также как и экономики других стран и глобальная экономика в целом, сейчас находится в переходном состоянии. Происходит переход из «доцифровой» экономики в цифровую и связанная с этим смена экономической модели, сопровождаемая скачкообразным изменением структуры экономики и перестройкой всех составляющих её компонент, включая систему ИБ.

Перестройка, как и любое кризисное явление, открывает окно возможностей и даёт шанс сконструировать новую экономическую модель и новую систему ИБ в предпочтительном для нас виде. Но ровно такая же возможность открывается и для наших геополитических соседей-противников. В этой игре на опережение выиграет тот, кто сможет лучше воспользоваться новыми возможностями. Можно не сомневаться, что наши соседи постараются реализовать их по-максимуму и в своих интересах. Как показывает вся предыдущая история, до сих пор они это делали очень эффективно, и здесь нам есть чему у них поучиться.

Поэтому, если мы хотим на выходе из переходного периода получить нужную нам национальную систему ИБ, надо действовать оперативно, проактивно, эффективно и целенаправленно, т.е. имея продуманное долгосрочное целеполагание и стратегию. Но именно с целеполаганием и стратегией у нас и возникают проблемы в силу отмеченного выше отсутствия у задачи создания системы ИБ единого хозяина.

Принципиальное отличие процессов формирования системы ИБ в 90-е и последующие годы от процессов, происходящих сегодня, в том, что в 90-е годы перестройки как таковой не было

В своём анализе автор ссылается на классический подход к прогнозированию, основанный на экстраполяции прошлых событий и опыта в будущее. Такой подход, действительно, может успешно применяться во многих ситуациях, но в рассматриваемом случае развития системы ИБ, его применимость, на наш взгляд, вызывает вопросы, поскольку экстраполяция возможна только, если система, поведение которой описывается, находится на стационарной траектории. В случае системы ИБ это условие сегодня не выполняется.

Принципиальное отличие процессов формирования системы ИБ в 90-е и последующие годы от процессов, происходящих сегодня, в том, что в 90-е годы перестройки как таковой не было. Происходило формирование системы ИБ в рамках существующей модели экономики (в основном сложившейся в первой половине 90-х) и можно было говорить о стационарной траектории. Сегодня же, как отмечалось выше, происходит смена экономической модели, при которой система претерпевает скачкообразную перестройку и переходит на новую траекторию. В этой ситуации говорить о движении по стационарной траектории нельзя, что ограничивает возможности применения метода экстраполяции.

В условиях переходного периода более эффективен метод «забегания вперёд» с попыткой стратегического долгосрочного целеполагания: проактивным конструированием возможных вариантов целевых моделей системы ИБ, выбором предпочтительной модели и разработкой стратегии её реализации.

* * *

Очевидно, что в рамках действующей «ведомственной» модели управления действующие разрозненно ведомства не могут решить сложную комплексную задачу проектирования долгосрочной целевой архитектуры национальной системы ИБ и разработки стратегии достижения сформулированных целей. Решение такой задачи под силу только уже упомянутому центру стратегического анализа в области ИБ.



Дмитрий СКОБЕЛКИН
заместитель председателя
Банка России

СТРАТЕГИЧЕСКИЕ ПРИОРИТЕТЫ

ОБ ИЗМЕНЕНИЯХ В «ОСНОВНЫХ НАПРАВЛЕНИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВОЙ СФЕРЫ НА 2019–2021 ГГ.»¹

Вопросы информационной безопасности и операционной надежности для Банка России является одним из стратегических приоритетов. Наши задачи в этом направлении детализированы в одобренных Советом Директоров Банка России «Основных направлениях развития информационной безопасности финансовой сферы на 2019–2021 гг.».

РИСКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

При подготовке этого документа мы исходили из очевидной необходимости минимизировать те риски, которые наряду с многочисленными преимуществами создает цифровая трансформация.

В кредитно-финансовой сфере к ним относятся:

- ♦ финансовые потери клиентов и финансовых организаций;
- ♦ нарушение операционной надежности и непрерывности работы финансовых организаций, и как следствие — репутационный ущерб и социальная напряженность;
- ♦ развитие системного кризиса вследствие кибератак в значимых для рынка организациях.

В этой связи стоит сказать о том, что повышает значимость информационной безопасности финансового рынка Российской Федерации.

Во-первых, это скорость развития новых финансовых технологий, в том числе, обусловленная активной поддержкой создания цифровой экосистемы руководством страны.

Во-вторых, необходимость защиты потребителей финансовых услуг от потерь и, как следствие, поддержания доверия к финансовой системе России.

В-третьих — задача по интеграции показателей киберрисков в состав основных рисков финансовых организаций.

С УЧЕТОМ ТРЕНДОВ

Развитие цифровой среды — это непрерывное появление и внедрение новых цифровых технологий. Это как многочисленные прорывные разработки финтех-стартапов, так и крупные инфраструктурные цифровые проекты. В отношении некоторых из них Банк России уже устанавливает требования по информационной безопасности. Это единая биометрическая система, система быстрых платежей и платформа Маркетплейс.

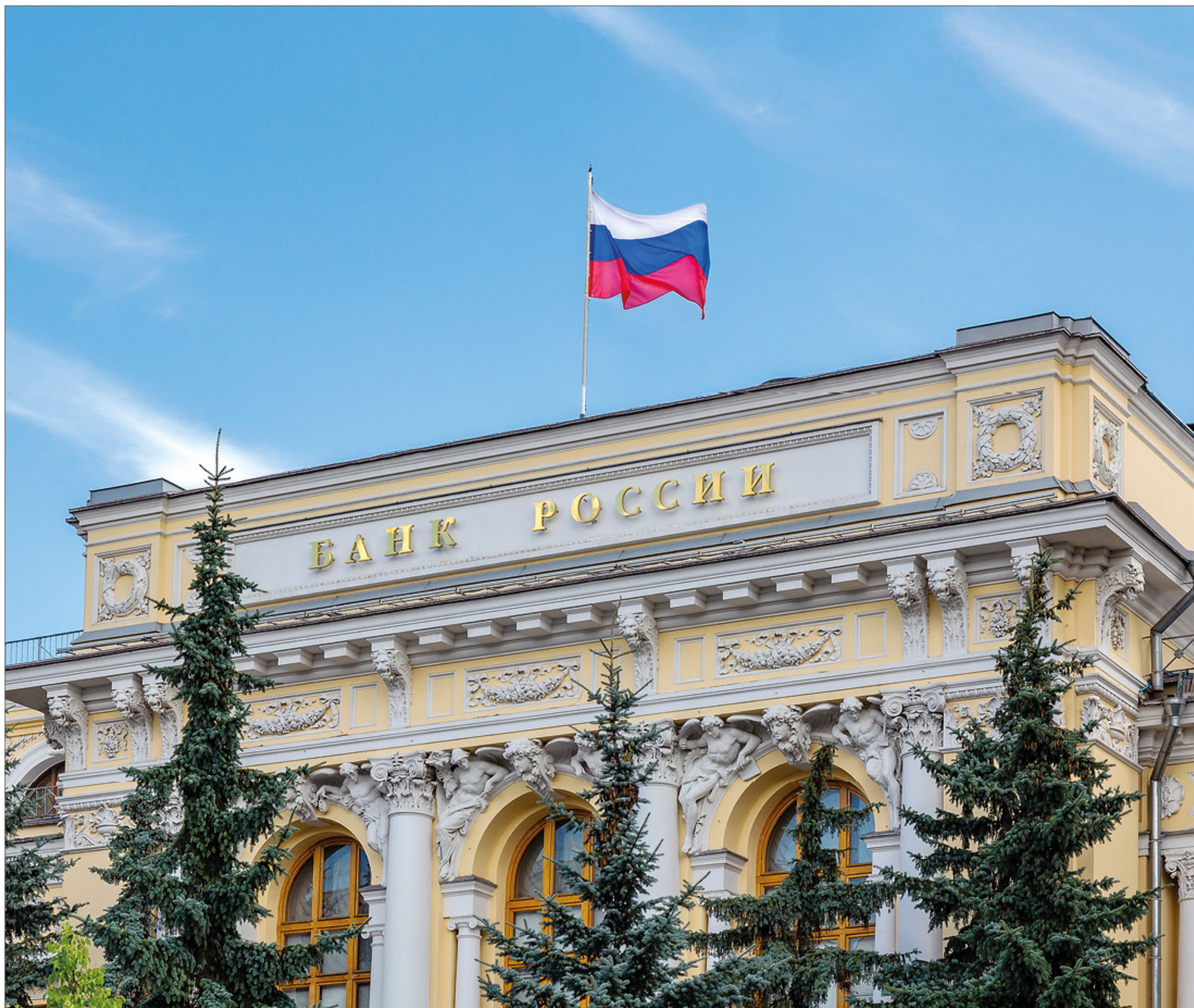
В будущем требования к киберустойчивости финансовой экосистемы мы будем формулировать с учетом глобальных трендов развития финтеха. В первую очередь, таких как использование технологий распределенного реестра, развитие удаленного доступа, Big Data, искусственного интеллекта и «Интернета вещей» как элемента платежного пространства.

ЗАДАЧИ СЕГОДНЯ

Однако это нам пока только предстоит. Вернемся в сегодняшний день, когда нашей приоритетной задачей является реализация информационной безопасности финансовых организаций на следующих уровнях:

- ♦ безопасность инфраструктуры, или инфраструктурный уровень;
- ♦ безопасность прикладного программного обеспечения, или уровень приложений;
- ♦ безопасность технологий обработки данных, или уровень технологий обработки данных;
- ♦ а также протоколирование действий и операций (транзакций).

¹ Публикация подготовлена по итогам выступления заместителя председателя Банка России Дмитрия Скобелкина на XII Уральском форуме.



НОРМАТИВНАЯ БАЗА

Практическую реализацию стратегии мы начали в прошлом году с разработки необходимой нормативной базы.

Мы исходили из того, что правовой механизм обеспечения информационной безопасности на финансовом рынке должен гарантировать предсказуемость реализации Банком России своих полномочий, предсказуемость надзора за исполнением требований участниками финансового рынка и в конечном итоге обеспечивать выполнение ключевого показателя эффективности обеспечения информационной безопасности в финансовой сфере. Напомню, им является доля объема операций без согласия клиентов в общем объеме операций, совершенных с использованием платежных карт, не превышающая 0,005 %.

Могу сказать, что Банк России провел беспрецедентную по своему масштабу работу по нормативному закреплению полномочий и механизмов противодействия информационным угрозам в кредитно-финансовой сфере.

Начиная с 2016 года сотрудники Банка России участвовали в разработке принятого в 2018 году Федерального закона от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» (далее — Федеральный закон № 167-ФЗ). В дальнейшем в дополнение к нему был издан ряд конкретизирующих и уточняющих нормативных актов. Указанные документы позволили:

- ♦ создать механизм противодействия переводам денежных средств без согласия клиента, предусматривающий как обязательные требования к защите информации, формируемой кредитными организациями, так и процедуры управления рисками, разрабатываемые кредитными организациями на основе анализа характера, параметров и объема совершаемых их клиентами операций (осуществляемой клиентами деятельности);
- ♦ организовать информационное взаимодействие кредитных организаций с Банком России по обмену информацией

об инцидентах защиты информации, о случаях и попытках осуществления переводов денежных средств без согласия клиента, включая формирование и ведение Банком России базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента;

♦ обеспечить реализацию кредитными организациями в целях противодействия осуществлению переводов денежных средств без согласия клиента в рамках осуществляемой ими банковской деятельности, некредитными финансовыми организациями в целях противодействия незаконным финансовым операциям в рамках осуществляемой ими деятельности в сфере финансовых рынков уровня защиты информации, соответствующего потенциальным угрозам безопасности с учетом пропорционального метода регулирования.

Помимо этого, Банком России в течение 2016–2018 гг. были изданы следующие нормативные акты:

♦ Указание № 4793-У², устанавливающее требования к прикладному программному обеспечению (в части сертификации, анализа уязвимостей, ежегодного тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, применения отдельных технологий), к обеспечению защиты информации с помощью средств криптографической защиты информации, к порядку информирования Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств;

♦ Указание № 4753-У³, которое устанавливает обязанность операторов по переводу денежных средств и операторов услуг платежной инфраструктуры по предоставлению в Банк России отчетности по форме 0403203 «Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств» (далее — отчетность по форме 0403203) на ежеквартальной и полугодовой⁴ основе.

АСОИ

В целях противодействия осуществлению денежных переводов без согласия клиентов кредитных организаций, противодействия осуществлению незаконных финансовых операций Банк России ведет сбор и обработку поступающей от кредит-

ных и некредитных финансовых организаций информации о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, а также о планируемых мероприятиях в отношении инцидентов защиты информации.

Информацию об угрозах информационной безопасности Банк России получает как от поднадзорных финансовых организаций, так и от компаний-интеграторов, разработчиков антивирусного программного обеспечения, иностранных финансовых организаций и регуляторов, групп реагирования на инциденты (в том числе иностранных), провайдеров и операторов связи, а также правоохранительных, иных государственных органов, наделенных полномочиями в области информационной безопасности.

Для упрощения процесса информационного обмена, а также повышения оперативности и уровня его защищенности используется автоматизированная система обработки инцидентов (далее — АСОИ), к которой в настоящий момент подключены все кредитные организации Российской Федерации. Также осуществляется подключение страховых организаций и иных участников информационного обмена. Всего к АСОИ подключено 826 организаций. Число участников информационного обмена из категории «некредитные финансовые организации» (НФО) по сравнению с периодом 2017–2018 гг. увеличилось более чем на 100 организаций. Также участниками информационного обмена стали более 20 вендоров защитных решений, разработчиков банковского программного обеспечения, операторов связи, провайдеров хостинга и иных заинтересованных организаций.

Взаимодействие с вышеуказанными организациями осуществляется на безвозмездной основе в соответствии с соглашениями о взаимодействии по вопросу предупреждения и противодействия компьютерным атакам (в 2018 г. заключено 21 такое соглашение). За период с сентября 2018 года по настоящее время количество активных участников информационного обмена, регулярно передающих информацию о выявленных угрозах и уязвимостях, увеличилось на 48% (с 315 до 465). Данное обстоятельство связано в том числе с активной реализацией участниками информационного обмена стандарта Банка России СТО БР БФБО-1.5–2018.

Функционал АСОИ позволяет автоматизировать следующие процессы между участниками информационного обмена и Банком России:

♦ получение данных от участника (информация об инцидентах в организации, выявленных уязвимостях, угрозах, данных о раскрытии информации, запросах);

♦ передача участнику данных об актуальных угрозах информационной безопасности в кредитно-финансовой сфере (в том числе из 589 выпущенных Банком России бюллетеней);

♦ оперативное взаимодействие между участником и Банком России по инцидентам и запросам;

♦ мониторинг информационных атак на организации кредитно-финансовой сферы и поддержка взаимодействия Банка России с регистраторами и хостерами по инициации разделения/блокировки мошеннических и вредоносных ресурсов.

² Указание Банка России от 07.05.2018 № 4793-У «О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

³ Указание Банка России от 30.03.2018 № 4753-У «О внесении изменений в Указание Банка России от 9 июня 2012 года № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств».

⁴ Для операторов по переводу денежных средств (операторов по переводу электронных денежных средств), являющихся небанковскими кредитными организациями, имеющих право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций, у которых средний за полгода объем обязательств перед клиентами по переводу денежных средств без открытия банковских счетов в течение месяца не превышает 2 млрд рублей.



Выступление Д.Г. Скобелкина на XII Уральском форуме

КПЭ

Доля объема операций без согласия клиентов в общем объеме операций, совершенных с использованием платежных карт, в 2019 г. составила 0,0023 % (в 2018 г. — 0,0018 %). Указанные значения не превышают установленный Банком России целевой показатель доли таких операций в общем объеме операций, совершенных с использованием платежных карт. Повторюсь, этот показатель установлен на уровне 0,005 %.

Наблюдаемое в отчетном периоде изменение нисходящей динамики 2015–2017 гг., а также качественно более высокие показатели операционной отчетности указывают на имевшую место реальную необходимость повышения прозрачности предоставляемых банками данных и подтверждают правильность разработки и внедрения мер по минимизации риска осуществления операций без согласия клиентов, принимаемых участниками рынка и Банком России, а также необходимость их дальнейшего развития.

ПРОВЕРКИ

Мы считаем, что основой эффективной деятельности в сфере обеспечения информационной безопасности является применение подхода, основанного на оценке кибер-риска, или, другими словами, риск-ориентированный подход. Банк России планируют сформировать профиль риска, а также опре-

делять операционную надежность и киберустойчивость каждой поднадзорной организации на основе данных, которые мы получаем в ходе анализа поступающей отчетности, сообщений участников информационного обмена об инцидентах, а также проверок соблюдения требований по информационной безопасности. В 2019 году мы провели порядка 170 таких проверок как в кредитных организациях, так и в некредитных финансовых организациях.

КИБЕРУЧЕНИЯ

По направлению киберучений осуществляются следующие мероприятия:

1. Формирование риск-ориентированного задания на киберучения на основе:

- ♦ информации об инцидентах, характерных для вида деятельности;
- ♦ информации об инцидентах, характерных для технологических участков;
- ♦ информации о проведенных ранее проверках/киберучениях в поднадзорной организации;
- ♦ информации об актуальных атаках.

2. Проведение киберучений на площадке поднадзорной организации:

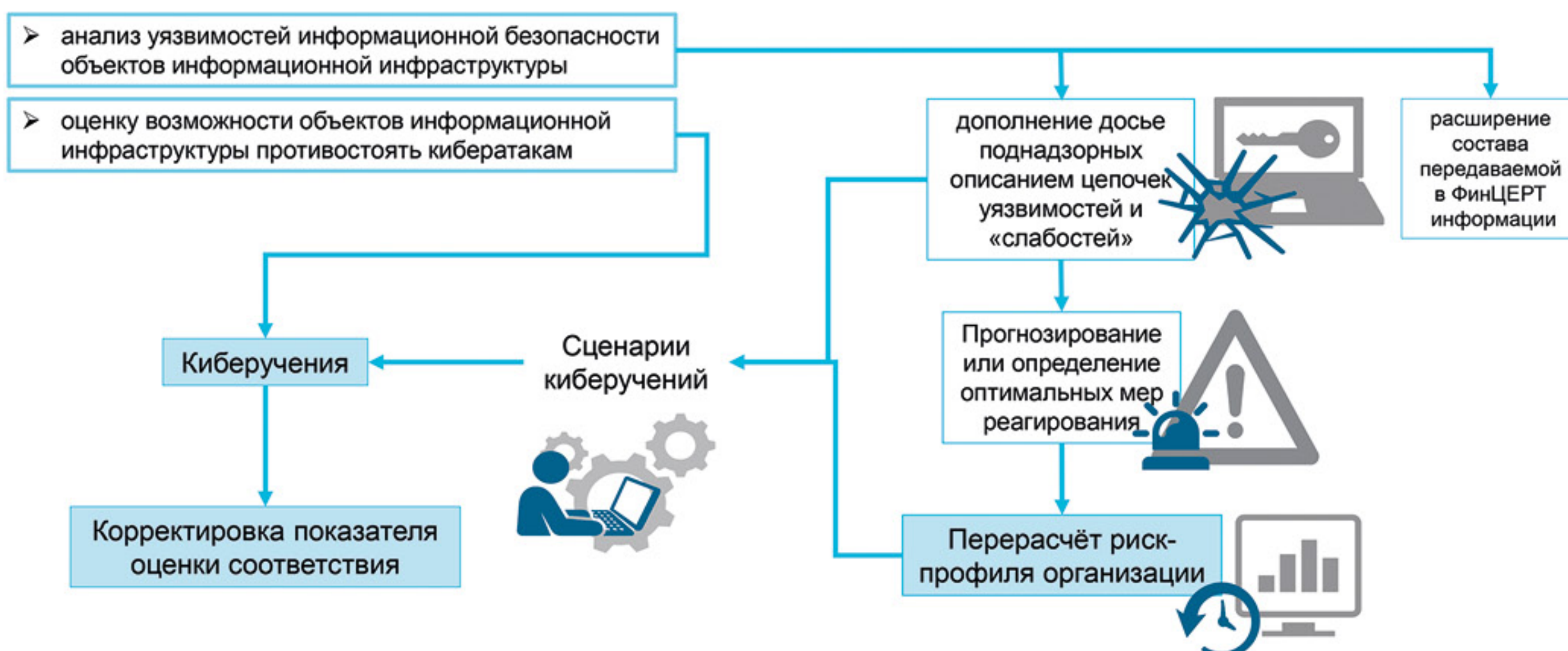
- ♦ анализ инфраструктуры, актуализация СРЕ;
- ♦ определение актуальных слабостей (CWE);



Банк России

Реализация стратегии: риск-ориентированный подход

В рамках риск-ориентированного подхода финансовые организации должны выполнять:



- ♦ определение актуальных атак (CAPEC);
- ♦ определение актуальных инцидентов;
- ♦ определение максимально возможных финансовых потерь.

3. Подготовка отчетного документа по результатам киберучений:

- ♦ корректировка показателя оценки соответствия;
- ♦ определение и применение мер воздействия⁵;
- ♦ направление в профильные департаменты информации для учета показателей информационной безопасности при применении мер воздействия.

Организацией и проведением киберучений в рамках надзорных мероприятий занимается Департамент информационной безопасности Банка России.

УПРАВЛЕНИЕ КИБЕРРИСКАМИ

В рамках управления киберрисками задачами каждой финансовой организации в первую очередь будут являться:

- ♦ обеспечение соответствия фактических потерь в результате инцидентов защиты информации допустимым потерям;
- ♦ формирование финансового резерва на покрытие потенциальных финансовых потерь либо страхования такого риска;
- ♦ своевременное восстановление непрерывности технологических и бизнес-процессов;
- ♦ и в целом защита интересов клиентов и соблюдение требований законодательства Российской Федерации в области защиты информации.

⁵ В случае отрицательных результатов проверки

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Анализ, проведенный Банком России, показывает, что в 2019 году значительная часть хищений со счетов физических и юридических лиц была совершена с использованием приемов социальной инженерии, введением в заблуждение путем обмана или злоупотребления доверием. Мы можем сколь угодно устранять пробелы в периметрах защиты кредитных организаций, но до тех пор, пока люди сами будут сообщать мошеннику свои кодовые слова, иные платежные данные, хищения будут продолжаться.

Единственным способом борьбы с социальной инженерией мы считаем информационные кампании при содействии федеральных и региональных СМИ, а также социальных медиа. Главное — предупредить наших граждан о схемах обмана, телефонном мошенничестве, а также дать рекомендации по противодействию им.

Сегодня все территориальные подразделения Банка России проводят публичные мероприятия по безопасности, по безопасному использованию платежных инструментов и банковских услуг для разных целевых аудиторий.

Кроме работы по киберграмотности Банк России видит необходимость и в законодательных изменениях. В настоящее время в Государственной думе готовятся ко второму чтению два на наш взгляд важнейших законопроекта, которые существенно усложнят жизнь злоумышленникам. Первый — это законопроект о блокировке в интернете фишинговых ресурсов и ресурсов, распространяющих вредоносное программное обеспечение. Конечно, это не панацея от всех бед, но это не даст возможность злоумышленникам заманивать в свои сети простых граждан.

Второй — это закон об информационном обмене банков с операторами связи. Такой информационный обмен не даст развиваться такому способу мошенничества, как замена без ведома самого пользователя телефонного номера его сим-карты. Мы понимаем, что постепенно номер телефона пользователя финансовых услуг становится его полноценным идентификатором, особенно часто используемым в динамично развивающемся финтех-направлении. Поэтому важно обеспечить превентивную защиту, а не ждать, когда проблема будет нарастать и только потом на нее реагировать.

Мы уверены, что оба законопроекта будут скоро приняты.

УТЕЧКА ДАННЫХ

Отдельно хотел бы остановиться на проблеме утечки данных. Всем понятны громкие сообщения в прессе о продаже и утечке баз данных, содержащих персональные данные граждан. К сожалению, такие утечки случались и из финансовых организаций. Безусловно, без реакции такое оставить нельзя. Обязанность любой финансовой организации — защищать свои активы, а самым главным активом являются данные ее клиентов. Поэтому Банк России в ходе своей инспекционной деятельности будет обращать самое серьезное внимание на вопросы контроля информационных потоков в финансовых организациях, обеспечение безопасности данных.

Но только надзорными методами проблему решить невозможно. Мы полагаем, что создать условия для упорядоченного доступа к персональным данным, которые содержатся в различных информационных системах, можно совместными усилиями Банка России, Минкомсвязи, Роскомнадзора. Необходимо упростить работу правоохранительным органам по противодействию тем субъектам, которые незаконно получают, продают и используют персональные данные. Соответствующие инициативы мы сейчас готовим и в ближайшее время направим в адрес наших коллег в Минсвязи и в Роскомнадзор.

Я думаю, назрел уже вопрос изменения законодательства, которое регулирует вопросы сохранности и использования персональных данных, и на сегодняшний день это, наверное, уже третье глобальное законодательное направление, с которым мы работаем.

МЕЖДУНАРОДНОЕ ВЗАИМОДЕЙСТВИЕ

Глобальные угрозы в сфере кибербезопасности носят трансграничный характер. Меняются устоявшиеся бизнес-модели, появляются новые вызовы для международных экономических отношений. Все это требует от государств совместных усилий. Мы считаем, что основными задачами здесь являются:

- ♦ обмен информацией о киберугрозах;
- ♦ содействие внедрению единых стандартизированных подходов в области обеспечения кибербезопасности;
- ♦ обмен опытом по регулированию и внедрению финансовых технологий.

В этой связи Банк России и впредь будет углублять, и расширять международное взаимодействие. Уже традиционными стали встречи на полях Уральского форума представителей пяти национальных банков государств-членов евразийского экономического союза. Сформирована рабочая группа по вопросам обеспечения информационной безопасности финансового рынка. Ее цель — создание единого киберпространства и доверенной среды в рамках ЕАЭС.

В этом году нашими гостями стали также представители Туркменистана и Узбекистана, с которыми мы обсуждаем возможность сотрудничества. Потенциальными партнерами для нас являются страны БРИКС. Мы рады встречам с представителями финансовых регуляторов Индии и Бразилии, а также коллегами из Японии, Индонезии, Вьетнама.

КАДРЫ

Информационная безопасность — это та сфера, где успеха можно достичь только совместными усилиями регулятора, экспертного сообщества и, безусловно, участников рынка. Одним из важнейших направлений в нашей общей работе является подготовка кадров. Здесь Банк России видит свою роль в качестве связующего звена между высшими учебными заведениями и организациями кредитно-финансовой сферы. Наша задача — создать условия для подготовки специалистов в области информационной безопасности, которые действительно нужны рынку.



Участники международной программы XII Уральского форума



Вадим УВАРОВ
директор Департамента
информационной
безопасности Банка России

«ЕСЛИ КТО-ТО КОЕ-ГДЕ У НАС ПОРОЙ...»

ВЗАИМОДЕЙСТВИЕ ОРГАНИЗАЦИЙ ФИНАНСОВОЙ СФЕРЫ И ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ¹

На XII Уральском форуме особенный интерес вызвала сессия под названием «Если кто-то кое-где у нас порой...». Она была посвящена взаимодействию организаций финансовой сферы и правоохранительных органов. Предлагаем в сокращенном варианте самые важные, на наш взгляд, выступления, прозвучавшие в ходе этого обсуждения.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ТРЕНДЕ

По итогам 2019 г. выявлена тенденция — растет количество преступлений, связанных с мошенничеством в отношении физических лиц. Увеличиваются и число, и объемы несанкционированных операций. Нередко владельцев средств побуждают самостоятельно совершить перевод в пользу мошенников путем обмана или злоупотребления доверием. Всё это — методы так называемой «социальной инженерии».

В основе таких преступлений лежит утечка персональных данных физических лиц, а также отсутствие у граждан понимания как правильно хранить свои данные в эпоху высоких технологий.

Основная схема в арсенале преступников — мошенничество с использованием мобильных телефонов. Злоумышленники звонят гражданам под видом представителей служб безопасности банков. С помощью всевозможных ухищрений

они выманивают у пользователей онлайн-ресурсов данные о банковской карте и паролях с целью дальнейшего доступа в личный кабинет и хищения денежных средств.

В 2019 г. были выявлены и случаи хищения денежных средств с использованием вредоносного программного обеспечения. Таким образом, утечка персональных данных, низкая финансовая и киберграмотность населения, слабая уголовно-процессуальная база и практика привлечения к ответственности за киберпреступления в комплексе приводят к тому уровню активности преступников, который мы имеем.

Как выглядит реальная картина?

РЕАЛЬНАЯ КАРТИНА

В 2018 и 2019 гг. ФинЦЕРТ Департамента информационной безопасности Банка России осуществлял блокировку выявленных фишинговых ресурсов и ресурсов с вредоносным программным обеспечением. В 2019 г. по сравнению с 2018 г. количество заблокированных ресурсов увеличилось в пять раз и составило более 12 тыс. (из них 1107 ресурсов, распространяющих вредоносное программное обеспечение). Также в части взаимодействия с операторами связи выявлено более 13 тыс. номеров мобильных операторов и номеров в коде 8–800, действовавших в мошеннических звонках и SMS-рассылках. По сравнению с 2018 г. инцидентов с использованием телефонных методов социальной инженерии стало больше в 29 раз.

Можно выделить несколько типов мобильного мошенничества на основе имеющейся у нас статистики:

- ♦ 47 % случаев — мошенники используют методы социальной инженерии для получения доступа к личному кабинету жертвы на сайте банка;
- ♦ 34 % случаев — собственноручно переведенные денежные средства пользователями на счета злоумышленников;

¹ Публикация подготовлена по материалам сессии «Если кто-то кое-где у нас порой...» XII Уральского форума

По итогам 2019 г. выявлена тенденция — растет количество преступлений, связанных с мошенничеством в отношении физических лиц. Увеличиваются и число, и объемы несанкционированных операций



Взаимодействие Банка России с правоохранительными органами

♦ 13% — кражи карточных данных при онлайн покупках в интернете;

♦ 6% — sms-сообщения с фишинговыми рассылками от лжебанков и пр., в результате которой мошенники получают информацию для совершения своих преступлений. За прошедший период было заблокировано 370 массовых фишинговых sms-рассылок.

ВЗАИМОДЕЙСТВИЕ

Департамент информационной безопасности Банка России взаимодействует по этим вопросам с МВД России, Следственным комитетом, Федеральной службой безопасности, Генеральной прокуратурой и подразделением Интерпола в России.

За прошедший год в рамках взаимодействия с ГосСОПКА было выявлено и направлено 558857 доменных имен, задействованных в осуществлении фишинговой деятельности и распространения вредоносного программного обеспечения. Так как взаимодействие у нас осуществляется в обе стороны, от ГосСОПКА мы получили порядка 60 сообщений о выявленных угрозах.

В Генеральную прокуратуру направлено 250 доменов с целью ограничения доступа на территории РФ.

В ФинЦЕРТ существует техническая лаборатория. В 2019 г. специалисты Департамента по запросам правоохранительных органов провели 21 исследование носителей информации, подвергшихся воздействию вредоносного программного обеспечения при совершении хищений. Было осуществлено пять исследований мобильных устройств, скиммеров и иных технических устройств, а также осуществлено пять выездов по запросам поднадзорных организаций и их клиентов для своевременного реагирования на инцидент.

КАК ДЕЙСТВУЕТ ФИНЦЕРТ

Что делает ФинЦЕРТ при хищении денежных средств? Прежде всего, мы организуем взаимодействие с кредитными организациями — получателями денежных средств, занимаемся организацией взаимодействия с правоохранительными органами по вопросам оперативно-розыскной деятельности, а также оказываем иную помощь, направленную на содействие в блокировке похищенных денежных средств. В 2019 г. нами оказано содействие в расследовании хищений денежных средств более чем по 180 эпизодам.

Хищение денежных средств и среднее время, которое преступники тратят на эту деятельность, — всего один-два часа. К сожалению, многие поднадзорные обращаются к нам, когда время уже упущено, в результате мы не можем реагировать на совершение факта преступления в самом начале атаки.

НОВАЯ УГРОЗА

Сегодня развивается еще один инструмент, который используют злоумышленники с целью хищения денежных средств у граждан. Это финансовые пирамиды нового типа. Все больше инвестиций в сомнительные проекты привлекается через интернет, используются социальные сети, небольшие иностранные платежные системы и реклама с лозунгами «Хватит работать на дядю — пора зарабатывать». Такой подход привлекает в проекты молодежь и людей с низким уровнем финансовой грамотности. А с приходом криптовалюты классические пирамиды переросли в криптоинвестиционные проекты, которые обещают баснословный заработок. С этим мы также боремся во взаимодействии с правоохранительными органами.

Валерий ЛЯХ
Банк России

НАСТУПЛЕНИЕ НА ФИНАНСОВЫЕ ПИРАМИДЫ

С конца 2017 года Банк России выявляет нелегальных участников финансового рынка с использованием региональной модели. В главных управлениях Банка России по всей стране были образованы специальные отделы, которые должны заниматься выявлением такой деятельности. Созданы два центра компетенции — в Хабаровске и Краснодаре. Один — по выявлению финансовых пирамид, и второй — по выявлению участников нелегальной финансовой деятельности.

За 2019 год Банком России было выявлено 237 финансовых пирамид и организаций, имеющих признаки финансо-

вых пирамид. Статистический рост по сравнению с 2017–2018 гг. связан с более эффективной системой выявления. Проактивная модель выявления пирамид позволила также отследить еще около 80 организаций, которые могли бы ими стать, но не успели — их деятельность прекращена.

Большинство финансовых пирамид работают и рекламируют деятельность через интернет. Срок жизни современной пирамиды — 3–5 месяцев. За это время они стремятся быстро собрать деньги с граждан, чтобы те не успели «выскочить». Как только люди начинают приходить за «инвестициями», пирамида исчезает: компания закрывается.

Филипп НЕМОВ
Главное управление уголовного
розыска МВД России

«ВОЗНИКАЕТ ОЧЕНЬ МНОГО ВОПРОСОВ...»

Сегодня мы имеем колоссальный рост социальной инженерии. Органами внутренних дел за 2019 г. зарегистрировано порядка 300 тыс. заявлений граждан, которые мы относим именно к преступлениям, связанным с IT-технологиями. В соответствии с уголовно-процессуальным законодательством при наличии признаков состава преступления по заявлению гражданина возбуждается уголовное дело. Соответственно возбуждено 300 тыс. уголовных дел. Но это вершина айсберга, часто люди не обращаются в правоохранительные органы. Поэтому реальная картина неизвестна.

Органами МВД выявлены более 44 тыс. лиц, причастных к совершению 65 238 преступлений в сфере IT-технологий. В том числе, 15 920 лиц, причастных к хищению денежных

средств со счетов граждан с использованием сети интернет и средств мобильной связи.

При похищении денег коммуникация преступника с потенциальной жертвой осуществляется посредством сотовых операторов или IT компаний, ip- и sip-телефонии. Каждое седьмое тяжкое и особо тяжкое преступление сейчас совершается с использованием IT-технологий.

Сложность раскрытия таких преступлений — анонимность. Нужен доступ по цепочке от лиц, совершающих преступление, до бенефициаров, получающих денежные средства. Есть сложность в проведении оперативно-технических мероприятий и в доказывании.

Схема преступления распадается на подставных лиц, «дропов», которые предоставляют свои персональные данные

BIS-КОММЕНТАРИЙ

Наиболее распространенные виды «бизнеса» с признаками нелегальной деятельности в 2019 году это:

- ♦ нелегальные кредиторы — компании, которые не входят в реестр Банка России по предоставлению услуг микрокредитования, микрофинансирования;
- ♦ нелегальные форекс-дилеры — еще один раскрученный проект по привлечению в «инвестиционную» деятельность;
- ♦ иная деятельность: это — участники «страхового рынка», нелегальной брокерской деятельности, всевозможные «инвесторы» в металлы, ценные бумаги и даже в экзотические проекты.

Банк России направил материалы в отношении выявленных нелегальных участников финансового рынка в правоохранительные органы, в ФНС и ФАС для принятия мер реагирования.

Нелегальный рынок имеют региональную специфику, и именно в регионах следует планомерно работать для предотвращения деятельности таких структур при взаимодействии с правоохранительными органами и с органами государственной власти на местах.

Банк России выявляет нелегальных участников рынка и взаимодействует с правоохранительными органами, чтобы способствовать неотвратимости наказания за нелегальную деятельность на финансовом рынке.

Нелегалы, помимо угроз для потребителя, создают угрозу и для легальных организаций. «Услуги» нелегалов стоят гораздо дешевле, что создаёт нездоровую конкуренцию и легальные участники рынка оказываются в проигрыше.

Организаторы современных финансовых пирамид не разрабатывают хитрые схемы финансовой деятельности, их нет как таковых. Эти люди освоили два направления деятельности: маркетинг и инжиниринг. Они умеют привлечь на сайт новых клиентов и грамотно управлять этим потоком, предлагая услуги. Сфера борьбы с финансовыми пирамидами и нелегалами — это высокоинтеллектуальная деятельность, направленная в том числе и на привлечение технологического инструментария для ее предотвращения.

* * *

Законопроект о прекращении деятельности фишинговых сайтов и финансовых пирамид внесен в Госдуму и должен быть рассмотрен в ближайшее время. Надеюсь, что этот закон в случае принятия поможет быстро прекращать деятельность сайтов и финансовых пирамид, не допускать разрастания таких организаций в масштабные проекты.

BIS-КОММЕНТАРИЙ

для получения карточек, куда зачисляются денежные средства. Зачастую их используют втемную. И только глобальной разработкой мы можем доказать наличие преступного сообщества, созданного с целью хищения денежных средств у граждан.

Расследование преступлений в сфере IT — это фактически движения по цифровому следу. Для этого необходимо получение судебных санкций на проведение тех или иных мероприятий. Начиная от получения данных о движении по счету, заканчивая различными техническими средствами. В данный момент это сложно организовать и согласовать.

Общая сумма хищений у физических лиц — незначительна для банковского сектора. Однако для простого гражданина это, как правило, все накопления, деньги, на которые он рассчитывает в повседневной жизни. И пострадавший справедливо требует возмещения потерь. При том, что в договорах с банками прописано, что передача информации третьему лицу не является основанием для выплаты. И тут есть большая проблема.

Правоохранительные органы взаимодействуют со многими банками. Часть банков идет навстречу клиентам и в наиболее тяжелых жизненных ситуациях возмещают похи-

щенное. Но проблема остается и возникает вопрос о разработке механизмов полной идентификации клиента или иной идентификации лица, который непосредственно получает доступ к системам ДБО.

Мы готовы направить в Центральный Банк предложения и обсудить вопросы затруднения хищений средств со счетов граждан.

Возникает и кадровый вопрос: в кибербезопасности не так много специалистов, а для системы МВД — это новая тема. В 2019 г. прошла Коллегия МВД, посвященная преступлениям, совершаемым с использованием IT-технологий, было заявлено о создании в структуре Министерства подразделений, которые будут специализироваться на противодействии преступлениям, совершаемым с использованием IT-технологий. Для успешной работы необходим опыт и методы, которые уже накопили специалисты в сфере информационной безопасности банков, и успешное взаимодействие разных ведомств и организаций.

Дмитрий АНТОНОВ
Генеральная прокуратура РФ

BIS-КОММЕНТАРИЙ

«КИБЕРПРЕСТУПЛЕНИЯ — НОВАЯ ТЕМА...»

Тема киберпреступлений — новая для органов МВД и прокуратуры. Есть, к сожалению, и проблемы взаимодействия граждан с правоохранительными органами, отсюда и частое нежелание возбуждать уголовные дела по фактам мошенничества и доводить их до суда.

В рамках надзорных полномочий Прокуратура на постоянной основе проводит работу с такими преступлениями, как кибермошенничество. В 2019 г. было зарегистрировано 300 тыс. таких преступлений. Это на 68 % больше, чем в 2018 г. В два раза выросло количество преступлений, связанных с использованием кредитных карт. Рост наблюдается во всех регионах нашей страны, треть таких преступлений совершается в Москве, Санкт-Петербурге, Татарстане и Калининграде.

Для помощи гражданам планируется создание специализированного ресурса по приему сообщений об инцидентах, связанных с кибермошенничеством. Его концепция разработана, однако сам вопрос пока законодательно не урегулирован, и обсуждать его преждевременно.

Есть и другой вопрос. Сегодня все правоохранительные ведомства используют собственные системы регистрации правонарушений. Мы хотим, чтобы использовалась единая система. Поэтому для повышения прозрачности регистрации правонарушений Генеральной прокуратурой РФ разрабатывается Государственная автоматизированная система правовой статистики, которую мы планируем ввести в промышленную эксплуатацию в 2022 г.

Алексей ВОЙЛУКОВ
Ассоциация банков России

BIS-КОММЕНТАРИЙ

«НЕОБХОДИМО ВЫРАБОТАТЬ МЕХАНИЗМЫ ВЗАИМОДЕЙСТВИЯ»

300 тысяч заявлений от граждан, зарегистрированных полицией, и чуть больше 180 совместных случаев расследования и помощи, оказанной Банком России правоохранительным органам! Это меньше одной десятой процента. Слабая уголовно-процессуальная и законодательная база, а главное — бюрократическая схема взаимодействия между ведомствами приводят к тому, что преступления не раскрываются, чем и пользуются мошенники.

Что делать, когда деньги гражданина ушли, когда у него тем или иным способом вывели пароли и коды по смс? Человек обращается в банк, пытается вернуть деньги. А его отправляют в правоохранительные органы, где нужно собрать и представить доказательства... Дальше суд. Все это растягивается на 1–2 года. А вывод средств происходит за 1–2 часа!

Что нужно сделать для отладки взаимодействия? Наладить двусторонние взаимоотношения между всеми ведомствами, исключив формальный бюрократический подход. В Центральном банке есть серьезная аналитическая база, нужно дать возможность пользоваться ей всем учреждениям: и правоохранительным органам, и службам безопасно-

сти коммерческих банков. Возможность получить необходимую информацию и это в течение часа поможет вернуть средства сотням тысяч клиентов! И нужно наладить электронное взаимодействие, чтобы забыть, наконец, про бумажную волокиту.

Вполне возможно наладить взаимодействие между пятью сторонами-участниками: гражданами, банками, Центральным банком, правоохранительными органами и судами. При обращении гражданина в свой банк этот банк может в электронном виде организовать заявку с его подписью и тут же направить ее в Центральный банк и правоохранительные органы, а дальше в судебные инстанции, сократив тем самым время процессуальных действий в разы.

* * *

АБР готова работать в этом направлении. Мы приглашаем и Центральный банк, и правоохранительные органы, чтобы выработать именно те механизмы решения и взаимодействия, которые позволят остановить эту, нарастающую как снежная лавина, проблему.

**Андрей ВЫБОРНОВ**

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

ПРОВЕРКА БОЕМ

ШТАБНЫЕ КИБЕРУЧЕНИЯ ВЫЯВЛЯЮТ РЕАЛЬНЫЙ УРОВЕНЬ БЕЗОПАСНОСТИ, А НЕ ФОРМАЛЬНОЕ ВЫПОЛНЕНИЕ БАНКАМИ НОРМАТИВНЫХ ТРЕБОВАНИЙ

Нормативное регулирование и надзорная деятельность Банка России в отношении обеспечения информационной безопасности финансовой сферы — многоплановая деятельность, динамично развивающаяся в соответствии с новыми задачами. Ряд актуальных вопросов в этой сфере, встающих перед кредитно-финансовыми организациями, собранных Ассоциацией Банков России, заслуживают детальных разъяснений.

УСТРАНЕНИЕ РАЗНОЧТЕНИЙ

Формулировки нормативных документов Банка России в настоящее время предоставляют банкам и некредитным финансовым организациям (НФО) неравные возможности разрабатывать и проверять на уязвимость программное обеспечение. Что не может не вызывать вопросов со стороны организаций финансовой сферы.

В Положении Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» указано, что для этих целей банки могут только привлекать стороннюю компанию-лицензиата.

Положение № 684-П от 17 апреля 2019 года «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» предоставляет МФО возможность делать это самостоятельно.

Формулировку в 684-П считаем более приоритетной, различие будет устранено, нормативная документация гармонизируется. Банки, как и МФО, обладая необходимыми компетенциями, вправе самостоятельно проводить разработку безопасного программного обеспечения. Если таких

компетенций нет, они могут привлекать для этого сторонние организации, у которых есть лицензия ФСТЭК России на осуществление такого рода работ.

СРОКИ АУДИТА И ОТЧЁТНОСТИ

Сроки прохождения аудита и предоставления в Банк России отчётности о соответствии ГОСТ Р 57580.1–2017 таковы. Было запланировано, что 3-й уровень должен быть достигнут в январе 2021 года, а 4-й — в январе 2022 года. Для оформления итогов аудита будет создана специальная форма отчётности на базе 202-й, которую дополняют показателями, насколько информационная безопасность отвечает нормам государственного стандарта.

Нужно быть готовым провести оценку соответствия в 2021 году, к моменту, когда соответствующая форма отчётности вступит в силу в начале 2022 года. Таким образом, для проверки у финансовых организаций в запасе достаточно времени, почти два года.

К вопросу о профессиональных стандартах для аудиторов информационной безопасности финансовых организаций. В настоящее время разрабатывается только стандарт деятельности таких организаций, но не их сотрудников.

Вопрос аттестации специалистом ИБ преждевременный, потому что профессиональные стандарты должны быть увязаны с образовательными стандартами по этой специализации. Кроме того, необходимы аттестационные центры, где специалисты могли бы подтверждать актуальность своей квалификации, получить сертификат. Когда эта система сложится, станет возможным её нормативное закрепление.

НОВЫЙ МЕТОДИЧЕСКИЙ ДОКУМЕНТ

Федеральный закон № 173-ФЗ от 3 июля 2019 года «О внесении изменений в Федеральный закон «О национальной платёжной системе» и отдельные законодательные акты Российской Федерации» ввёл новые объекты регулирования.

Не имея возможности напрямую воздействовать на вендоров, Банк России будет стремиться при помощи других средств добиться от них необходимого результата

Ими стали новые типы организаций — платёжные агрегаторы, операторы информационного обмена и поставщики платёжного программного обеспечения.

Это новшество заставило пересмотреть Положение № 382-П от 9 июня 2012 года «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». Более того: новый состав субъектов регулирования предполагает издание нового нормативного акта.

Для банков существенных новых требований в нём не появится. Для выполняющих только функции операторов переводов денежных средств будет ссылка о защите информации на Положение № 683-П. Для банков, которые выполняют функции расчётных, клиринговых центров и другие, отдельная совокупность требований появится в новом нормативном акте, гармонизированном с 683-П.

Этот документ прошёл все предварительные процедуры согласования, Совет директоров Банка России, в настоящее время согласует в федеральных органах исполнительной власти, ФСБ России и ФСТЭК России. Принятие его ожидается к середине 2020 года, а вступление в силу — с 2021 года. До тех пор Положение № 382-П пребудет в силе.

В новом положении устраняется пересечение требований проведения финансовыми организациями аудита при помощи сторонних организаций: с одной стороны, на соответствие ГОСТ Р 57580.1–2017, с другой — требований Положения 382-П. Для оптимизации ресурсов остаётся необходимость проведения аудита только выполнения норм государственного стандарта защиты информации, а 382-П прекращает своё действие.

СЕРТИФИКАЦИЯ И АНАЛИЗ УЯЗВИМОСТЕЙ

Устраняются разночтения, постепенно накопившиеся в разных нормативных актах, унифицируются требования к сертификации и проведению анализа уязвимостей программного обеспечения. Гармонизированная с 683-П и 684-П редакция, в том числе в Положении № 672-П от 9 января 2019 года «О требованиях к защите информации в платёжной системе Банка России», такова.

Программное обеспечение для финансовых операций через интернет (чаще всего это мобильные приложения), которое предоставляют клиенту, должно быть протестировано анализом уязвимостей, либо требуется наличие сертификата. Более детальной классификации прикладного программного обеспечения для идентификации его как объекта оценки и определения приоритетности работ по анализу уязвимостей не предусмотрено.

Нормативно Банк России будет требовать проведения оценки соответствия прикладного программного обеспечения по уровню доверия ОУД4. Это блок вопросов, связанных не только с классом доверия AVA — анализом уязвимостей, одной из составных частей оценки

соответствия по ОУД4. Недостаточно провести анализ уязвимостей, определённый в компонентах доверия AVA_VAN.5 (усиленный методический анализ), AVA_CCA_EXT.1 (анализ скрытых каналов) и AVA_VAN.3. Необходима полная оценка соответствия по всем параметрам, подпадающим под ОУД4.

ОТВЕТСТВЕННОСТЬ НА СТОРОНЕ БАНКОВ

Анализ уязвимостей программных продуктов, предоставляемых вендорами — сторонними разработчиками, является известным вопросом. Требования к безопасности такой продукции накапливаются, их можно свести воедино. Но Банк России не обладает полномочиями регулировать деятельность вендоров — разработчиков программного обеспечения.

Ответственность за безопасность поставляемой сторонними разработчиками продукции Банк России может требовать только от подведомственных финансовых организаций, банков. Только сами финансовые организации в рамках договорных отношений могут предъявлять подобные требования безопасности к своим контрагентам, поставщикам программного обеспечения.

Подобным образом банк может выступать пользователем автоматизированной системы сторонних поставщиков услуг. Это тема аутсорсинга, когда обработка данных передаются на аутсорсинг поставщику услуг. Но ответственность за безопасность, с точки зрения регулирования и надзора, остаётся на стороне банка. Подробный стандарт процедур управления рисками аутсорсинга СТО БР ИББС-1.4–2018 действует уже давно.

БЕЗОПАСНОСТЬ СО СТАДИИ РАЗРАБОТКИ

Успех многих компьютерных атак на финансовые сервисы, предоставляемые клиентам, объясняется отсутствием должного контроля безопасности программного обеспечения на этапе его создания, невыявленными уязвимостями. Наибольшая часть типичных уязвимостей связана с недостатками разработки. Разработчики банковского программного обеспечения обязаны самостоятельно обеспечивать контроль уязвимостей и их устранение.

Если прямой договорной механизм не будет работать, придётся разбираться и находить механизм, который бы обязал вендоров обеспечивать безопасность поставляемого ими программного обеспечения. Как вендоры будут этого достигать, проведением анализа уязвимостей на этапе разработки, сертификации или другим путём, — неважно, важен положительный итог.

Не имея возможности напрямую воздействовать на вендоров, Банк России будет стремиться при помощи других средств добиться от них необходимого результата. Вряд ли для этого потребуются такие серьёзные меры, как изменение федерального законодательства.

САМОСТОЯТЕЛЬНО ИЛИ АУТСОРСИНГ

Проект методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций» предусматривает два варианта проверки на наличие уязвимостей. Первый вариант — самостоятельный, при наличии документально оформленного прохождения организацией процедур сертификации ФСТЭК России. Такой вариант возможен.

Второй вариант — анализ соответствия ГОСТ Р ИСО/МЭК 15408–3–2013 по ОУД4, который может выполняться как самостоятельно, так и с привлечением стороннего исполнителя. Методический документ не будет распространяться на организации, являющиеся лицензиатом ФСТЭК России по ТЗКИ (пункты «Б», «Д» или «Е»), проводящие работы по анализу уязвимостей в соответствии с ГОСТ Р ИСО/МЭК 15408–3–2013 и ГОСТ Р ИБО/МЭК 18045–2013.

Формальное требование таково, что организация, которая привлекается для проведения сертификации, должна обладать лицензией ФСТЭК России. Содержательное условие — наличие у организации-исполнителя компетенций качественно выполнить порученные работы.

Методический документ будет введён в действие по аналогии с отраслевыми стандартами. Его нормы нацелены на обеспечение информационной безопасности программно-го обеспечения для использующих его клиентов. Общая методология проведения процедуры оценки соответствия согласно ОУД4 увязывается с разными видами программного обеспечения, не только банковского.

Методический документ, нося рекомендательный характер, востребован и субъектами отрасли, не подпадающими под прямое регулирование Банком России, — вендорами и испытательными лабораториями. Потому нормы методического документа учитываются в техническом задании на проверку уязвимостей, которое заказчики, финансовые организации, составляют для исполнителей — разработчиков программного обеспечения.

УРОВНИ СООТВЕТСТВИЯ

Динамика достижения банками уровней соответствия требованиям информационной безопасности по срокам закреплена в нормативных документах. Микрофинансовые организации (МФО) в сфере информационной безопасности пока остаются вне подобного детального регулирования со стороны Банка России. На них пока не распространяются нормы Положения № 684-П.

Оценка текущего уровня обеспечения информационной безопасности и киберустойчивости в поднадзорных кредитных организациях была проведена Департаментом информационной безопасности Банка России согласно письму от 8 октября 2019 года № 56–З–7/611. Оценивались не только собственно уровень информационной безопасности, но и другие показатели надёжности.

Первые три уровня показателей включали количество прерываний деятельности из-за компьютерных атак, потери от инцидентов защиты информации, уровень фрода к общим

объёмам платежей, возврат клиентам денежных средств при несанкционированных транзакциях. Только четвёртый уровень использовавшихся показателей определял оценку соответствия отраслевым нормативам информационной безопасности. Пятый уровень — показатели качества управления рисками информационной безопасности.

Эта система показателей уровня соответствия и рисков будет развиваться в отношении и банков, и других финансовых организаций. Показатели деятельности поднадзорных субъектов по обеспечению информационной безопасности должны агрегироваться и интегрироваться в другие нормативные акты.

По мнению ДИБ Банка России, уровень информационной безопасности должен являться для банков такой же частью общих показателей экономического состояния, как и внутренние процедуры оценки достаточности капитала в соотношении с операционными рисками. В частности, одним из элементов качества управления банком рисками, который будет внедряться, станет стандарт безопасности аутсорсинга СТО БР ИББС-1.4–2018.

ШТАБНЫЕ УЧЕНИЯ — НЕ ФОРМАЛИСТИКА

Разработка методик проведения проверок финансовых организаций в сфере обеспечения информационной безопасности является внутренним делом Банка России. Подобная документация относится к служебной, а не публично распространяемой информации. Общая идеология проведения проверок заключается не в поиске формальных нарушений нормативных требований, не в определении комплаенса.

В ходе проверки, во-первых, нужно понять вероятность компьютерных атак, способных привести к инцидентам. Во-вторых, главная задача — оценить готовность поднадзорных организаций своевременно их выявить и реагировать. То есть купировать атаку, обеспечить операционную устойчивость и надёжность. Риски поднадзорных оцениваются с точки зрения потенциальных инцидентов и возможностей минимизировать их негативные последствия.

Методология проведения киберучений в финансовой сфере именно такая. Подобные учения во всех крупных, системно-значимых кредитных организациях запланированы на второе полугодие текущего 2020 года. Это будет практическая проверка подходов, применяемых в ходе проверок по инструкциям Банка России.

Предстоящие киберучения — не имитация атаки, не сканирование на уязвимости, не тесты на проникновение. В формате штабных учений будут проводиться сбор информации и другие процедуры. Цель — оценить реальную защищённость ото всех актуальных компьютерных атак.

* * *

Оценке подвергнутся наличие уязвимостей, вероятность атак и инцидентов, возможный ущерб, меры противодействия и процедуры реагирования, способности минимизировать потери. С последующей интеграцией полученных данных в общие показатели экономического состояния поднадзорных организаций.



**Денис
СЕРЕДЕНКО**
управляющий
директор, член
правления
ПАО «Плюс Банк»

ИТ И ИБ — КОНЪЮНКЦИЯ ИЛИ ДИЗЪЮНКЦИЯ?

ВЗГЛЯД СО СТОРОНЫ ИТ НА СОВРЕМЕННУЮ ПРОБЛЕМАТИКУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКАХ

Для начала обсуждения того, как сосуществуют информационная безопасность и автоматизация деятельности в рамках финансовых организаций, давайте определимся, с какими угрозами прежде всего приходится сталкиваться в аспектах информационной безопасности. Отмечу несколько угроз в порядке убывания массовости и соответственно увеличения негативных финансовых последствий.

УТЕЧКА ДАННЫХ

Утечка данных за периметр организации является сейчас наиболее массовым явлением в различных индустриях, и поэтому борьба с этим злом многофакторная и имеет разные уровни: от организационных мер до разделения уровней доступа, технических средств слежения за доступом, контроля копирования данных и многого другого. Основной ущерб — это потеря данных относящихся к коммерческой тайне и потеря персональных данных клиентов, сотрудников и контрагентов.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Этот вид угроз представляет из себя коммуникацию с клиентом или сотрудником банка, для того чтобы тот выполнил необходимые злоумышленникам действия по самостоятельному переводу им денежных средств или предоставлению необходимых данных для совершения таких операций. Обычно мошенники представляются операционными сотрудниками банка или сотрудниками службы безопасности. Для финансо-

вых учреждений такой вид мошенничества сложен к разбирательству именно потому что для банков они выглядят как совершенно легитимные операции, выполненные самим клиентом и не имеют никаких следов преступных действий.

ЗАРАЖЕНИЕ ПОЛЬЗОВАТЕЛЬСКИХ КОМПЬЮТЕРОВ

Заражение пользовательских компьютеров является обычно методом для несанкционированного получения доступа к данным и проведения незаконных операций, тем не менее мы выделяем его в списке современных угроз.

ВЫВОД ИЗ СТРОЯ ИНФРАСТРУКТУРЫ

Уничтожение бизнес-данных или их шифрация так же, как и удаление конфигураций оборудования, компонентов системного программного обеспечения являются угрозами вывода инфраструктуры из строя, использующегося в недобросовестной конкурентной борьбе и иных противоправных действиях. Одной из разновидностей вывода инфраструктуры из строя можно считать DoS-атаки, когда нецелевым трафиком заполняются ресурсы вычислительных мощностей или систем хранения данных.

ВЗЛОМ СИСТЕМ ДБО

Самыми заветными для злоумышленников являются системы, которые позволяют напрямую получить доступ к денежным средствам. Первой категорией таких систем являются системы дистанционного банковского обслуживания и особенно системы ДБО юридических лиц. Взлом системы ДБО не является взломом учётных систем и не меняет балансов на остатках счетов клиентов, но даёт доступ к расходным операциям по этим счетам, и поэтому системы ДБО юридических лиц подвержены в большей степени таким атакам — остатки у компаний гораздо больше, чем у частных клиентов. Более

Самыми заветными для злоумышленников являются системы, которые позволяют напрямую получить доступ к денежным средствам. Первой категорией таких систем являются системы ДБО

распространённым этот риск является потому, что системы ДБО по умолчанию выведены в публичную сеть интернет для использования клиентами.

ВЗЛОМ УЧЕТНЫХ СИСТЕМ

Получение доступа к учётным системам, как и следующий пункт в списке, являет собой банковский «Форт Нокс». Учётные системы — это системы которые хранят остатки на депозитных, текущих или карточных счетах, что является наиболее чувствительной информацией. Изменение информации в этих системах приводит к прямым финансовым убыткам.

ВЗЛОМ ИНФРАСТРУКТУРЫ ВЗАИМОДЕЙСТВИЯ С ПЛАТЕЖНЫМИ СИСТЕМАМИ

Инфраструктура платежных систем (SWIFT, РКЦ, карточные платёжные системы) — это компоненты ИТ-ландшафта, отвечающие за взаимодействие с другими финансовыми институтами. Заветной целью злоумышленников является вывод денег из финансового учреждения, а платёжные системы стоят как раз на стыке такого взаимодействия. Поэтому, получив контроль над этой инфраструктурой, можно от лица банка сообщать о движении средств внешним контрагентам. Например, карточной платёжной системе «сказать» при запросе на выдачу денег в банкомате другого банка, что платёжное средство проверено и транзакция авторизована, не выполняя реальную проверку.

ПРОБЛЕМАТИКА БАЛАНСА БЕЗОПАСНОСТИ И СКОРОСТИ РАЗВИТИЯ

Много перечислено угроз, и первый вывод, который приходит в голову, — всё запретить, всё отключить и действовать только после многократных проверок подлинности и достоверности. Вот тут и встаёт главная проблематика взаимодействия информационной безопасности и других служб финансовой организации: как найти баланс между скоростью развития, удобством клиентского сервиса и безопасностью информационных систем. Если выстроить очень сложную систему доступа клиентов к своим счетам через дистанционные каналы, то клиенты не будут пользоваться такими сервисами, и конкуренты, построившие данный процесс эффективнее, получают преимущества. Например, не очень далеки те времена, когда банки раздавали своим клиентам так называемые САР-калькуляторы или скретч-карты для получения одноразовых паролей, подтверждающих выполнение действий. Из-за сложности

дистрибуции и неудобства использования они ушли в прошлое в розничном обслуживании физических лиц, и баланс безопасности и удобства сместился в сторону клиентского сервиса.

ПУТИ НАХОЖДЕНИЯ ИДЕАЛЬНОГО БАЛАНСА

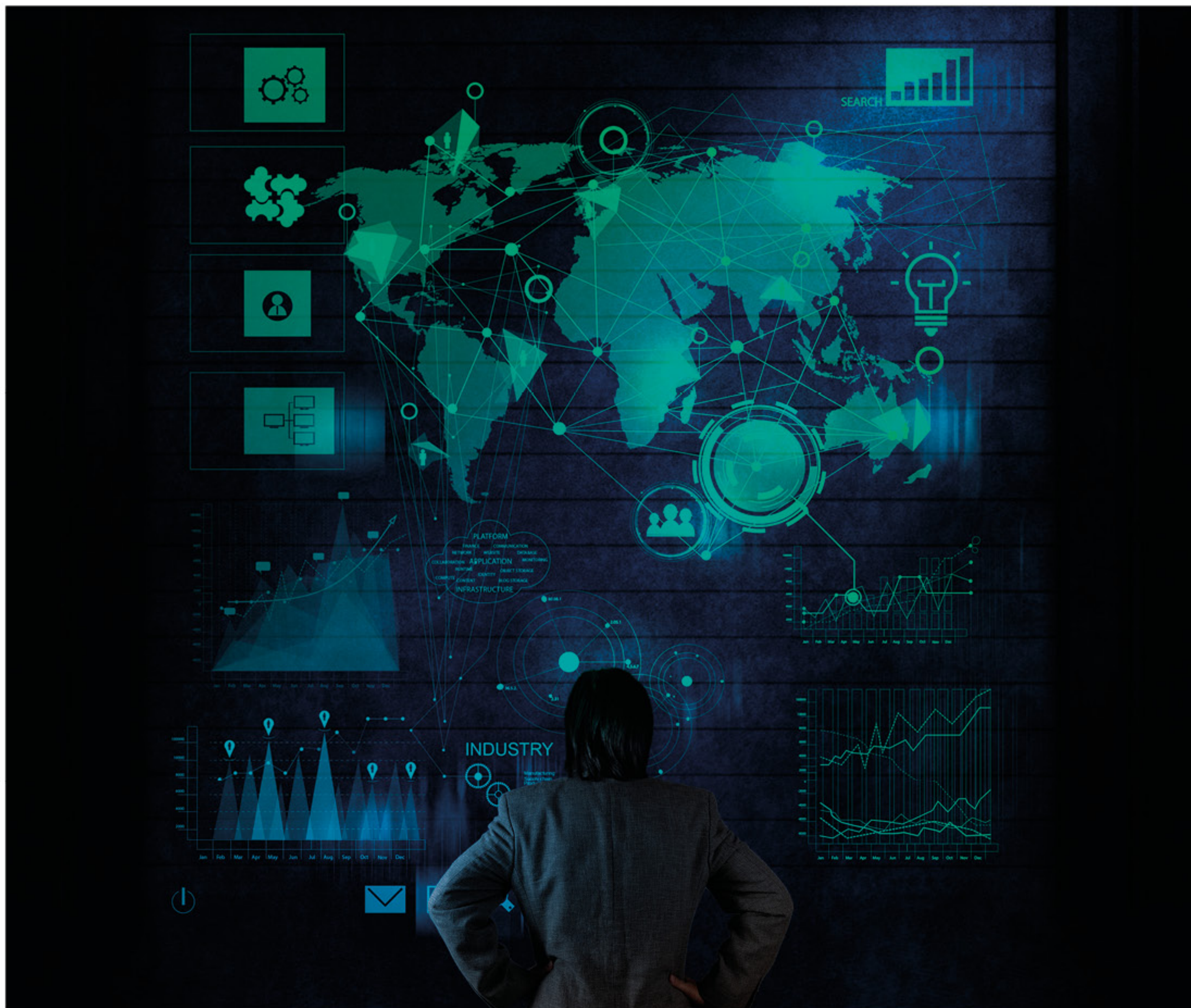
Однозначного лекала, позволяющего определить что есть истина, в данном вопросе не существует. Есть методики, определяющие уровень риска, но самый действенный метод — это опыт, эффективно построенная операционная работа по определению минимально возможных дополнительных мер, обеспечивающих безопасность информационных систем, постоянная оценка уровня риска и быстрое реагирование на возникающие угрозы. Для быстрой реакции должны быть выстроены процессы, обеспечивающие минимальный time-to-market. Но это уже тема отдельной беседы.

ПРОБЛЕМАТИКА МАСШТАБА. СИСТЕМЫ КОНТРОЛЯ ДЕЙСТВИЙ

Как в бизнесе, так и в области информационной безопасности банков, на первый план выходит эффект масштаба финансовой организации. В связи с постоянной «гонкой вооружений» между средствами защиты и средствами атак постоянно совершенствуются и усложняются технологии работы. Субъектов ИТ-инфраструктуры и их разновидностей становится с каждым годом всё больше и больше, и поэтому необходимые инвестиции в программно-аппаратные комплексы, обеспечивающие информационную безопасность, растут и уже очень заметны на фоне всех административно-хозяйственных расходов. Закономерность тут проста: чем крупнее бизнес, тем больший объём инвестиций в информационную безопасность он может себе позволить и тем меньше удельная стоимость такой безопасности для кредитной организации. Также, чем крупнее бизнес, тем интереснее он злоумышленникам.

БЕЗОПАСНОСТЬ VS УДОБСТВО

Очень важным аспектом, зачастую упускаемым из виду, является удобство не только клиентов, использующих банковские продукты, но также и удобство работы внутренних пользователей-сотрудников банков — пользователей информационных систем. Неэффективная и неудобная работа внутренних пользователей зачастую приводит к текучке кадров, невысокой производительности и, как следствие, к общей неэффективности производственного процесса. В этом вопросе надо так же, как и в вопросе удобства клиентов, проявлять повышенное



внимание, проводить постоянную оценку и использовать всесторонние подходы — не только технические, но и организационные — для решения проблем рисков халатности или внутреннего мошенничества (фрода).

ИТ И ИБ — КОНЪЮНКЦИЯ ИЛИ ДИЗЪЮНКЦИЯ?

В ситуации некоторой полярности интересов служб ИБ и ИТ встаёт вопрос эффективности их взаимодействия и нахождения компромиссов, способных устроить обе стороны. ИТ заинтересовано в максимальном упрощении процессов, «лёгкости» и доступности информационных систем для пользователей внутри банка, отсутствии большого количества уровней авторизации для доступа к данным и т.д. У ИБ полярный взгляд на данные вопросы. В такой ситуации на первый план выходят вопросы внутренних

коммуникаций и эффективно построенной модели управления, когда с одной стороны идёт постоянное общение на всех уровнях менеджмента между ИТ и ИБ, и кроме этого настроена качественная система эскалации вопросов и принятия решений в спорных ситуациях.

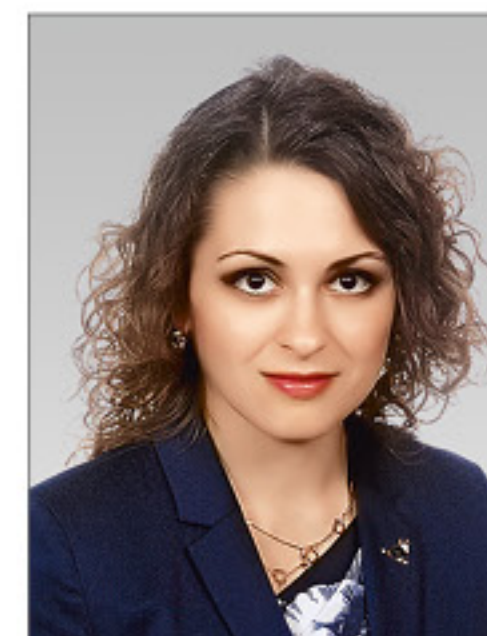
МОБИЛИЗАЦИЯ УСИЛИЙ

Хорошим примером такой слаженной и эффективной работы можно считать события последних дней, когда сотрудникам ИТ и ИБ пришлось вместе искать быстрые способы трансформации работы организаций и перевод их в дистанционные режимы работы. Коллективы показали свою нацеленность на результат и возможность работать как единый организм, обеспечивающий технологическое совершенство операционных процессов с соблюдением современных норм информационной безопасности.

ВРЕДНЫЕ СОВЕТЫ

Ещё Григорий Остер говорил, что есть ситуации, когда нужно давать не полезные, а вредные советы. Люди все сделают наоборот, и получится как раз правильно. Вот и мы попробуем. В этой рубрике мы будем предлагать материалы, разборы, трактовки, альтернативные пути реализации «проблемных» регуляторных требований по ИБ. Начнём с тех, которые выберем на своё усмотрение, а дальше надеемся, будут поступать и вопросы от читателей.

Наш первый вопрос: *В каких случаях банки обязаны использовать сертифицированные СКЗИ при передаче ПДн по каналам связи общего пользования, а в каких этого можно не делать?*



Екатерина РАЧКОВА (КАЛАШНИКОВА)
эксперт BIS Journal,
заместитель
начальника
Управления
по обеспечению ИБ
Банка ВТБ (ПАО)

ЧТО ВЫ ТОЧНО ДОЛЖНЫ ПО ЗАКОНОДАТЕЛЬСТВУ

Подпункт 13 г), включая ссылки на него из пунктов 14, 15, 16, Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в соответствии с частью 3 статьи 19 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ (далее — Закон) устанавливает необходимость использования средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Статья 19 часть 4 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ определяет, что состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с требованиями к защите персональных данных (далее — ПДн) устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК и ФСБ России), в пределах их полномочий.

ПО ЛИНИИ ФСТЭК

В соответствии с требованиями ЗИС.3 Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных» (далее — Приказ ФСТЭК № 21) и Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее — Приказ ФСТЭК № 17), должна обеспечиваться защита ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

Здесь надо отметить, что ФСТЭК поддерживает тенденцию регуляторов задавать базовый набор требований ИБ, который организация при разумном формализованном обосновании вправе адаптировать к своей технологической и экономической специфике (см. п. 10 Приказа ФСТЭК № 21 и п. 23 Приказа ФСТЭК России от 11.02.2013 № 17).

Т.е. если по всей форме разработать и утвердить у руководства банка обоснование, почему выполнить это требование технически невозможно или экономически нецелесообразно, но применить компенсационные меры, направленные на минимизацию вероятности или потерь от реализации соответствующих угроз. Более жёсткий сценарий — вообще принять регуляторные и операционные риски, связанные с невыполнением этих требований, но тогда надо быть готовым к возможным последствиям согласно части 6 (и части 2 в некоторых случаях) статьи 13.12, части 1 статьи 19.5 КоАП РФ, а также перспективам возмещать клиентам средства, если угрозы безопасности реализуются, и клиент обратится в суд. Если банк оценивает совокупные затраты на выполнение требования регулятора меньше возможных потерь

от реализации угроз от его невыполнения, то риск скорее всего будет обработан именно путём принятия.

ПО ЛИНИИ ФСБ

Пункт 2 «Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утверждённых руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6–432 (далее — Методические рекомендации), указывает, что *использование средств криптографической защиты информации* (далее — СКЗИ) для обеспечения безопасности ПДн необходимо, если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, в этом же пункте отнесена *передача ПДн по каналам связи, не защищённым от перехвата нарушителем передаваемой по ним информации* или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования).

Кроме того в том же пункте указано, что для обеспечения безопасности ПДн при их обработке в информационных системах *должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия*.

В силу Положения об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов её проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, утверждённым постановлением Правительства Российской Федерации от 15.05.2010 № 330, на которое ссылается Информационное сообщение ФСТЭК России от 04.05.2012 № 240/24/1701, *оценка соответствия средств, предназначенных для защиты информации конфиденциального характера, средств, в которых они реализованы, а также средств контроля эффективности защиты информации, используемых в целях защиты государственного информационного ресурса и (или) ПДн, осуществляется в форме обязательной сертификации*.

ФСБ ДАЁТ РЕКОМЕНДАЦИИ. ДЛЯ КОГО ОНИ ОБЯЗАТЕЛЬНЫ?

Указанные Методические рекомендации согласно разделу Введение предназначены для федеральных органов исполнительной власти, осуществляющих функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органов государственной власти субъектов Российской Федерации, органов государственных внебюджетных фондов, иных государственных органов, которые, в соответствии с частью 5 статьи 19 Закона, в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке ПДн в информационных системах персональных данных (далее — ИСПДн), эксплуатируемых при осуществлении соответствующих видов деятельности, с учётом содержания ПДн, характера и способов их обработки.

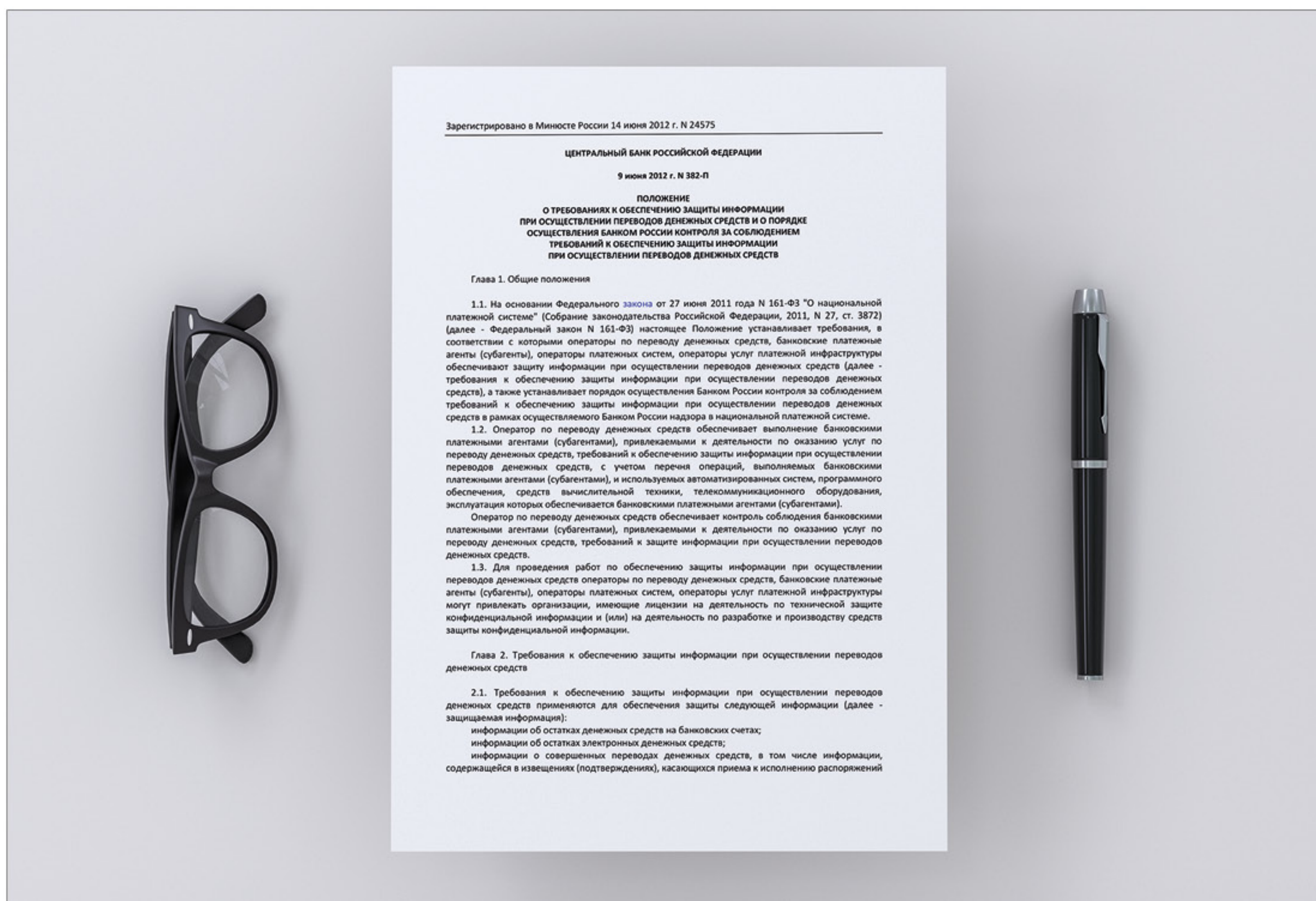
Во Введении также указано, что настоящими методическими рекомендациями *целесообразно также руководствоваться* при разработке частных моделей угроз операторам ИСПДн, *принявшим решение об использовании СКЗИ* для обеспечения безопасности ПДн.

Если банк не подпадает под указанные выше условия и(или) решения об использовании СКЗИ для обеспечения безопасности ПДн не принимал, Методические рекомендации для него не являются обязательным к исполнению документом, а соответственно и пункт 2 Методических рекомендаций не является обязательным к выполнению в банке.

А КАК БЫТЬ, ЕСЛИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ОБРАБАТЫВАЮТСЯ В ПЛАТЁЖНОЙ СИСТЕМЕ (НАПРИМЕР, ДБО)?

Если *передача ПДн осуществляется системой, выполняющей банковский платёжный технологический процесс*¹, то в соответствии с действующим законодательством Российской Федерации и требованием Б.3 национального стандарта Российской Федерации ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» банк устанавливает критерии отнесения автоматизированных информационных систем к ИСПДн банка. При этом Банком

¹ В терминологии пункта 3.28 Стандарта Банка России СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (далее — СТО БР ИББС-1.0–2014).



России в пункте 7.10.3 СТО БР ИББС-1.0–2014 дана рекомендация не относить к ИСПДн системы, реализующие банковский платёжный технологический процесс. Весомость этого аргумента усилится, если в своё время банк ввёл у себя комплекс стандартов Банка России приказом («присоединился» к стандарту).

Система, выполняющая банковский платёжный технологический процесс, попадёт в область действия Положения Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (далее — Положение № 382-П).

Согласно пункту 2.9.1 Положения № 382-П, только в случае если оператор по переводу денежных средств, банковский платёжный агент (субагент), оператор услуг платёжной инфраструктуры *применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа*. Там же указано, что обеспечение

защиты ПДн с помощью СКЗИ должно осуществляться в соответствии с приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости» (далее — Приказ № 378).

В соответствии с пунктом 16 с учётом ссылки из него на пункт 5г Приказа № 378 для защиты ПДн при их обработке в ИСПДн необходимо использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз. Этот пункт снова приводит нас к Методическим рекомендациям, о применимости которых было сказано выше.



Дмитрий ГАДАРЬ
вице-президент —
директор
департамента
информационной
безопасности,
Tinkoff.ru



Игорь КУБЫШКО
глава направления
Security Operations
Center, Tinkoff.ru

ЭФФЕКТИВНЫЙ SOC — ЭТО СЛОЖНО

НО НЕДОРОГО

Тинькофф — первый и единственный в России полностью онлайн-банк и финансовая экосистема, обслуживающая свыше 11 миллионов клиентов дистанционно через онлайн-каналы и контакт-центр. Структура экосистемы накладывает высокие требования к уровню информационной безопасности как внутренних ИТ-систем, так и финансовых продуктов, сервисов. В этом контексте ключевые приоритеты для Тинькофф — стабильное бесперебойное функционирование операционных процессов и защита от широкого спектра киберугроз, несущих потенциальные риски для ежедневной работы банка.

На прошедшем в феврале XII Уральском форуме Дмитрий Гадарь и Игорь Кубышко рассказали об уникальном опыте и эффективной работе центра оперативного управления информационной безопасностью Тинькофф. Публикуем их выступление в кратком изложении.

КОМПОНЕНТЫ SOC

Большинство Security Operations Center строится сегодня из одинаковых компонентов: системы безопасности, источники событий, SIEM, SOAR. К первым можно смело отнести антивирусы, системы обнаружения вторжений и прочие, источниками же информации могут быть операционные системы, серверы, рабочие станции, прикладные системы.

SIEM (Security Information and Event Management) — система, предназначенная для анализа информации, поступающей от различных других систем, таких как DLP, IDS, антивирусов, различных железок и дальнейшего выявления отклонения от норм по заданным критериям. При выявлении отклонения генерируется инцидент.

SIEM включает:

- ♦ транспортировку и нормализацию поступающих данных: в общую архитектуру могут входить коллекторы, коннекторы и дополнительные брокеры данных;
- ♦ хранение и визуализацию данных;
- ♦ правила корреляции, обогащения и алертинг: это правила SIEM, которые позволяют оповещать об атаках, изменениях показателей

защищенности инфраструктуры и внутренних процессах в компании, отправлять оповещения в e-mail, мессенджер, тикет системы.

SIEM для эффективного и быстрого реагирования на инциденты не всегда важен, без него можно обойтись, например, заменив обычной системой log management. Важно правильно построить процессы, подобрать персонал, который сможет заниматься инцидентами информационной безопасности и быть основой для SOC. То есть SOC возможен без SIEM.

Один из процессов, без которого не может обойтись ни один SOC — Incident response.

Это реагирование на инциденты информационной безопасности, выстраивание правильных процессов и автоматизация реагирования. Есть индикаторы компрометации, по которым мы ищем аномалии в поведении. Среди индикаторов компрометации — IP, домены, хеши файлов, размеры файлов. Здесь есть два подхода: первый — поиск чего-то известного, злодейского в поведении; второй — профилирование поведения системы, пользователя и поиск отклонений от профиля. При этом считаются любые отклонения и выстраивается реагирование на них. Но второй вариант применим лишь для некоторых систем. Ярким примером являются банкоматы, поведение которых хорошо профилируется и любое отклонение от штатного поведения можно считать инцидентом.

Следующий компонент — MISP (Malware Information Sharing Platform) — это платформа для сбора, агрегации, актуализации базы IoC. Система позволяет удобно хранить данные, полученные с помощью поиска информации об атаках и IoC, как из открытых источников — Twitter, Allien Vault, Telegram каналов, так и платных источников.

Playbooks — это не просто бумажка, а техническое описание управляемых процессов. Часть из них может быть автоматизирована. При этом важно поддерживать их в актуальном состоянии: избавляться от старых, создавать новые, релевантные тем угрозам, которые существуют у организации.

Немного отдельно стоят аддоны: threat hunting, machine learning, antifraud, которые хорошо коррелируют со всеми частями SOC.

Threat hunting позволяет осуществлять активный поиск угроз. Здесь могут применяться индикаторы, техники и тактики поведения злоумышленников.

Совместно с ИБ-компаниями Тинькофф проводил «пентест наизнанку»: искали признаки того, что в данный момент банк находится под атакой. Если бы атака обнаружилась, банк оплатил бы работу.

Так, если рассматривать, что среднее время атаки составляет три месяца, то такая аналитика раз в квартал с большой вероятностью поможет выявить злоумышленника ещё до того, как он нанёс ущерб компании.

Машинное обучение в будущем может заменить безопасность, поскольку ищет как раз отклонения от нормального поведения.

Очень важно при планировании своей архитектуры и в целом информационной безопасности опираться на цели, ради которых вы это делаете, и основываться на тех потребностях, которые есть у вашей организации, конкретно с вашими рисками в той области угроз, в которой вы находитесь.

SOC — ГЛАЗА ВСЕЙ БЕЗОПАСНОСТИ

Тинькофф использует как внешний, так и внутренний SOC. Базовые сервисы и всё, что профилируется, стандартизируется, отдано под внешний SOC, а специфические темы или темы,

которые вряд ли нужны всему рынку, делаются самостоятельно.

Ключевую роль при построении ИБ в Тинькофф играет персонал, который может поддерживать систему и решать бизнес-задачи. На второй уровень выходят процессы, а уже потом возникают технологии.

При работе с инцидентами есть определённый план действий. На первом этапе Incident Response стоит подготовка к инциденту: различные комплаенс контроли, настройка средств защиты, в том числе написание плейбуков. Далее начинается работа SOC — обнаружение злоумышленников.

SOC не всегда может обнаружить аномалии, потому что информация может прийти и со стороны: от клиентов или сотрудников. После обнаружения необходимо сдерживать злоумышленников. И тут опять нужен выработанный план действий в случае обнаружения какой-либо угрозы в инфраструктуре. С помощью внутренней команды Red Team проводятся учения и проверяются актуальность и работоспособность playbook и правил корреляции.

Последний этап — это выводы: где они хорошо сработали, а где плохо, как в дальнейшем сделать так, чтобы атака не повторилась, какие контроли сработали эффективно, а какие нет. После прохождения всех этапов по реагированию процесс повторяется.

ОБЗОР

Threat Intelligence. Регулярный и системный сбор информации об угрозах, её улучшение и обогащение, применение этих знаний для защиты, а также возможность делиться ими с теми, кому они могут быть полезны, а также анализ вредоносного ПО собственными силами. Например, Тинькофф регулярно делится с доверенными компаниями информацией об индикаторах компрометации.

Технологии: Open source. В банке есть компетенции, позволяющие дорабатывать тот или иной open source под свои задачи. Политика в данном вопросе такова: мы своими силами оперативно стараемся найти решение, а не покупать его или запрашивать на стороне. Зачем? Для достижения цели наименьшими усилиями. Далеко не все решения, которые предоставлены на рынке, могут оперативно покрыть внутренние специфические задачи, а предлагаемые решения могут содержать не актуальный для наших условий функционал.

Архитектура: Системы безопасности. Используются стандартные антивирусные решения, EDR, различные песочницы и т.д. Однако в последнее время EDR в плане детектирования злоумышленника выходит на высший уровень. К классическим средствам также добавлены расширенный мониторинг, TI (OSINT), red teaming, интегрированный в оценку реальных рисков, расширенное журналирование и реагирование...

Аналитика. Для аналитика SOC быстро собрать какие-то аномалии внутри той или иной машины, того или иного сервера, EDR решение — это прекрасная вещь. В этот момент даже не нужен SIEM.

EDR позволяет не только заблокировать активность, но и предоставить ход заражения (Timeline) сервера или рабочей станции для анализа и эффективного реагирования.

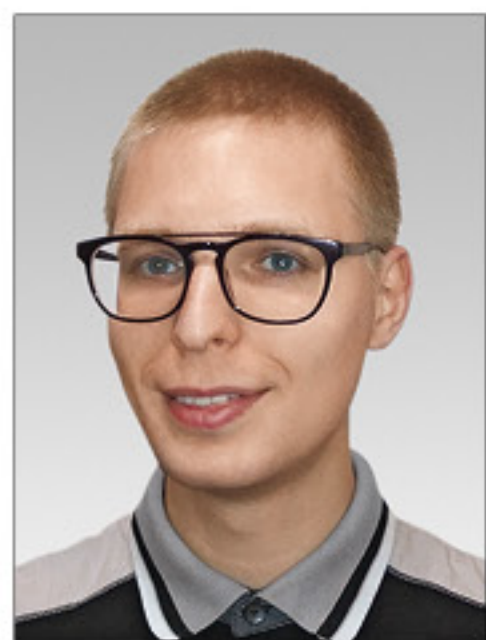
Стандартизация правил. Аналитика берётся извне, например, из сигма-правил, в простом формате эти правила можно транслировать как в Arcsight, так и на стек ELK или другую SIEM систему.

Песочницы. В Тинькофф эшелонная защита из решений нескольких вендоров. Ежегодно пересматривается эффективность каждого эшелона по отношению к актуальным угрозам на рынке.

Отправка и нормализация данных. В этом вопросе тоже классический подход — использование коллекторов. Банк собирает события средств защиты и кладёт на хранение в брокер Kafka, который позволяет 12 часов хранить большой поток данных, не боясь их потерять.

Хранение данных и визуализация. Здесь за основные системы используют Elastic и Arcsight. Дальше уже внутренняя разработка, обвязки, которая позволяет оптимизировать проблематику эластичности. Также они используются другие различные системы визуализации.

Оркестрация и автоматизация управления инцидентами. Тинькофф использует open source, который в большей части переделан под собственные задачи и специфику внутренних процессов.



Денис КОРЯКОВСКИЙ
ведущий инженер
Управления
экспертизы
кибербезопасности
Сбербанка



Алексей ТЕРЕНИН
директор
проектов Центра
внутрикорпоративного
взаимодействия
Сбербанка

ИИ НА СТРАЖЕ БАНКОВСКИХ ДАННЫХ

ОПЫТ СБЕРБАНКА

Оперативный обмен большими объемами данных и их обработка стали необходимым условием для успешного ведения бизнеса — включая, разумеется, банковский. При этом данные — ценный актив, который привлекает внимание злоумышленников, особенно когда речь идет о финансовых организациях. За сохранностью данных всё пристальней следит государство: компании, которые не обеспечили должный уровень безопасности, могут быть наказаны значительными штрафами. Поэтому любой обмен данными в банках должен оперативно контролироваться и быть безопасным. Один из ключевых вопросов — как в огромных объемах информации быстро и эффективно выявлять данные, которые должны быть защищены? И здесь на помощь приходит автоматизация на основе искусственного интеллекта.

В Сбербанке накоплен огромный массив данных, на материале которых обучены модели искусственного интеллекта. Теперь эти модели сами адаптируются к внутренним изменениям и позволяют осуществлять быстрые проверки на наличие защищаемых данных. Эта статья о том, как мы используем нейронные сети для обнаружения таких данных.

ПОЧЕМУ ДАННЫЕ СЛОЖНО КОНТРОЛИРОВАТЬ

С технической стороны большие данные постоянно меняются. Во-первых, изменения затрагивают правила и шаблоны заполнения вну-

тренных систем банка. Во-вторых, в различных бизнес-процессах могут возникнуть ошибки: например, может произойти сдвиг полей, и данные в таблицах не будут соответствовать атрибутивному составу. Наконец, клиенты банка могут ввести не те данные, для которых предназначено поле: например, указать номер карты в назначении платежа или комментария. Поэтому проверяющие системы должны не только отслеживать атрибутивный состав данных, но и контролировать сами данные, проверяя их построчный состав в таблицах.

Наиболее популярные системы противодействия утечкам построены с использованием фильтров на регулярных выражениях. С одной стороны, такие фильтры классифицируют текстовые виды защищаемых данных не так хорошо, как числовые. С другой — их проще составить, и они работают гораздо быстрее ручной проверки. Один из выходов — применять словари с экземплярами защищаемых данных и, используя статистический анализ, пытаться интерпретировать результат. Однако есть и альтернатива: использовать для поиска и классификации данных алгоритмы машинного обучения.

ОДНО ИЗ РЕШЕНИЙ СБЕРБАНКА

В основе большинства информационных систем Сбербанка используются СУБД. Во внешние контуры передаются уже готовые данные в табличном виде. Поэтому в первую очередь мы решили создать классификатор уровня требуемой защиты данных, представленных в табличном виде.

Основной составляющей части рассматриваемого решения мы используем несколько нейросетей. В качестве дополнительных элементов мы применяем проверки на контрольные разряды, например, у номеров карт; и регулярные выражения с достаточно высокими — более 95% — показателями точности и полноты. Итоговый результат обрабатывается алгорит-

Проверяющие системы должны не только отслеживать атрибутивный состав данных, но и контролировать сами данные, проверяя их построчный состав в таблицах

мом интерпретации результатов предыдущих модулей с применением математической статистики (рис. 1).

На рисунке 1 показано, что на вход системе подаются таблицы, которые могут быть представлены, например, в формате.xls, после чего информация классифицируется по видам защищаемых данных. Среди алгоритмов классификации есть нейросети, фильтры на регулярных выражениях и проверка на контрольные разряды. Результат предварительной классификации передаётся на следующий этап, на котором даётся итоговая оценка каждой ячейки с учётом ранее вычисленных показателей качества классификации вышеуказанных алгоритмов. Кроме того, производится классификация всей таблицы по категории требуемой защиты информации. На выходе получается таблица, размеченная тегами, которые соответствуют видам защищаемой информации (рис. 2) и отчёт, в котором приводится подробная информация о классифицированном составе данных.

Для решения задачи поиска и классификации защищаемых данных в табличном представлении требуется выбрать алгоритмы и данные для обучения. Необходимо сделать выбор: обучение с учителем или без учителя? Мы выбрали первый вариант, так как в нашем банке накоплен объёмный массив защищаемой информации, и обучение можно проводить с её использованием. Для обучения и проверки качества нейросетей нужны специальные выборки: заранее подготовленные для обучения размеченные данные. Их можно взять из баз данных внутренних информационных систем, благодаря чему увеличивается качество распознавания.

Разработчики не должны работать с данными ограниченного доступа (это создаёт дополнительные риски), поэтому требовалось решить проблему создания обучающих выборок, которые будут соответствовать этому условию. Размеченные выборки для каждого вида данных получаются с помощью загрузки одной колонки из таблицы с экземплярами конкретного вида защищаемых данных, которые без связи со значениями из остальных полей таблицы зачастую теряют свою значимость и требуют меньшей защиты (рис. 3). Такой способ получения обучающих выборок допустим для большинства видов данных. Однако существуют некоторые виды данных, например, номера карт, которые являются конфиденциальными сами по себе без связи с дополнительными полями из таблиц, поэтому их следует генерировать с помощью программы.

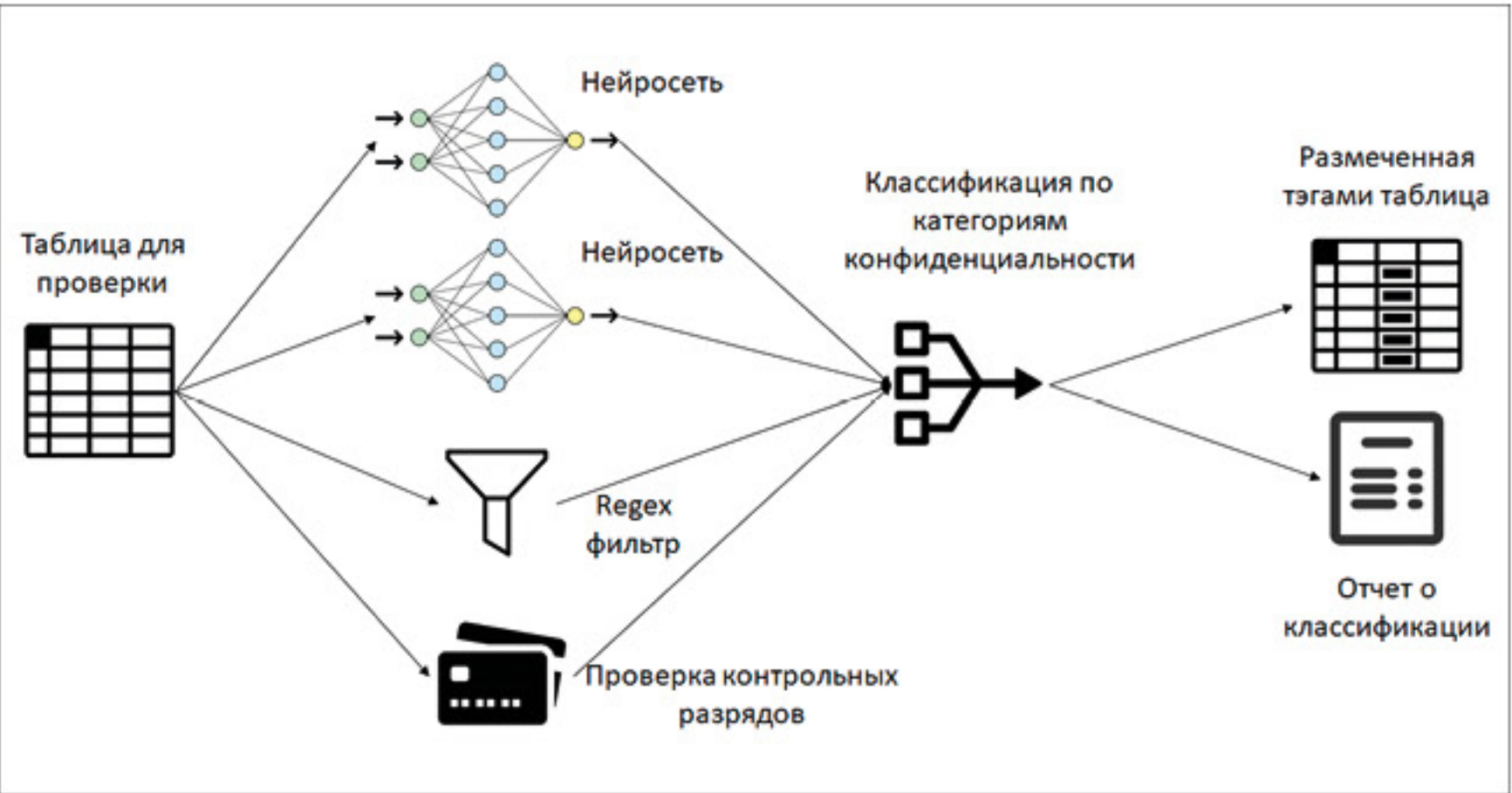


Рисунок 1. Структура системы поиска и классификации данных, требующих защиты

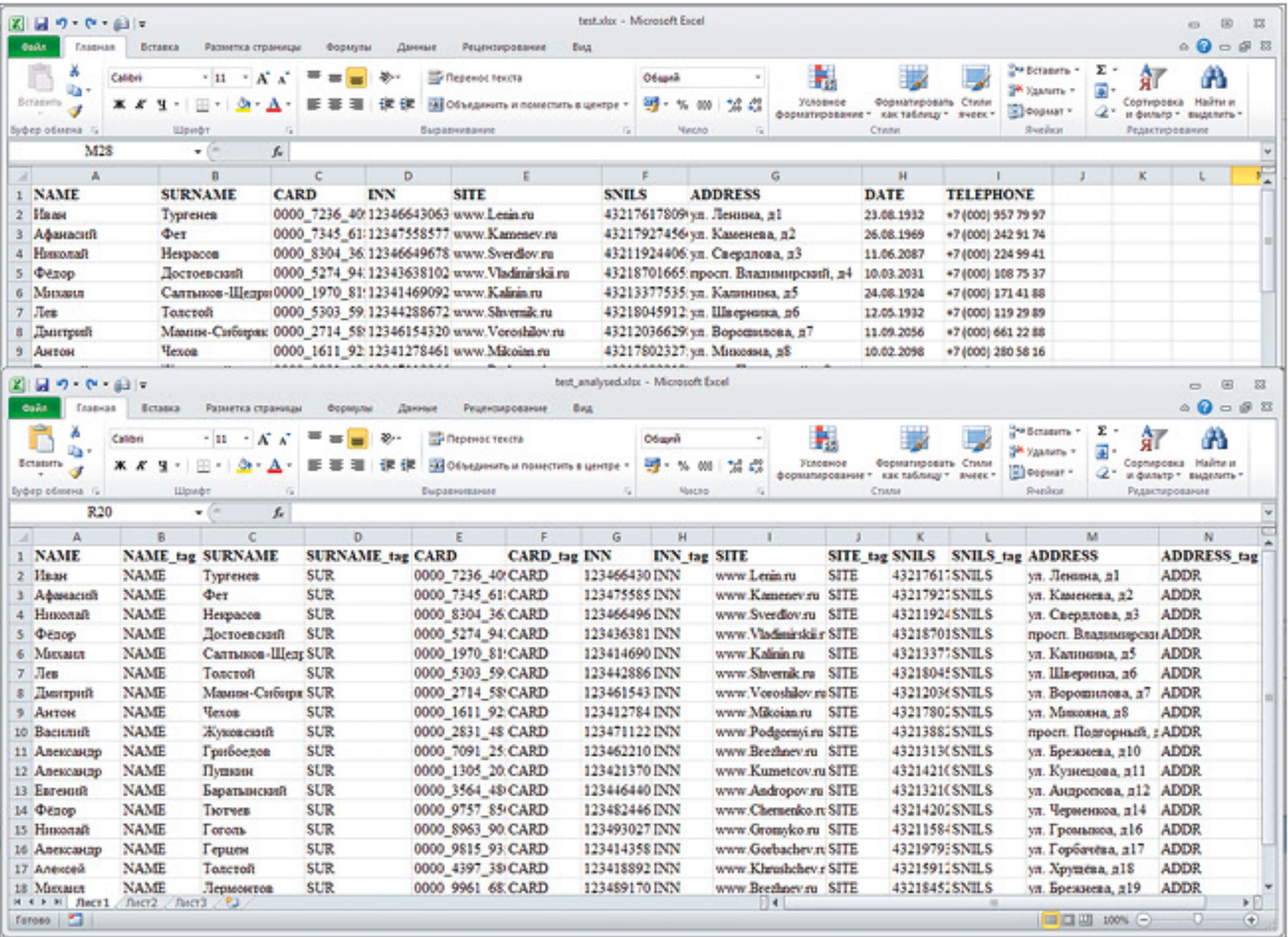


Рисунок 2. Пример разметки таблицы тегами. Сверху находится исходная таблица, снизу — проверенная, с предоставленными тегами

NAME	SURNAME	CARD	INN	NAME
Иван	Тургенев	0000_7236_40	12346643063	Иван
Афанасий	Фет	0000_7345_61	12347558577	Афанасий
Николай	Некрасов	0000_8304_36	12346649678	Николай
Фёдор	Достоевский	0000_5274_94	12343638102	Фёдор
Михаил	Салтыков-Щедрин	0000_1970_81	12341469092	Михаил
Лев	Толстой	0000_5303_59	12344288672	Лев
Дмитрий	Мамин-Сибиряк	0000_2714_58	12346154320	Дмитрий
Антон	Чехов	0000_1611_92	12341278461	Антон
Василий	Жуковский	0000_2831_48	12347112266	Василий
Александр	Грибоедов	0000_7091_25	12346221010	Александр
Александр	Пушкин	0000_1305_20	12342137040	Александр
Евгений	Баратынский	0000_3564_48	12344644017	Евгений
Фёдор	Тютчев	0000_9757_85	12348244692	Фёдор
Николай	Гоголь	0000_8963_90	12349302711	Николай
Александр	Герцен	0000_9815_93	12341435822	Александр
Алексей	Толстой	0000_4397_38	12341889264	Алексей
Михаил	Лермонтов	0000_9961_68	12348917011	Михаил

Рисунок 3. Пример зависимости значимости данных от контекста и объединения с другими данными

"... Так говорила в июле 1805 года известная Анна Павловна Шерер, фрейлина и приближенная императрицы Марии Феодоровны, встречая важного и чиновного князя Василия, первого приехавшего на ее вечер. Анна Павловна кашляла несколько дней, у нее был грипп, как она говорила (грипп был тогда новое слово, употреблявшееся только редкими). В записочках, разосланных утром с красным лакеем, было написано без различия во всех..."

До

"Так говорила в известная, фрейлина и приближенная императрицы, встречая важного и чиновного князя Василия, первого приехавшего на ее вечер. кашляла несколько дней, у нее был грипп, как она говорила (грипп был тогда новое слово, употреблявшееся только редкими). В записочках, разосланных утром с красным лакеем, было написано без различия во всех"

После

Рисунок 4. Пример создания выборки незначимых данных

Далее часть каждого набора данных разделяется случайным образом на три части — тренировочную, тестовую и валидационную выборки, на которых уже и ведётся обучение алгоритма, настройка его параметров, предварительная проверка и окончательная оценка качества классификации, получившейся после обучения модели.

Для обучения алгоритмов нужны выборки данных, которые не требуют защиты, — такой набор данных был получен путем загрузки слов и словосочетаний из нескольких документов и книг, далее были убраны элементы, которые потенциально могут быть отнесены к видам защищаемой информации: например, имена и фамилии (рис. 4).

Для некоторых числовых видов данных (например, дат) достаточно создать фильтры с использованием регулярных выражений. Точность распознавания дат с помощью регулярных выражений составляет чуть менее 100 %. Поэтому для оптимизации работы нейросетей было решено добавить в систему некоторые фильтры на регулярных выражениях. Для других данных, таких как номера карт, ИНН, ОГРН, существует проверка с помощью алгоритма Луна¹ на соответствие контрольных разрядов. Система, состоящая из фильтров на регулярных выражениях, модуля проверки контрольных разрядов и ансамбля из четырёх моделей имеет точность классификации 95 %.

Для повышения точности распознавания защищаемых данных проводится обучение нескольких моделей. Для объединения результатов классификации несколькими моделями (ансамблем моделей) применяется алгоритм, основан-

ный на анализе матриц классификации (рис. 6). Они показывают, сколько экземпляров каждого вида защищаемых данных было классифицировано как один из их видов. Таблицы на этом этапе строятся следующим образом: по вертикали указывается реальная классификация данных, а по горизонтали то, как они распознаны алгоритмом. В ячейках указано, сколько экземпляров конкретного вида защищаемых данных было распознано как их вид.

Сравнение моделей производилось на синтетически генерируемой таблице, содержащей все используемые в модели виды данных и состоящей из 1000 экземпляров каждого вида (рис. 5). Исходя из этого, максимальное возможное число в каждой ячейке — 1000.

Соответственно, главный критерий хорошо обученной модели — увеличение значений элементов, лежащих на диагонали матрицы, они подсвечены зелёным фоном, и уменьшение значений, не находящихся на диагонали — ошибок первого и второго рода, они подсвечены оттенками красного.

В качестве метрик успешности обучения и, соответственно, весов алгоритма итоговой классификации была выбрана F-мера, которая является средним гармоническим для точности и полноты (рис. 7). Точность (precision) — доля экземпляров, действительно принадлежащих данному классу, относительно всех экземпляров, которые система отнесла к этому классу. Полнота (recall) — доля найденных классификатором экземпляров, принадлежащих классу относительно всех экземпляров этого класса в тестовой выборке. На рисунке 8 показаны показатели точности и полноты классификации защищаемых данных.

	$y = 1$	$y = 0$
$\hat{y} = 1$	True Positive (TP)	False Positive (FP)
$\hat{y} = 0$	False Negative (FN)	True Negative (TN)
$precision = \frac{TP}{TP + FP}$		$recall = \frac{TP}{TP + FN}$
$F_\beta = (1 + \beta^2) \cdot \frac{precision \cdot recall}{(\beta^2 \cdot precision) + recall}$		

Рисунок 7. Формулы для точности, полноты и F-меры

¹ Алгоритм Луна (англ. Luhn algorithm) — алгоритм вычисления контрольной цифры номера пластиковой карты в соответствии со стандартом ISO/IEC 7812. Не является криптографическим средством, а предназначен в первую очередь для выявления ошибок, вызванных непреднамеренным искажением данных (например, при ручном вводе номера карты, при приёме данных о номере социального страхования по телефону). Позволяет лишь с некоторой степенью достоверности судить об отсутствии ошибок в блоке цифр, но не даёт возможности нахождения и исправления обнаруженной неточности. Алгоритм разработан сотрудником фирмы IBM Гансом Питером Луном, описан в США в 1954 году, патент получен в 1960 году.

Рисунок 5. Таблица с синтетическими данными для проверки качества обучения моделей

Рисунок 6. Пример матрицы классификации для одного из алгоритмов



	neural_net_1	neural_net_2	neural_net_3	neural_net_4	regex	control_digit	result
O	99.9	100	100	42.1	0	0	100
ACCOUNT	0	0	0	0	100	100	100
COORD	1.5	100	99.5	0	0	0	100
VK	100	100	100	100	0	0	100
OGRN	0	0	0	0	0	100	100
MAIL	100	100	86.6	99.5	0	0	100
VOIN	0	0	0	35.3	100	0	100
KPP	0	0	0	0	100	0	100
INDP	100	100	99.8	99.8	0	0	100
INN	0	0	0	0	0	100	100
CARD	0	0	0	0	0	100	100
LEI	99.5	99.9	98.3	94.4	99.9	0	99.9
UL	95.2	97.9	92.3	99.6	0	0	99.6
DOLJN	68.9	85.9	63.8	99.3	0	0	99.3
PTS	0	0	0	0	98.7	0	98.7
ADDR	97.9	98.6	70	93.4	0	0	98.6
FLO	91.1	95.8	95.4	98.6	0	0	98.6
BANK	89.2	93.8	83	97.3	0	0	97.3
ALIAS	85.3	1.9	76.6	95.5	0	0	95.5
OGRNIP	0	0	0	0	0	94.7	94.7
SUR	93	71.5	78.6	48.7	0	0	93
OMS	0	0	0	0	0	91.9	91.9
OKPO	0	0	0	0	0	89.2	89.2
NAME	0	85.2	5.2	88.7	0	0	88.7
FNAME	0.5	85.6	76.1	87.2	0	0	87.2

Рисунок 9. Фрагмент матрицы мер (F-меры) качества распознавания данных каждым используемым алгоритмом. Тегом «O» обозначаются незначимые данные (сокращённо от «other»)

Веса классификации каждого алгоритма заносятся в таблицу. Они применяются в специальной формуле, которая, используя информацию о классификации конкретного экземпляра данных и метрики качества алгоритмов, выдаёт итоговую классификацию каждой ячейки в подлежащей проверке таблице. Точность классификации каждого алгоритма и системы в целом показаны на рисунке 9.

На рисунках 10, 11, 12 показаны веса качества классификации. Настройки каждой нейросети отличаются, что позволяет по-разному распознавать каждый вид защищаемых данных. Так, нейросети 2 и 4 лучше распознают словосочетания, а нейросети 1 и 3 специализируются на отдельных словах. Некоторые защищаемые данные могут быть отнесены сразу к нескольким видам. Например, номер банковской карты Visa может содержать 13 цифр, так же, как и ОГРН, и различные алгоритмы проверки контрольных разрядов могут одновременно выдавать положительный результат.

Как видно из таблицы, итоговые показатели классификации, которые помечены чёрной линией, лучше показателей алгоритмов, работающих по отдельности. В редких случаях возможны «выбросы» за чёрную линию — в этих случаях классификация некоторых алгоритмов выше качества классификации всей системы. Это связано с тем, что система считает веса всех алгоритмов для каждого вида защищаемых данных, после чего сравнивает суммы весов — классификация зависит от того, у какого вида данных сумма весов больше. Для уменьшения эффекта от суммы нескольких неверных классификаций нужно подбирать итоговую взвешивающую функцию. На данный момент выбрана та, которая создаёт менее значимую ошибку.

Применение нескольких видов алгоритмов позволяет использовать преимущества каждого из них, что в итоге повышает общее качество классификации системы. Экспериментально было установлено, что нейросети лучше распознают текстовые виды данных, а регулярные выражения лучше распознают числовые данные.

Для классификации всей проверяемой таблицы по классам требуемой защиты данных строится алгоритм классификации, обучающийся на данных вида «атрибутивный состав — его классификация». Они были получены на основе архивов с информацией о ручной классификации данных экспертами по кибербезопасности и по оценке рисков. В зависимости от требований, регулирующих этот процесс, и нормативных документов можно учитывать не только весь список найденных в таблице защищаемых данных, но и количество вхождений каждого из видов в таблице.

ПРИКЛАДНАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ КЛАССИФИКАЦИИ

В качестве прикладной реализации системы классификации защищаемых данных был создан веб-интерфейс, где фокус-группа, состоящая из заказчиков данной услуги, протестировала разработанный алгоритм. Пользователь загружал файл в формате.xlsx на сайт. Обратно он получал таблицу, в которой каждая ячейка была распознана как вид информации, и отчет об атрибутивном составе таблицы с указанием категории требуемой защиты, по которой строго определяются правила работы с данной информацией.

Применение тестирования с помощью фокус-группы позволяет не только выявить достоинства и недостатки реализации алгоритма и интерфейса, лучше понять пожелания конкретного заказчика, но также получить новые данные для обучения моделей в том формате, в котором они будут использоваться заказчиком.

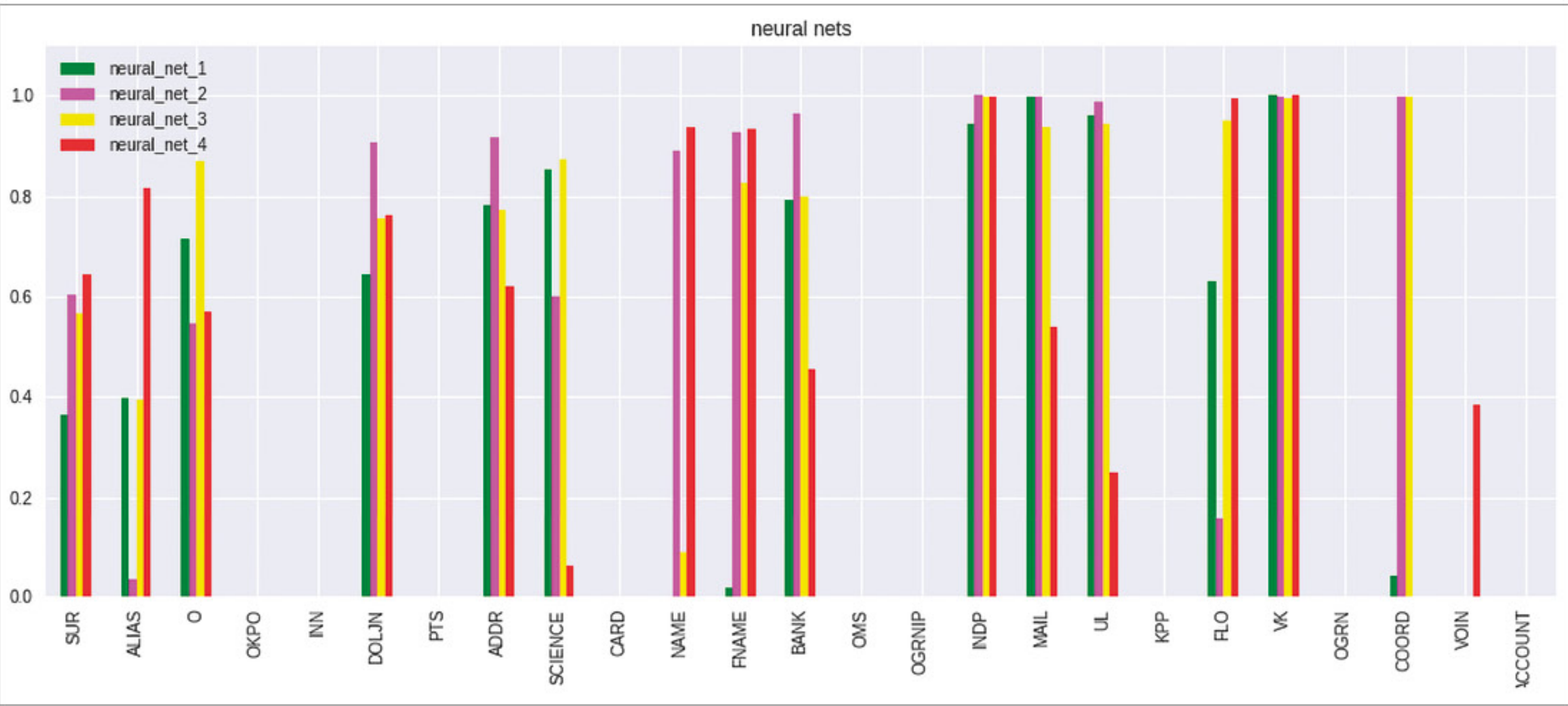


Рисунок 10. Метрики (F-меры) качества нейросетей

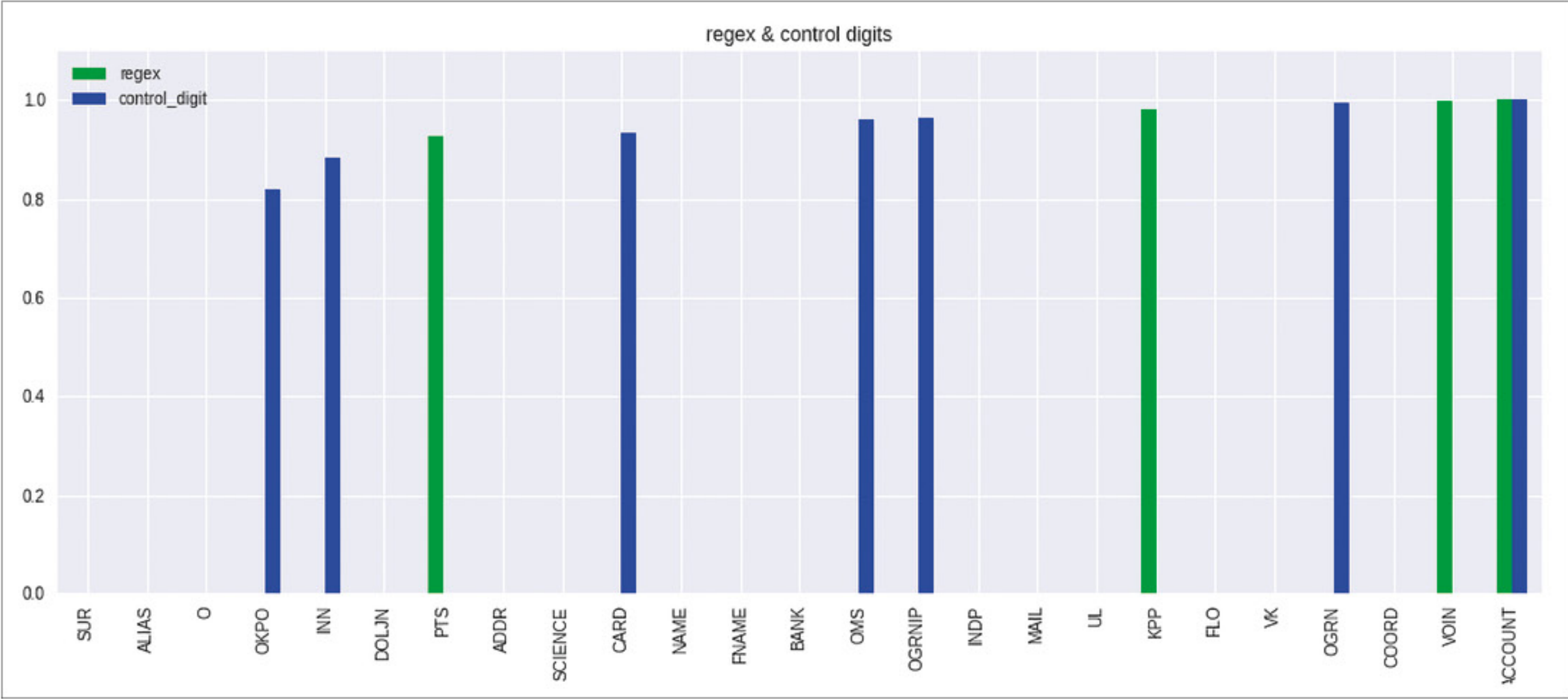


Рисунок 11. Метрики (F-меры) качества регулярных выражений и проверки контрольных разрядов

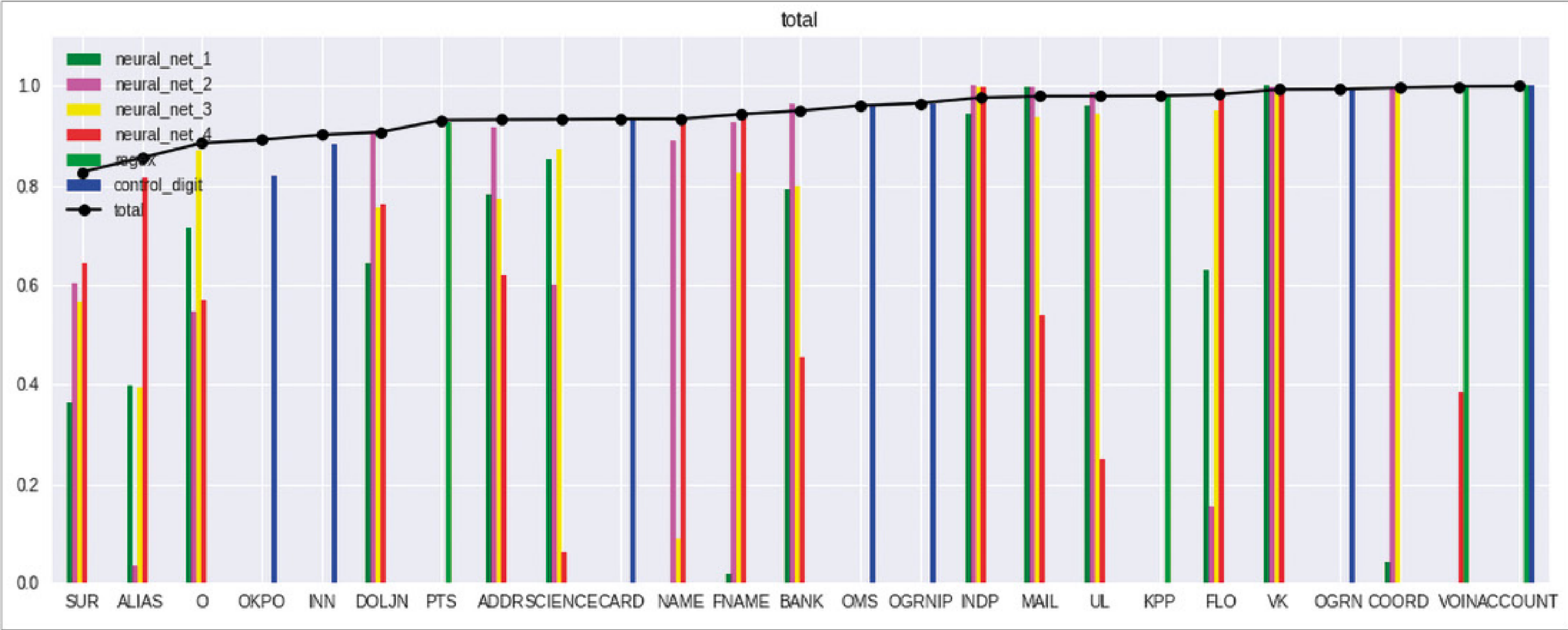


Рисунок 12. Метрики (F-меры) качества полученного алгоритма. В большинстве случаев точность всей системы выше точности используемых алгоритмов



Каждый пользователь оставил отзыв разработчику модели, в котором указал все неправильно классифицированные данные. Полученная информация помогла правильно настроить алгоритмы определения категории требуемой защиты, а также позволила дообучить нейросети и повысить качество классификации.

При промышленной эксплуатации сервиса сотрудникам компании предоставляется возможность создать заявку на проверку данных, которая исполняется автоматически. Создание такой заявки позволяет всем сотрудникам банка быстро проверить файлы, участвующие во внутрибанковском обороте. Популяризация подобных услуг департамента кибербезопасности способствует распространению киберграмотности и уменьшает риски, связанные с ненадлежащим обращением с данными.

Для сотрудников департамента кибербезопасности создан отдельный сервер проверки данных, позволяющий обрабатывать большие объёмы.

РЕЗУЛЬТАТЫ И ПЕРСПЕКТИВЫ

Объединение ансамбля нейросетей, модуля с регулярными выражениями и модуля проверки на контрольные разряды позволяет отслеживать как числовые, так и текстовые виды защищаемых данных с точностью выше 95 %. Применение справочника защищаемых данных, содержащего принадлежность к видам тайн, позволяет без отключения изменять параметры работы всей системы при изменении регулирующих их нормативных документов.

Промышленное внедрение исключило при проверке данных человеческий фактор. В результате выросла как скорость проверки, так и

её качество. Это, в свою очередь, положительно сказывается на скорости поставок данных для бизнеса, что способствует быстрой разработке и выводу банковских продуктов в промышленную эксплуатацию. Применение данного решения в качестве дополнения к DLP-системе (Data Loss Prevention — система противодействия утечкам данных) позволяет качественнее выявлять попытки нарушений и быстрее выявлять нарушителей, что повышает устойчивость организации к умышленным и непредумышленным утечкам.

* * *

Следующим шагом должна стать полная автоматизация проверки и передачи данных в Сбербанке. Для этого потребуются увеличить количество видов распознаваемых данных, а также повысить вариативность внутри каждого вида защищаемых данных, чтобы охватить как можно большее число их видов, как можно в большем количестве систем и баз данных. Чтобы достичь желаемого результата, необходимы взаимодействие и заинтересованность всех сторон, участвующих в обороте данных, анализ их пожеланий и идей. Сбор, анализ и обработка информации из различных источников значительно повысит качество распознавания защищаемых данных. Как при этом предотвратить увеличение времени работы системы? Чтобы ответить на этот вопрос, нам потребуются дальнейшие исследования и внедрение новых алгоритмов машинного обучения.

ТРЕТИЙ ПУТЬ

КАК ПРЕВРАТИТЬ ИЗДЕРЖКИ ОТ АНТИФРОД-СИСТЕМЫ В ПРИБЫЛЬ

Кибертоника и партнеры с 2015 года предоставляют платёжный и поведенческий антифрод. Есть достаточный опыт по работе с небольшими и средними заказчиками, включая банки. Хотелось бы затронуть две темы:

- ♦ во-первых, поделиться, как можно для малых и средних банков организовать актуальный конкурентоспособный антифрод, какие факторы на это влияют и,

- ♦ во-вторых, как можно превратить подразделение, которое отвечает за антифрод (это может быть информационная безопасность, риски или ИТ), в подразделение, приносящее бизнесу явную выгоду и помогает увеличить выручку.

ПОЧЕМУ НУЖНО РЕШАТЬ ПРОБЛЕМУ С АНТИФРОДОМ

Первый фактор. Если лет пять назад можно было довольно эффективно защищаться, т.к. мошенники использовали простые вещи, например, подбирали коды для карточных транзакций, то сейчас угрозы серьёзно усложнились и простыми методами с ними бороться не получается.

Второй фактор. У платежных сервисов очень сильная конкуренция и, как следствие, снижается маржинальность для транзакционного бизнеса. Это приводит к тому, что бизнесы берут на себя дополнительные риски и идут в более рискованные сегменты рынка, чем создают еще больше проблем для подразделений, занимающихся антифродом. Также, поскольку маржинальность падает, а следовательно и денег в бизнесе меньше, то и денег на решение проблемы — тоже меньше.

Кроме того, между игроками на рынке существует очень большое неравенство. Представим, что есть 10 банков и вдруг в одном из них что-то меняется. В результате этот банк довольно быстро оказывается под атакой. Мошенники концентрируют свои усилия только на нём. Ужас этой ситуации в том, что банк не сделал ничего плохого. Просто он немного «отстал» от остальных, стал временно самым слабым звеном, вот атаки и переключились на него.

К сожалению, такая картинка встречается достаточно часто, потому что банки, которые активно сотрудничают с платежными шлюзами-а-

грегаторами, подвергаются недобросовестной конкуренции, вернее встречаются с регуляторными рисками. Тот самый случай, когда платежные шлюзы, занимающиеся рискованным бизнесом, сообщают о том, что у такого-то банка есть проблемы либо регулятору (и регулятор начинает действовать по своему усмотрению), либо сообществу, в котором в том числе присутствуют недобросовестные элементы и которые занимаются противоправными действиями... и банк становится объектом атаки.

Нам кажется, что никто не хочет оказаться таким слабым звеном.

Отдельно важно отметить, что нужно нанимать людей, которые способны реагировать на сложные угрозы. И тут мы сталкиваемся с тем, что:

- ♦ во-первых, такие специалисты очень дорого стоят, т.к. рынок ИТ серьезно перегрет;

- ♦ во-вторых, найти таких людей очень сложно в принципе;

- ♦ есть и другие факторы: импортозамещение, сложности с интеграцией и т.д.

Таким образом бизнес оказывается между молотом и наковальней: с одной стороны, более сложные угрозы, уменьшение финансирования, развитие внутренней компетенции, с другой — решать эти проблемы как-то надо, потому что регулятор требует выполнения регламентирующих обязательств. И если крупные банки могут себе позволить разрабатывать собственные решения или покупать чужие, то что делать множеству малых и средних банков?

Еще одно соображение. Наверное, это грубо — оценивать возможности организации сделать хороший антифрод по объему активов, но, как ни крути, деньги помогают решать проблемы.

ЧТО ДЕЛАТЬ?

Чтобы понять стратегию решения проблемы, нужно определиться с отношением к тому, что такое антифрод для организации, где собираются решать эту проблему. Существуют два разных подхода:

- ♦ для кого-то антифрод — это просто издержки для бизнеса, и тут цели две: первая — выполнить минимум требований регулятора, и вторая — не оказаться тем самым слабым звеном;

- ♦ другой подход, когда банк считает, что антифрод — это важно, что он может нести допол-



Алексей ВОЙЛУКОВ
вице-президент
Ассоциации банков
России



Сергей ВЕЛЬЦ
технический
директор
и сооснователь
компаний
«Кибертоника»

нительные возможности для бизнеса. Например, где-то банк участвует в цифровой трансформации и система фрода становится источником информации для скоринга, для каких-то новых таргетированных предложений для клиента.

В соответствии с отношением банка к антифроду есть несколько путей решения проблемы.

Первый путь. Если организация не занимается активно транзакционным бизнесом или его уровень риска низкий, то вполне можно обойтись часто встроенными модулями антифрод-системы в ДБО или процессинге. Это нормально — такой вариант работает.

Второй путь. Крупные организации могут:

- ♦ делать in-house разработку;
- ♦ частично использовать опенсорсинг решения, которых сейчас стало гораздо больше.

Между этими двумя путями лежит **третий** — использование платформы или сервиса. При этом платформа может внедряться либо внутри банка, либо в облаке. С нашей точки зрения, платформа — самое оптимальное решение.

САМОПИСНЫЙ АНТИФРОД — ПЛОХОЕ РЕШЕНИЕ

Из практики. В 40 % случаев у банков возникает желание (особенно у цифровых банков, электронных кошельков, платежных систем) создать собственную антифрод-систему. Существует заблуждение, что сделать это достаточно просто.

Ситуация усугубляется, когда внутри есть «талантливые» разработчики, которые убеждают, что за четыре месяца напишут фрод-систему. Мы видим такое часто: в половине случаев компании выбирают этот путь, и всегда это выливается в следующую историю.

♦ Первый этап — «изобретение велосипеда» — занимает, как правило, полтора года, т.к. выясняется, что для написания этой системы нужны дополнительные компетенции.

♦ Второй этап. Написанная система — «сырая», а пользователи (фрод-офицеры) хотят иметь понятный интерфейс и не хотят настраивать систему. Также выясняется, что объем данных возрастает и требуется создать модуль отчетности, а далее еще сложнее.

♦ Заключительный этап. В какой-то момент менеджмент сталкивается с тем, что развития системы нет, т.к. антифрод-разработчики уходят, то есть носители знаний покидают компанию, и поддерживать систему становится некому.

После этого заказчик приходит к провайдеру услуг и начинает выбирать решения.

ВЫБОР: СЕРВИС ИЛИ ПЛАТФОРМА?

Важный момент: в случае с антифродом нужно отличать сервис от платформы, потому что ан-

тифрод как сервис для банков сложно сделать универсальным — у банка всегда есть масса своей специфики, свой взгляд на процессы и на то, как должен работать антифрод. Как правило банки не ищут сервис с антифродом, то есть готовое решение стандартной проблемы. Банки ищут конструктор, который могут настроить с помощью поставщика или без него. Они могут собрать решение, которые идеально подходят именно для них. Важно подчеркнуть, что для банков нужно обеспечить не только защиту какого-то платежного канала или канала ДБО, а комплексную защиту кросс-канального мониторинга. Как правило сервисы этого сделать не могут.

О ПРЕИМУЩЕСТВАХ И НЕДОСТАТКАХ ОБЛАЧНЫХ ПЛАТФОРМ

Важное преимущество облачной платформы для антифрода, как минимум на начальном этапе: данные можно обновлять каждый месяц, что очень важно для антифрода. Мошенники активно подстраиваются и обновлять антифрод два раза в год нельзя, это — не эффективно, это не работает!

Из недостатков облака:

♦ первое — проблема доверия. Игроки на рынке не доверяют друг другу, не доверяют поставщикам данных. Трудно представить, что конкурирующие между собой банки или банки, принадлежащие разным группам, давали бы друг другу антифрод (возможно, для других сервисов ИБ — это и не такая проблема);

♦ вторая проблема — обработка персональных данных и банковской тайны. Решается она путем анонимизации данных. Возможно, есть и какие-то другие варианты решения.

Важное преимущество платформы — уметь работать с данными, которые поставляют игроки рынка. Поясним, в цепочке платежа может участвовать много игроков, и каждый из них может иметь антифрод. В каждом случае могут быть внутренние нарушители и, в идеале, платформа в рамках рынка должна уметь работать со всеми участниками и обеспечивать обмен данными между участниками — как поведенческими профилями, включая транзакционные профили в обезличенном виде (с их согласия), так и данными с поставщиками внешних данных (провайдеры или регулятор).

Платформа должна обеспечивать две вещи с точки зрения интеграции:

♦ первое — сбор цифровых отпечатков устройств и поведенческих профилей, что важно для того, чтобы обнаруживать ботов, автоматизацию мошеннических платежей, а так-



же пользователей, которые активно меняют устройства, используют виртуальные машины, что актуально в большей степени для рисков IML комплаенс;

♦ второе — транзакционный мониторинг.

АНТИФРОД КАК ИСТОЧНИК ВЫГОДЫ

Практические кейсы. Первый — банк-эмитент. Была внедрена платформа антифрода для кросс-канального фрод-мониторинга. Оказалось, что антифрод в банке — уникальное место: в нем в режиме реального времени есть: 1) платежные данные, 2) поведенческие данные, 3) данные от поставщиков данных (это может быть что-то от intelligence, а может — что-то связанное с интересами пользователя, маркетинговые данные). И тут же в режиме реального времени можно применять, как минимум, бизнес-правила, а как максимум — статистические модели машинного обучения. Как результат — антифрод стал источником данных для решения задач не только кибербезопасности — подразделение, занимающееся антифродом, вышло с инициативой и получило поддержку у бизнес-подразделения. Были написаны новые бизнес-правила — стали предлагать адресные предложения клиентам в режиме реального времени. Более того, теперь бюджет антифрода финансируется другими бизнес-подразделениями банка.

Второй кейс. Банк-эквайер с достаточно большим портфелем мерчантов. И у мерчантов и у эквайеров проблема в том, что маржинальность бизнеса падает, конкуренция очень большая, т.к. эквайринг совершенно стандартная услу-

га. С внедрением системы фрода были достигнуты следующие результаты: банк был выведен из программы рисков Визы и Мастер-кард, конверсия повысилась на 4%, а количество чарджбэков снизилось в два раза — за счёт более грамотного управления: в политиках безопасности банка были сделаны изменения. Первое — по рекомендациям фрод-системы определенные транзакции были направлены не через 3D-secure, и второе — карточки иностранных эмитентов тоже принимаются.

Третий кейс — Яндекс-такси во время Чемпионата мира по футболу. Существовали риски — приедет много иностранцев, а истории платежей по их карточкам нет. Внедрение фрод-системы (за два месяца) на стороне платежного шлюза позволило оперативно отслеживать платежи, даже с учетом того, что иностранцы переезжали из города в город.

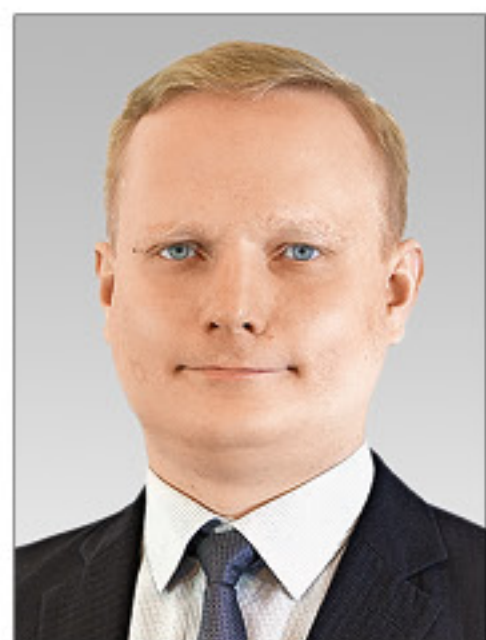
* * *

Подводя итоги, хотелось бы отметить три момента.

1. Антифродом заниматься нужно, чтобы не оказаться самым слабым звеном.

2. Малым и средним банкам для выполнения фрода нужно выбирать не сервис, а облачную платформу с инструментарием, который позволяет настроить платформу под свои правила и нюансы.

3. Антифрод может превратить издержки в прибыль за счет создания дополнительного дохода на базе исходных данных, которые получают от фрод-системы.



Евгений КАРПОВ
начальник отдела
информационной
безопасности
АО КБ «Хлынов»

РАЗУМНЫЙ КОМПРОМИСС

МЕЖДУ УДОБСТВОМ СХЕМЫ РАБОТЫ
И ОСТАТОЧНЫМИ РИСКАМИ, ОТ КОТОРЫХ
ОНА НЕ ЗАЩИЩАЕТ

Эта статья интересна тем, что представляет видение ИБ со стороны «экономичного» крыла отрасли — малых и средних банков. Не обладая избыточными средствами, безопасники, работающие «далеко от Москвы», вынуждены проявлять чудеса профессионализма, чтобы защитить свои банки и их клиентов от злоумышленников. Часто условия и инструментарий их работы значительно отличаются от передовых, читай, столичных. Тем более полезно знать, как у них получается минимумом средств достигать нужного результата. Также интересно, что статья адресована не столько коллегам-безопасникам, сколько клиентам банков.

Тема статьи: степень защищённости клиентов при работе через каналы дистанционного банковского обслуживания. Клиенты обычно мало интересуются защитой, по их мнению, она должна быть «по умолчанию». Но есть проблема: злоумышленники действуют не только на территории банков, но и на территории клиентов тоже.

Для понимания значимости проблемы с верхнего уровня рассмотрим долю несанкционированных переводов денежных средств к их общему объёму. Он установлен ЦБ РФ на уровне 0,0050% — как предельно допустимый. По сравнению с другими странами это достаточно жёсткий лимит на такие операции. По мнению ЦБ РФ, всё что ниже, не оказывает существенно негативного влияния, а если выше, то может привести к серьёзным последствиям: вынудит переходить к товарным отношениям, использованию денежных суррогатов и иных заменителей.

ЗЛОУМЫШЛЕННИКИ

Способов украсть деньги из банка сегодня не так уж и много. Это:

- ♦ взломы компьютеров клиентов, банков и отправка платежей от имени клиентов или самих банков;
- ♦ обман, выдача себя за тех, кто имеет право проводить платежи, контрагентов, руководство, технические службы — для того, чтобы заставить исполнителя ввести нужные реквизиты и отправить платёж;

- ♦ использование предоставленных полномочий и прав для личного обогащения.

Кто крадёт? Хорошо организованные группы, имеющие чёткую иерархию, специализацию, знания, специально разработанный и поддерживаемый в актуальном состоянии инструментарий. В режиме подряда они привлекают другие группы. Да, есть и уникалы-одиночки, но основной ущерб наносят именно профессионалы.

Они постоянно совершенствуют технологии и активно пользуются услугами чёрного рынка Даркнета. А там можно найти всё необходимое для полноценной кооперации, чтобы проникнуть в банк. Например:

- ♦ купить готовый рабочий инструмент для формирования заражённого вложения, которое не будет обнаружено антивирусом;
- ♦ купить список почтовых адресов сотрудников одного или нескольких банков;
- ♦ нанять группу, которая разошлёт письма с заражённым вложением по сотрудникам банка;
- ♦ а также группу, которая уговорит кого-то из сотрудников банка под благовидным предлогом открыть заражённый файл;
- ♦ а также группу, которая, получив точку входа внутри периметра банка, проведёт взлом его внутренних ресурсов и организует отставку платежа по нужным реквизитам;
- ♦ а также обнальщиков, которые, получив платёж, превратят его в наличные деньги и положат их на ваш счёт.



ТИПИЧНЫЕ СЦЕНАРИИ И ИНСТРУМЕНТЫ

Давайте рассмотрим типичные сценарии и инструменты злоумышленников, а также меры по защите от них.

1. Удалённый доступ. Злоумышленникам надо разобраться с тем, что и как устроено у клиента. И они это успешно делают. Узнают динамику платежей, вычисляют, когда есть деньги и когда их легче украсть (например, в пятницу после обеда). Как им в этом помешать? Отсутствие прямого доступа к компьютеру, где работают с Интернет-банком, значительно осложнит им хищение. Для клиента — это отдельный компьютер (например, самый дешёвый ноутбук) с отдельным каналом доступа в интернет и хорошим антивирусом, платежи на который и с которого переносят на флешке. Не гарантия безопасности, но так украсть будет гораздо сложнее.

2. Кража средств доступа или управления. Если вы не подтверждаете паролем из СМС или паролем из токена с экраном каждый отправляемый из Интернет-банка документ или пакет документов, то злоумышленник может украсть у вас токен авторизации или криптографический ключ с флешки или жёсткого диска. После этого вы и ваш компьютер ему не нужны, он просто отправит нужную платежку за вас. Лучший вариант защиты — СМС на отдельное устройство (самый простой сотовый телефон) и использо-

вание криптографического ключа на специальном носителе, не позволяющем скопировать с него ключ.

3. Компрометация средств подтверждения. Использование СМС для подтверждения операций и токенов для хранения криптографических ключей заставляет злоумышленников преодолевать и эти трудности. Где-то используется социальная инженерия. «Уговаривают», представляясь сотрудниками Банка России, правоохранительных органов или сотрудниками обслуживающего банка, но уровень бдительности сегодня повысился и такое уже редко удаётся. Поэтому прибегают к выпуску «клона» SIM-карты или заражению вашего смартфона («Перейди по ссылке, чтобы посмотреть забавные фото котиков»). Защититься от незаконного получения SIM-карты, привязанной к вашему номеру телефона, тяжело, это больше относится к компетенции служб безопасности операторов сотовой связи. Но вот использовать для защиты криптографический ключ на токене, работающем в режиме «неизвлекаемого» ключа, заставит злоумышленников действовать только тогда, когда токен подключён. Если токен выключен и убран в сейф — ничего у них не получится. Удалённо сейфы пока ещё вскрывать не научились...

4. Антивирусная защита. Сегодня все антивирусы преодолеваются. Но антивирус со свежими базами заставляет злоумышленника использовать ещё более свежий инструмент. Да, от «пер-

вой волны» заражений такой антивирус не защитит, но от «второй волны» защитит. Он заставляет злоумышленника использовать свежие средства взлома и уникальные средства сбора информации — иначе тот будет обнаружен. Для сравнения: бегать можно и с чугунной гирей в два пуда, но это тяжело, неудобно и далеко не убежишь...

5. Преодоление антифрод-систем. Волшебное слово «антифрод». Модное, актуально, дорого и специалистов на рынке нет. Только у крупных банков. Что же это такое? Система сбора информации о платежах, их предварительной оценки на базе правил и принятия решения по исполнению платежа:

- ◆ «нет подозрений или они незначительные, отправить»;
- ◆ «сомнительный, пусть клиент подтвердит, после отправить»;
- ◆ «в высшей степени сомнительный, позволить клиенту и узнать, всё ли у него хорошо? Если клиент отвечает и подтверждает платёж, то отправить»;
- ◆ «блокировать сразу, КРАДУТ!»

В реальности антифрод эффективен, когда пытаются «дёрнуть» деньги сразу, много и нагло. Он не спасает от подготовленных взломов. Но эффективен для снижения размера ущерба — можно поставить планку, выше которой кражи без подготовки не получаются. В случае предварительной подготовки злоумышленник может поднять сумму возможного ущерба, но это становится для него сложной задачей, на поток её ставить сложно.

ПОЗИЦИЯ РЕГУЛЯТОРОВ

Что нам говорят об этом «сверху»? Чтобы не завязнуть в дебрях, посмотрим только основные моменты применительно к клиентам. Основных документов по защите два:

- ◆ положение «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации» Банка России от 09.06.2012 № 382-П;

- ◆ федеральный закон «О национальной платёжной системе» от 27.06.2011 № 161-ФЗ.

Основные моменты по 382-П:

- ◆ банк может по заявлению клиента устанавливать лимиты на совершение операций клиентом (вступил в силу с 01.01.2020, можно установить лимиты на сумму операции разово или за период, время осуществления платежей, список получателей и т.п.).

- ◆ С 01.01.2020 есть три возможных технологии работы клиентов, упрощённо это:

- банк контролирует антивирус на компьютере или смартфоне клиента (актуально для мобильных приложений);
- клиент составляет документы на одном техническом средстве, а подтверждает на другом;
- клиент обеспечивает приемлемый для себя уровень риска за счёт установки лимитов на операции.

Использование систем Интернет-банкинга и мобильных приложений после аудита безопасности или сертификации.

Основные моменты по 161-ФЗ:

- ◆ Есть разрешение на официальное применение антифрод-систем банками.
- ◆ ЦБ РФ будет вести базу признаков платежей злоумышленников и доводить её до банков. Насчёт оперативности ЦБ РФ ничего не обещает. Очень хорошо, если «в течении 5 рабочих дней» уже «после того, как» мошенники осуществили попытку списания денежных средств об использованном им счёте уведомят другие банки. Высока вероятность, что это просто заставит мошенников вовремя менять реквизиты для приёма украденных денег. В случае физических лиц «чистые» новые реквизиты одной операцией не окупаются, но в случае юридических лиц окупаются легко.
- ◆ Банк вправе приостанавливать платежи до подтверждения на срок до 2-х рабочих дней, если у него есть сомнения.
- ◆ Есть официальная процедура возврата платежа, осуществлённого злоумышленниками. Для клиентов тут главное — своевременно обратиться в банк. Злоумышленники не могут мгновенно снять деньги — если клиент обратился сразу после платежа, деньги обналичить не успеют.

ТЕХНОЛОГИИ ЗАЩИТЫ

Предлагаю кратко рассмотреть, а от чего меры безопасности, используемые банками, спасают.

1. Логин — пароль. От честных людей. От злоумышленников не спасает. Это средство идентификации, а не защиты.

2. Одноразовые пароли. Можно подтвердить факт совершения действия, но не его содержание.

3. Генераторы кодов подтверждения с клавиатурой. Подтверждение факта и основного содержания действия. Более 1–2 платежей в день — очень неудобны.

4. СМС с кодами подтверждения. Подтверждение факта и, при соответствующем тексте, содержания действия. Зависит от защищённости самого технического средства. Не защищает от возможного получения дубликата SIM-карты или компрометации смартфона.

5. Криптографический ключ на незащищённом носителе. Требуется дополнительных манипуляций от злоумышленника по получению доступа к ключу. Защищает только от явного перехвата в канале связи. Чтобы было понятно, передаваемые вами в Интернет-банк данные никто, после вашего компьютера, не видит в «читаемом» незашифрованном виде и не может ни изменить, ни подменить. Ни оператор связи, ни Роскомнадзор.

6. Криптографический ключ на функциональном ключевом носителе. Надёжная защита криптографического ключа — доверенный сеанс связи с банком и подтверждение авторства. Не защищает от подмены на компьютере клиента, но жёстко фиксирует точку «приложения силы» злоумышленников (клиентский компьютер). Подтверждение факта и, с оговорками, содержания действия.

7. MAC-токены. Надёжная защита криптографического ключа, надёжное средство подтверждения содержания действия — доверенный сеанс связи с банком и подтверждение авторства и содержания, показанного на экране. Защищает от подмены на компьютере клиента.

8. Приложения на смартфонах. Сильно зависит от функционала такого приложения. Если устройство защищено, то эффект может быть сравним с MAC-токеном. Если устройство может быть заражено или периодически подключается к внутренней сети организации, уровень безопасности не повышается заметно. Если устройство сертифицировано производителем и предприняты все меры безопасности — свежая версия, устройство без ROOT-доступа, стойкий код блокировки, система отладки отключена производителем, наличие антивируса и программы удалённой блокировки/сброса смартфона, отсутствие необходимых для работы программ и т.д., — то использование достаточно безопасно.

9. Антифрод. Спасает от попыток украсть много и сразу. Сильно осложняет существенные кражи.

10. Организационные меры. Наименее используемый раздел. Кто из клиентов с ним занимается серьёзно, кроме крупных государственных или окологосударственных контор? А многое можно использовать и защитить себя от внутренних нарушителей и сильно осложнить жизнь внешним. Как правило, очень дешёвые меры (кроме отдельного рабочего места для отправки платежей в Интернет-банке), которые дают очень существенный эффект.

Примеры:

- ♦ Можно персонально разграничить зоны ответственности сотрудников: «Ты пользуешься

токеном, а ты — получаешь и проверяешь СМС с кодами».

- ♦ Гарантированно лишить возможности осуществить переводы при сомнениях в лояльности: «Токен на стол».

- ♦ Защитить себя от переводов вне обычного времени: «Токен подключаешь только когда платежи отправляешь, потом сразу же отключаешь».

- ♦ Обеспечить контроль за переводами: «Доступ на просмотр, без права отправки переводов. Проверяешь ежедневно после отправки всех переводов. Платежи до 16:00, выверка и контроль до 16:15». Да, он не защитит от хищения, но позволит своевременно поднять тревогу и с высокой вероятностью вернуть деньги — их не успеют снять.

- ♦ Висящий на стене кабинета/шкафа или лежащий под стеклом на столе список основных контрагентов, которым делают крупные переводы: наименование, ИНН и последние 4–6 цифр номера счёта. Это осложняет злоумышленнику подмену реквизитов (№ счёта или ИНН не совпал) или отправку крупного платежа себе (нет в списке).

ПРЕДЛОЖЕНИЯ ПО ЗАЩИТЕ ОТ БАНКА

1. Чего хочет банк и что он может дать по технологиям защиты. Чего мы хотим от нашего Интернет-банкинга:

- ♦ Удобства и привлекательности для клиента.
- ♦ Защищённости и однозначности для обмена с клиентом.

- ♦ Гибкости настройки и работы.

Что мы можем предложить клиенту:

- ♦ Защиту с помощью криптографических методов. По-простому: «Посередине никто не влезет. Возможно получить однозначный ответ о том, было или не было направлено/получено, подделать невозможно или практически невозможно».

- ♦ Защиту с использованием СМС-сообщений. Удобно, можно быстро проверить и подтвердить платёж.

- ♦ Использование криптографических токенов с неизвлекаемым ключом — достаточно надёжное обеспечение защиты и полное обеспечение контроля.

- ♦ Использование мобильного приложения.

- ♦ Использование лимитов на операции.

- ♦ Использование схем подписания «n из M». Т.е. не менее n подписей из M возможных.

- ♦ Списки доверенных получателей.

- ♦ Договорные схемы работы для самых сложных случаев: «Если надо по 500 платежей в час, мы найдём надёжное и безопасное для вас решение».

2. Чего хочет клиент и на что он может согласиться. Взгляд третьей стороны. Клиент хочет удобства, скорости и не хочет платить или брать на себя риски. Очень редко он хочет быть защищённым. Ещё реже он задумывается о рисках «у себя».

Банк хочет большего числа клиентов, большего числа их. Вкладывать в защиту клиентов он хочет минимум, тем более, вкладывать не на стороне банка, а в собственно защиту клиентов. Но банк вынужден навязывать клиенту более защищённые схемы работы — для минимизации своих рисков, в первую очередь репутационных, и выполнения в минимально необходимом объёме требований регуляторов.

Может показаться, что компромисс и для клиента, и для банка — это точка где-то посередине? Это было бы слишком просто. На самом деле — это область решений, которые существуют с оглядкой и на меры защиты, имеющиеся у банка, и на специфику бизнеса клиента — кому-то крайне важно оплатить товар тут же, до того, как его «перекупит» кто-то из конкурентов.

Глупо использовать одну и ту же схему работы и для школы, и для частного магазина, завода или холдинга. Для одних она будет слишком неудобной, для других — слишком небезопасной. Лучше подбирать решения исходя из специфики конкретного клиента.

К сожалению, не всегда у клиента есть своё видение мер защиты и рисков, которые он готов принять на себя — надо искать разумный компромисс между удобством конкретной схемы работы и остаточными рисками, от которых она не защищает.

А ЕСЛИ ХОЧЕТСЯ НАДЁЖНО И ЕСТЬ НЕМНОГО СРЕДСТВ?

Если у вас крупные операции, существенные остатки по счетам, высокая динамичность платежей, понимание привлекательности всего этого для злоумышленников и небольшой бюджет «на оборону». Как защищаться? Стандартные меры уже не обеспечат требуемого высокого уровня защиты, но это не значит, что от них надо отказаться — можно из базовых кирпичей построить свою «крепость», например:

- ♦ Схема подписания документов: «Под документом должны быть любые 2 разные подписи из списка».

- ♦ АРМ бухгалтера с доступом в Интернет-банк для загрузки платежей и выгрузки информации по совершенным операциям.

- ♦ Отдельный выделенный АРМ Контроля для работы с Интернет-банком — с изоляцией от остальной сети и, желательно, своим каналом

доступа — для контроля операций и осуществления второй подписи под проверенными платежами.

- ♦ Минимум 2–3, а лучше 4–5 сотрудников, и у каждого свой токен с неизвлекаемым ключом, защищённым своим паролем.

- ♦ Хороший коммерческий антивирус.

- ♦ Регламентированные процедуры контроля платежей, списки обычных контрагентов (распечатка на стене — последние цифры номера счёта и наименование), процедуры контроля операций на сумму более 100–200–500 тысяч рублей.

КАК ЭТО БУДЕТ РАБОТАТЬ?

При проникновении во внутреннюю сеть организации злоумышленники увидят АРМ Бухгалтера, увидят процесс загрузки платёжных документов и технически они могут подменить платежку. Но они не видят АРМ контроля, а если и видят, то доступ к нему для них максимально затруднён — он автономен, и канал доступа в Интернет для злоумышленников не подконтролен (чтобы не допустить проникновение заражения). «Исправленные» и «левые» платежи будут выявлены при контроле другим сотрудником на выделенном АРМ. При увольнении/командировке/больничном имеющийся «запас» сотрудников с ключами доступа позволит продолжить работу. При этом каждый сотрудник знает, что его доступ персональный, и сказать «это не я» невозможно из-за персональных криптографических ключей. Указанная схема также защитит вас и от внутреннего мошенничества и позволит в большей степени контролировать платежи.

* * *

Да, по сравнению со схемой «1–2 токена и 2–3 человека без выделенного АРМ» есть дополнительные расходы: ноутбук, модем, дополнительные 2–4 токена и дополнительные 2–4 сертификата. Но зато от хакеров вы достаточно защищены (самый лёгкий из оставшихся каналов для них — создать в системе бухгалтерского учёта платёжный документ штатными средствами) при том, что попытка шаблонного вывода средств у вас с крайне высокой степенью вероятности будет вовремя обнаружена и пресечена до списания денег со счёта. У вас будет резервный доверенный канал до банка — вы сможете работать с выделенного АРМ Контроля, несмотря на борьбу с хакерами внутри вашей инфраструктуры.



Твоя сеть. Твои правила.

Гибкая защита — для растущего бизнеса.

Kaspersky Endpoint Security для бизнеса Универсальный защитит виртуальные и физические рабочие места в любом их соотношении и поддержит ваши планы по развитию корпоративной IT-инфраструктуры.



**Kaspersky®
Endpoint Security
для бизнеса
Универсальный**

kaspersky

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



Дмитрий МИХЕЕВ
технический директор
ООО «Айти БАСТИОН»

СОТРУДНИКИ «НА УДАЛЁНКЕ»

ЧЕМ ОПАСНА МАССОВОСТЬ И ЭКСТРЕННОСТЬ СИТУАЦИИ

Традиционно финансовые компании — одни из самых технически продвинутых в ИТ и ИБ. Они владеют развитыми инфраструктурами, которые поддерживают и развивают постоянно. Это приводит к тому, что внимание к вопросам удалённого доступа — как для внутренних сотрудников, так и для внешних подрядчиков — в банковском секторе всегда сильное и не ослабевает.

УДАЛЁННЫЙ ДОСТУП В БАНКАХ: ОРГАНИЗОВАТЬ НЕЛЬЗЯ ОТМЕНИТЬ

Возможность манёвра ресурсами технических специалистов, быстрого разрешения проблем в распределённом хозяйстве банка — удобна и позволяет решать задачи бизнеса лучше.

Понятно, что этот подход имеет и недостатки: система становится зависимой от надёжной работы сетевой инфраструктуры и от внешних специалистов. Существуют значимые риски информационной безопасности, связанные с доступом в периметр. Для управления данными угрозами нарабатаны стандартные компенсирующие меры, разработаны и поддерживаются стандарты безопасности, в т.ч. по требованиям соответствующих регуляторов. Банковские организации обязаны принимать во внимание требования нескольких регуляторов, в части, их касающейся: это и вопросы, связанные с персональными данными, и меры

в соответствии с требованиями Банка России, также актуальны вопросы, касающиеся тематики ключевой информационной инфраструктуры.

Как только мы пытаемся совместить вопросы соответствия требованиям регуляторов с привычными ИТ-практиками, возникают очевидные сложности. Как минимум, это финансовые и административные затраты — процессы категорирования, аттестации, применения мер защиты не очень просты и значимо затратны. Кроме того, **требований много, они не всегда хорошо совместимы между собой и с объективной реальностью — соответственно, реально-сти приходится «подвигнуться».**

Особенно это заметно в вопросах, связанных с удалённым доступом, где требования к мерам защиты и организационному их обеспечению вырастают настолько, что первой реакцией становится — вообще закрыть все возможности работать удалённо. При этом работа с современной инфраструктурой чаще всего подразумевает необходимость дистанционного режима. Развитые инфраструктуры, как правило, большие и распределённые, а обычно ещё и зависят от той или иной платформы виртуализации, так что непосредственное взаимодействие с техникой (оборудованием) отсутствует как таковое.

Общее направление мысли регуляторов можно только приветствовать, но практическая реализация требует изрядной гибкости ума и способности так

организовать инфраструктуру и описать её формально, чтобы конфликты с формальными требованиями были минимизированы. По сути, регуляторы в мудрости своей требуют вполне разумных вещей — разделить зоны ответственности, ограничить их инструментально, контролировать исполнение и его качество по спектру параметров.

Эти вопросы очень заметны на фоне ограничений, связанных с эпидемической угрозой коронавируса, когда компании вынуждены переводить большое количество обычных пользователей на дистанционный режим работы. С 19 марта 2020 года мы наблюдаем 50 % рост заявок на организацию узлов удалённого доступа, причём эти заявки касаются массового перевода «на удаленку» рядовых сотрудников. Даже в этих условиях заказчикам необходимо обеспечить выполнение бизнес-задач.

ФСТЭК России выпустил в этой связи письмо от 20 марта 2020 г. N240/84/389, в котором, с одной стороны, привёл список рекомендаций, с другой — выставил в них дополнительные ограничения. Оказалось, что продукт СКДПУ НТ, который мы разрабатываем, «закрывает» 14 пунктов из 14-ти в рекомендациях регулятора.

РИСКИ МАССОВОЙ УДАЛЁНКИ

Вполне понятно, что резкие массовые изменения, особенно если инфраструктура и процессы ранее не были

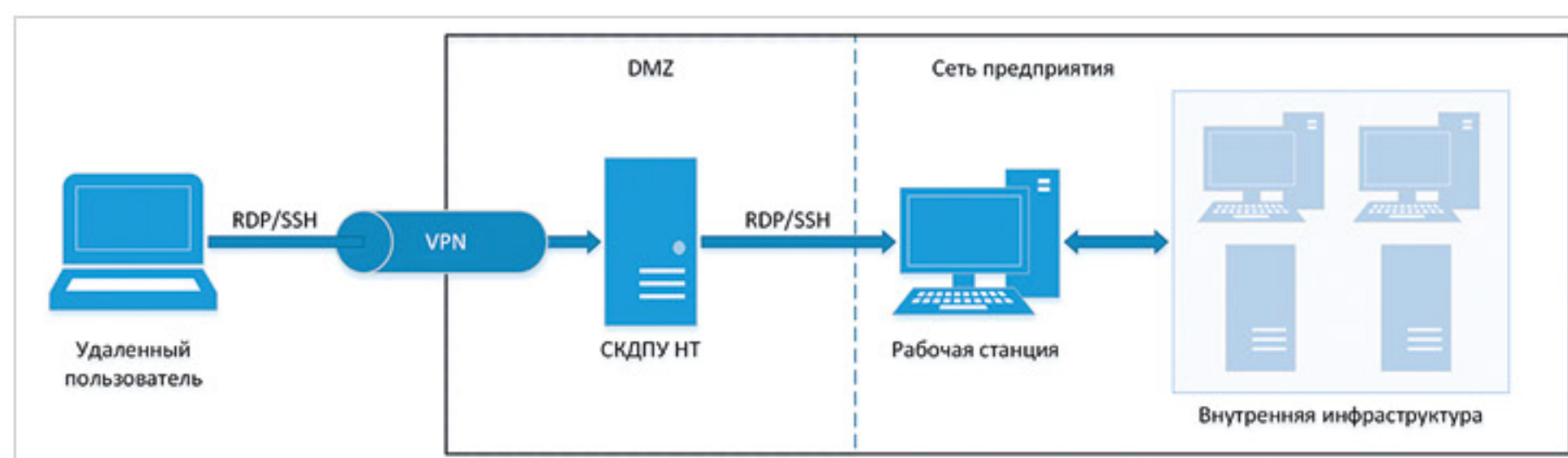


Рисунок 1. Принципиальная схема инсталляции СКДПУ НТ в сеть предприятия

подготовлены, несут серьёзные риски и надёжности, и безопасности.

Нам очень хорошо видно, практиковал ли заказчик ранее удалённый доступ для подрядчиков или части сотрудников: если да, то, по сути, компании требуется всего лишь масштабировать существующие решения или внедрить очень похожую на имеющуюся систему с минимальными изменениями. Если же ранее ничего подобного не было, приходится серьёзно вкладываться. Техническая инфраструктура требует дополнительных ресурсов и настройки, организационная часть — оформления и согласования документов.

Несомненно, массовое развёртывание удалённых рабочих мест — это серьёзное расширение периметра, влекущее за собой очевидные базовые риски. Если сотрудникам разрешается использовать собственное, «домашнее», оборудование для работы из дома — а это самый быстрый и относительно дешёвый вариант, — то требуется обеспечить соответствие этих рабочих мест стандартам безопасности — обновления для ОС, защита от вредоносного кода и т.п. Для собственного оборудования практически нереально отключить административные полномочия у пользователя, а также гарантировать нормальное развёртывание средств защиты — например, DLP.

Некоторые наши заказчики, тем не менее, вынуждены разрешать такую практику, т.к. в сложившейся ситуации с эпидемией коронавируса закупка большого количества ноутбуков не только привела к повышению цен на них, но и выбрала запасы у поставщиков, и на всех их не хватает. В результате, в ситуации экстренного перевода большого числа сотрудников на удалённый доступ подобные проблемы

усугубляются и масштабом операции — требуются дополнительные мощности на узлах доступа, резервирование каналов связи, дополнительные лицензии на терминальный доступ, дополнительные лицензии и ресурсы средствам защиты. Ответственным сотрудникам приходится решать серьёзные проблемы в сжатые сроки, перераспределяя и вводя новые мощности, договариваясь с производителем о расширении инсталляций.

ВРЕМЕННЫЕ, НО НАДЁЖНЫЕ РЕШЕНИЯ

Именно срочность запросов и желание пойти навстречу нашим заказчикам привело нас к новому опыту: мы предлагаем дополнительные лицензии в аренду на сложный период, чтобы коллеги могли выполнить свои задачи. Схема проста: мы расширяем существующую инсталляцию или проектируем совместно с заказчиком новую систему. И за день-два запускаем её для первой группы сотрудников «на удалёнке».

В текущей ситуации вопросы предоставления доступа с возможностью контроля действий внутри сессии удалённой работы позволяют закрыть внушительное количество рисков

безопасности в соответствии с требованиями регулятора — например, ограничить непосредственное взаимодействие с внутренними системами, ограничить время работы сессии, зафиксировать передаваемые данные на случай возможной проверки в будущем.

* * *

Наши решения позволяют, используя стандартные встроенные средства доступа, предоставлять возможность удалённой работы с различными информационными системами. При этом, например, мы используем собственные реализации RDP и SSH серверов, что отчасти защищает от zero-day уязвимостей соответствующих средств в среде Windows. Наши решения обращают внимание операторов безопасности на те сессии удалённой работы, которые выделяются по одному или нескольким показателям: командам, используемым приложениями, интенсивности запросов. Система реализует поведенческий анализ и фиксирует отклонения от стандартных действий, формируя с учётом уровня опасности цифровой профиль каждого пользователя. Мы обеспечиваем дополнительный автоматизированный анализ действий сотрудников на предмет аномалий, и это позволяет оператору видеть только отклонения от стандартного поведения пользователя и, таким образом, в разы сэкономить время на выявление инцидента безопасности в большом потоке действий сотрудника. Что особенно важно в условиях массового предоставления удалённого доступа.

РАЗВЁРТЫВАНИЕ СКДПУ НТ НА ИНФРАСТРУКТУРЕ ЗАКАЗЧИКА:

- ♦ Развёртывание виртуальной машины, запуск и первичная настройка — 40 минут,
- ♦ Внесение целевых учётных записей — 30 минут,
- ♦ Переключение 10 сотрудников на новую схему работы (без учёта организации VPN) — 20 минут.
- ♦ При использовании средств центральной авторизации (LDAP, например) за это время можно подключить больше сотрудников.



Екатерина СТЕПАНОВА
ведущий консультант отдела
аудита и консалтинга
ДИБ АМТ-ГРУП,
кандидат технических наук



Илья КОНДРАТЬЕВ
заместитель директора
ДИБ АМТ-ГРУП

ГОСТ ОПРАВДЫВАЕТ СРЕДСТВА?!

УПРАВЛЕНИЕ СЕТЕВЫМИ УСТРОЙСТВАМИ И ПОДСИСТЕМАМИ СЕТЕВОЙ ЗАЩИТЫ

Приближается 2021 год, а значит, и необходимость обеспечения финансовыми организациями выполнения требований ГОСТ 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (далее — Стандарт).

Стандарт разработан с целью унификации подходов к защите информации в финансовых организациях и затрагивает не только организационные, но, что немаловажно, технические меры обеспечения безопасности. Для выполнения требований к уровням защиты информации финансовым организациям уже не обойтись только «бумажными процедурами» и организационными мерами, потребуется внедрение средств защиты, а также инструментов управления ими.

НЕЛЁГКАЯ ЗАДАЧА

При ближайшем рассмотрении реализация организационных мер, определённых в Стандарте, не кажется легко выполнимой задачей и может потребовать существенного расширения штата

дорогостоящих специалистов информационной безопасности (далее — ИБ). Так, например, осуществление на регулярной основе контроля фактических параметров настроек технических мер защиты информации и информационной инфраструктуры (КЗИ.2¹) — достаточно трудоёмкий рутинный процесс. Существенно разгрузить офицеров безопасности и сфокусировать их внимание на реально важных задачах, требующих вдумчивого и ответственного подхода, позволяет использование средств автоматизации.

НУЖНА АВТОМАТИЗАЦИЯ!

В качестве примера таких средств рассмотрим системы централизованного управления сетевыми устройствами и подсистемами сетевой защиты — решения разработчиков Skybox, Tufin, AlgoSec.

Для оценки влияния внедрения данных систем на степень выполнения требований Стандарта нужно определить, какие организационные и технические требования и в каком объёме могут быть реализованы при применении средств данного класса. В По-

ложениях Банка России 672-П², 683-П³ и 684-П⁴ зафиксированы требования к уровню защиты информации (далее — УЗИ) для разных типов финансовых организаций. Так, преобладающему числу финансовых организаций, на которые распространяется действие указанных Положений Банка России, необходимо обеспечить стандартный (второй) УЗИ. Таким образом, оценка влияния внедрения на степень выполнения требований целесообразна в отношении требований, предъявляемых к стандартному УЗИ.

На рисунках 1 и 2 приведены результаты оценки количества реализуемых при внедрении систем рассматриваемо-

² Положение Банка России от 09.01.2019 № 672-П «О требованиях к защите информации в платёжной системе Банка России»

³ Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

⁴ Положение Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сферах финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

¹ Здесь и далее по тексту в скобках приведено условное обозначение меры Стандарта

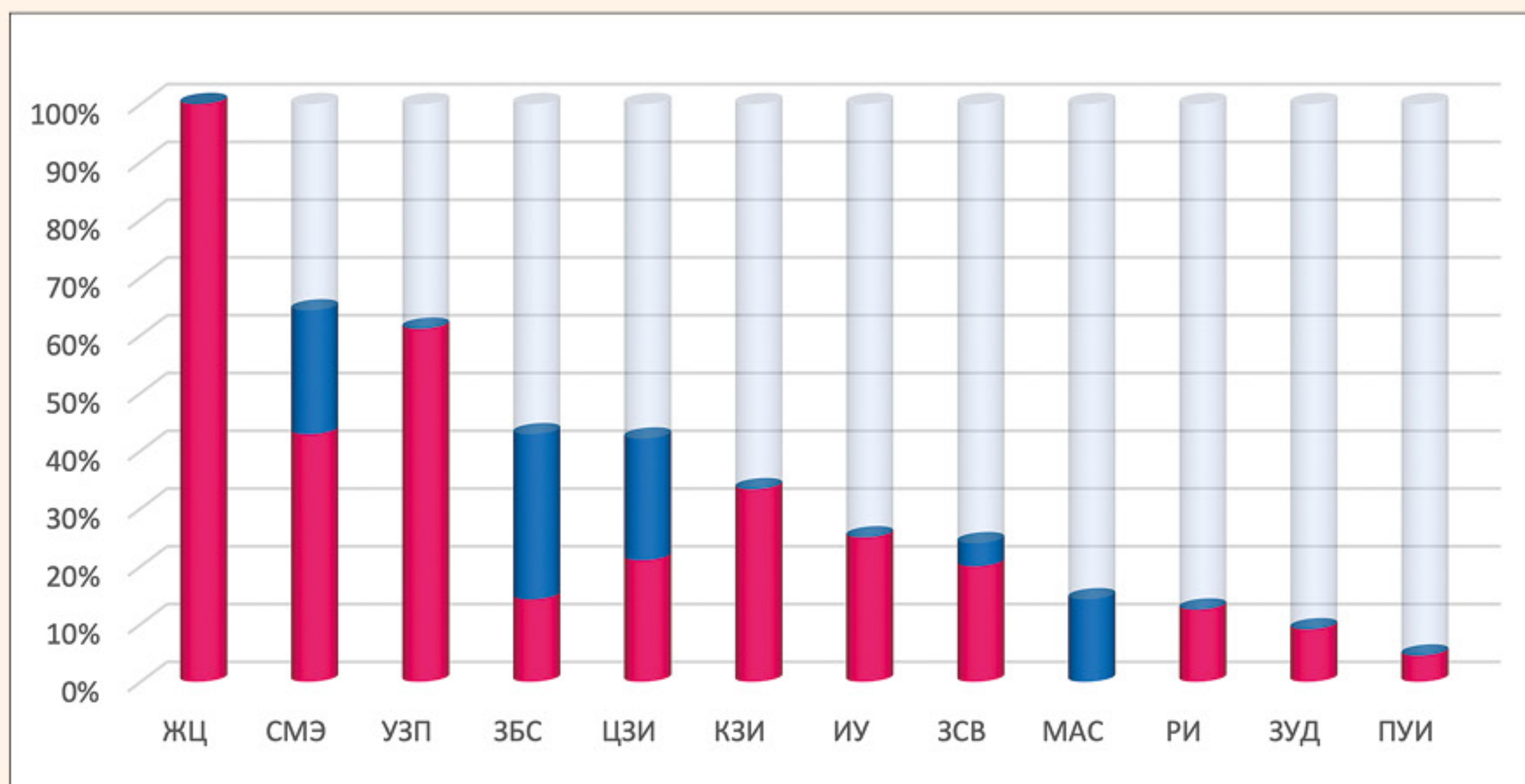


Рисунок 1. Количество технических мер, которые могут быть реализованы с использованием систем централизованного управления сетевыми устройствами и подсистемами сетевой защиты

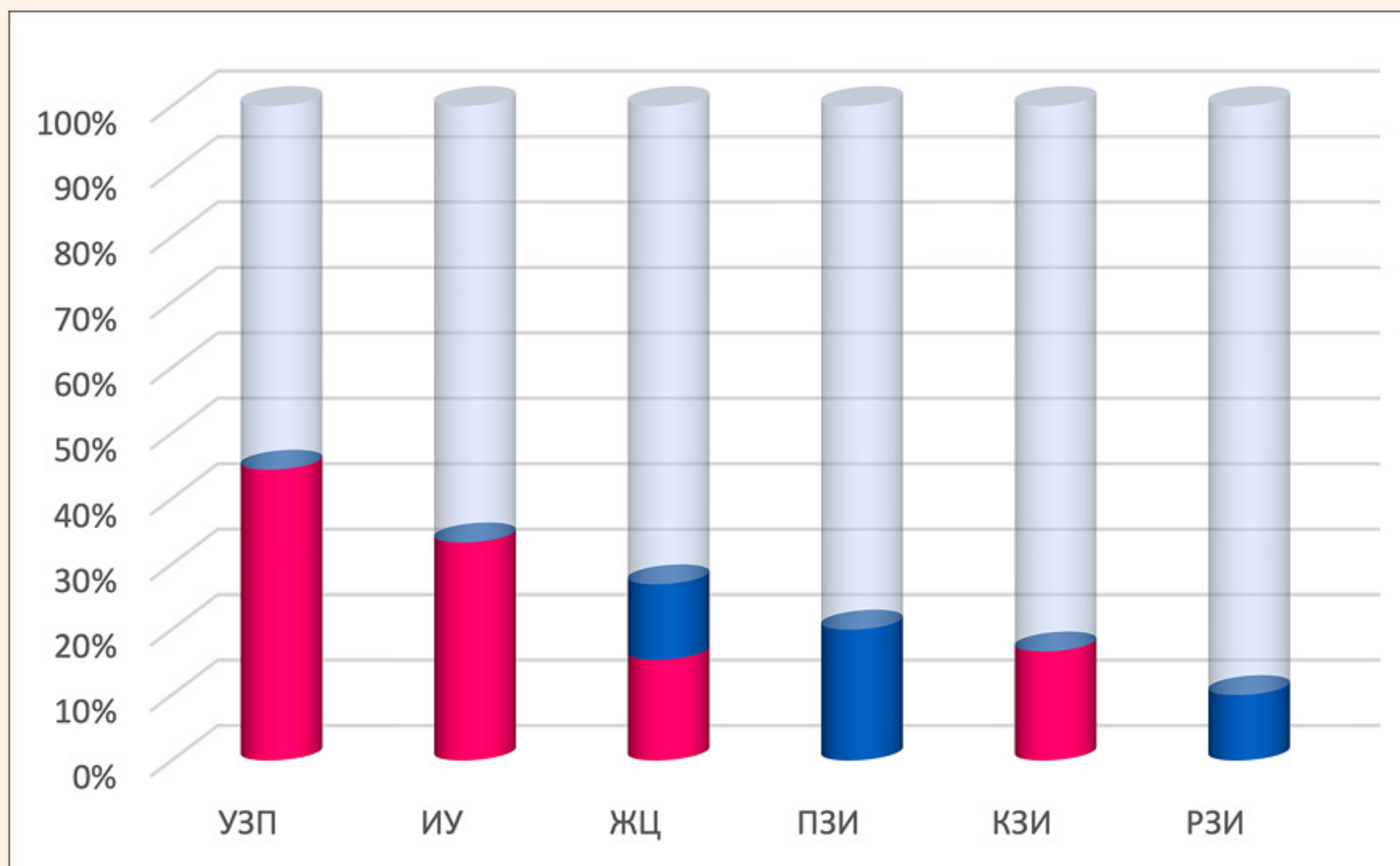


Рисунок 2. Количество организационных мер, которые могут быть реализованы с использованием систем централизованного управления сетевыми устройствами и подсистемами сетевой защиты

На рисунках приняты следующие цветовые обозначения и обозначения для доменов требований Стандарта:

■ требования Стандарта, реализуемые с использованием средства автоматизации;

□ требования Стандарта, не реализуемые с использованием средства автоматизации;

■ требования Стандарта, реализуемые с использованием средства автоматизации с ограничениями;

УЗП — Управление учётными записями и правами субъектов логического доступа;

ИУ — Идентификация и учёт ресурсов и объектов доступа;

СМЭ — Сегментация и межсетевое экранирование вычислительных сетей;

ЗБС — Защита беспроводных сетей;

ЦЗИ — Контроль целостности и защищённости информационной инфраструктуры;

ПУИ — Предотвращение утечек информации;

МАС — Управление инцидентами защиты информации;

РИ — Обнаружение инцидентов защиты информации и реагирование на них;

ЗСВ — Защита среды виртуализации;

ЗУД — Защита информации при осуществлении удалённого логического доступа с использованием мобильных (переносных) устройств;

ПЗИ — Планирование процесса системы защиты информации;

РЗИ — Реализация процесса системы защиты информации;

КЗИ — Контроль процесса системы защиты информации;

ЖЦ — Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений

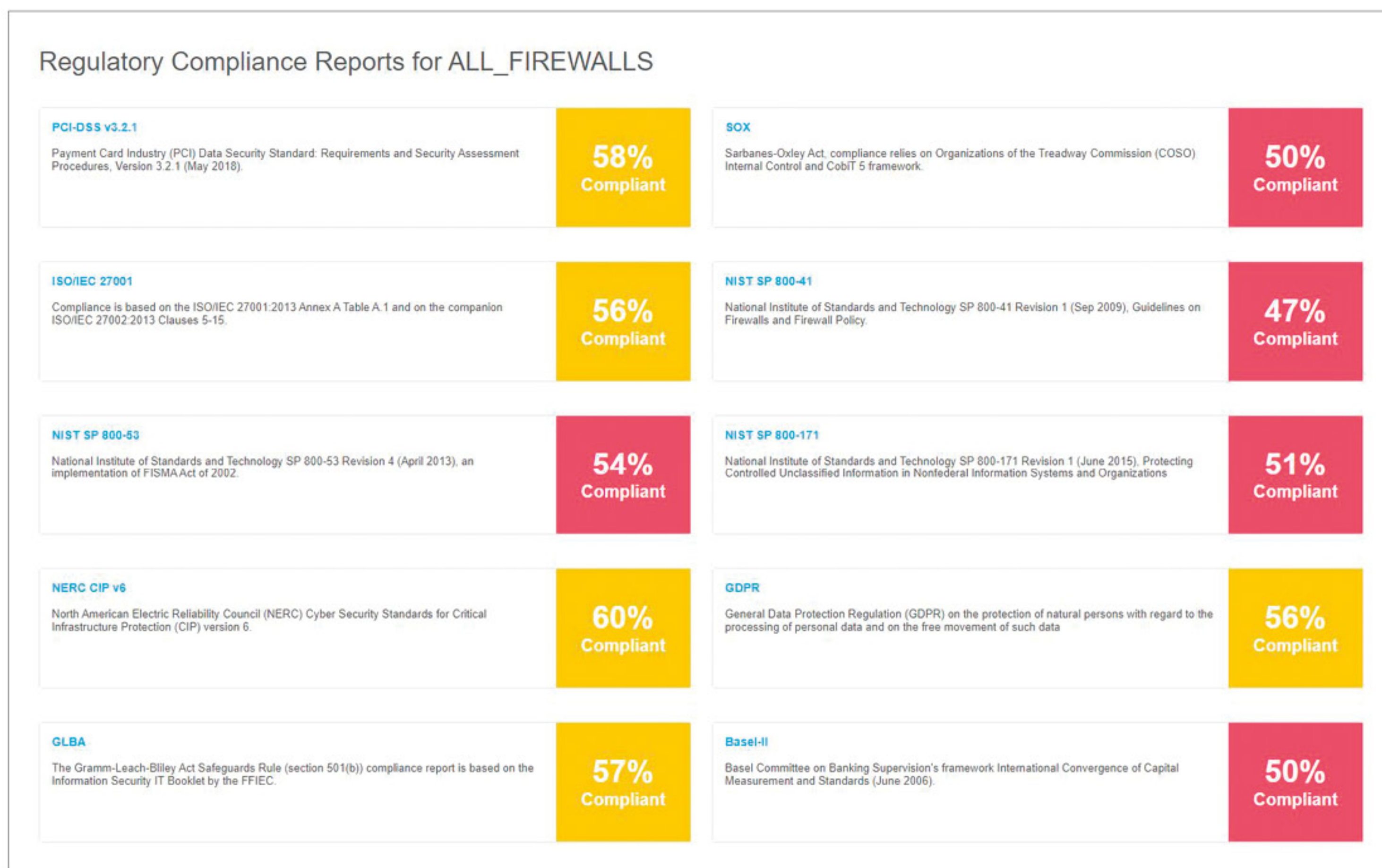


Рисунок 3. Возможные результаты автоматизированной оценки соответствия требованиям, доступные «из коробки»

го класса требований Стандарта, которые должны быть реализованы техническими и организационными мерами соответственно.

КАКАЯ ПОЛЬЗА?

Польза от применения систем данного класса для выполнения следующих требований Стандарта становится особенно очевидной при использовании в сетях крупного и среднего размера:

- ♦ реализация и контроль информационного взаимодействия между сегментами финансовой организации (СМЭ.4) и сетью Интернет (СМЭ.17) в соответствии с установленными правилами и протоколами сетевого взаимодействия;
- ♦ регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей финансовой организации (СМЭ.21);
- ♦ регистрация операций по изменению параметров настроек техниче-

ских мер системы защиты информации АС (ЖЦ.23).

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

В то же время стоит акцентировать внимание на дополнительных возможностях, появляющихся при внедрении данных решений:

- ♦ контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа (УЗП.9);
- ♦ установление фактов неиспользования субъектами предоставленных им прав доступа на протяжении некоторого периода времени (УЗП.14, УЗП.15);
- ♦ размещение и настройка (конфигурирование) технических мер системы защиты информации АС в информационной инфраструктуре, используемой для непосредственной реализации бизнес-процессов или технологических процессов финансовой организации, в соответствии с положениями проектной и эксплуатационной документации (ЖЦ.12).

ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ И ОГРАНИЧЕНИЯ

Реализация ряда требований Стандарта с использованием систем централизованного управления сетевым оборудованием и подсистемами сетевой защиты возможна при наличии дополнительных условий и ограничений. Рассмотрим типовые из них.

При условии интеграции со сканером уязвимостей системы данного класса позволяют осуществить приоритизацию работ по устранению уязвимостей. Это достигается за счёт моделирования сценариев реализации атаки, при котором во внимание принимаются открытые доступы на межсетевых экранах и актуальные уязвимости. Такой подход позволяет обеспечить оперативное устранение действительно опасных уязвимостей (ЦЗИ.4, ЦЗИ.5, ЦЗИ.6).

Вместе с тем в силу специфики, Skybox, Tufin, AlgoSec позволяют управлять только сетевым оборудованием и подсистемами сетевой защиты; не стоит ожидать от них управления хо-

стовым антивирусом. То есть данные системы позволяют осуществлять настройку (конфигурирование) технических мер защиты информации в информационной инфраструктуре (РЗИ.2) и контроль (тестирование) полноты реализации мер системы защиты информации (ЖЦ.9, ЖЦ.13) в отношении сетевых устройств и подсистем сетевой защиты.

ЕСЛИ НУЖНО БОЛЬШЕ?

Для финансовых организаций, которым необходимо реализовать усиленный уровень защиты информации, внедрение средств данного класса позволит обеспечить выполнение ряда дополнительных требований, неактуальных для стандартного УЗИ:

- ♦ реализация централизованного управления техническими мерами защиты информации (РЗИ.8);
- ♦ реализация и контроль информационного взаимодействия между отдельными пользовательскими сегментами, сегментами управления, сегментами общедоступных объектов доступа и иными сегментами вычислительных сетей в соответствии с установленными правилами и протоколами сетевого взаимодействия (СМЭ.12).

Кроме этого, системы Tufin, Skybox, Algossec поддерживают «из коробки» возможность проведения автоматизированной оценки соответствия устройств сетевой инфраструктуры требованиям PSI DSS, GDPR и др. стандартам и лучшим практикам. Это базовая функциональность систем, не требующая дополнительных настроек.

СЕТЕВЫЕ ПОТОКИ

Естественно, оценка соответствия требованиям — не единственное назначение этих систем. Многие наши заказчики решают с их помощью задачи комплексного управления информационными потоками на уровне сети.

С особенностями внедрения и некоторыми сценариями использования систем данного класса можно ознакомиться в статьях М. Ксенофонтова «Что? Где? Куда? в вашей сети» (BIS Journal № 2(33)/2019, с. 85–87) и Е. Степановой и А. Петляковой «Куда? Кому? Как? в вашей сети» (BIS Journal № 3(34)/2019, с. 60–62).

Данные системы позволяют не только предоставлять информацию, необходимую для расследования инцидентов ИБ, но и выявлять случаи неконтролируемого системой изменения сетевых доступов

Часто специалисты, отвечающие за сетевую инфраструктуру, располагают отрывочными знаниями о топологии сети, ограниченными их сферой ответственности. Без средства автоматизации не представляется возможным поддерживать в актуальном состоянии схемы сети и справочники с открытыми доступами. Ещё более нетривиальной задачей является определение информационных потоков, «скрытых» за правилами на межсетевых экранах, и выявление, какие из них нужны для решения бизнес-задач, какие уже потеряли актуальность, а какие были открыты нарушителями при реализации атаки.

Одна из систем рассматриваемого класса — Algossec — в своём составе имеет модули BusinessFlow и AutoDiscover, которые позволяют управлять сетевыми доступами для обеспечения функционирования информационных потоков бизнес-приложений. Данная цель достигается следующим образом:

- ♦ определяются и исключаются не используемые длительное время правила, конкретизируются «широкие» правила сетевого оборудования и подсистем сетевой защиты;
- ♦ после нескольких итераций текущие правила признаются легитимными, таким образом формируется baseline;
- ♦ на регулярной основе анализируются идентифицированные системой сетевые потоки; сетевые доступы, не входящие в состав легитимных и открытые без соответствующей заявки, подлежат расследованию в рамках процесса управления инцидентами ИБ.

И ИНЦИДЕНТЫ ТОЖЕ?

Все системы данного класса оперируют информацией об актуальных настройках сетевых устройств и подсистем сетевой защиты, а значит, с их помощью можно оценить сетевую доступность. Это часто востребовано при расследовании инцидентов ИБ, ког-

да в режиме реального времени необходимо оценить доступность сетевых сегментов с ключевыми информационными активами от скомпрометированного хоста.

Помимо этого, данные системы позволяют не только предоставлять информацию, необходимую для расследования инцидентов ИБ, но и выявлять случаи неконтролируемого системой изменения сетевых доступов. Так, в случае открытия нарушителем сетевого доступа на скомпрометированном межсетевом экране, системы данного класса предоставляют офицеру безопасности информацию о таких изменениях. Кроме предоставления подробной информации о внесённых изменениях, в интерфейсе систем будут сформированы рекомендации по блокированию небезопасного сетевого доступа. При условии активации соответствующих функций в системе возможно автоматизированное внесение изменений в конфигурацию управляемых устройств.

* * *

Безусловно, внедрение систем класса централизованного управления сетевыми устройствами и подсистемами сетевой защиты — непростой процесс, требующий не только модернизации систем финансовой организации, но и актуализации процессов обеспечения ИТ и ИБ. Однако использование Tufin, Skybox или Algossec даст офицерам безопасности глубокое понимание сетевой инфраструктуры, позволит контролировать все сетевые доступы, своевременно выявлять нелегитимные изменения и реагировать на них. Это повысит управляемость и защищённость сетевой инфраструктуры в целом, и в результате вы всегда сможете ответить на вопросы: Что? Где? Куда? Кому? Как? в вашей сети.



Дмитрий СУШКОВ
руководитель Службы
ИБ АО «МСП Банк»

ЦЕЛЬ ДОСТИГНУТА!

РЕШЕНИЕ SECRET CLOUD ENTERPRISE
ОТ SECRET TECHNOLOGIES ПОЗВОЛИЛО ГИБКО
ОРГАНИЗОВАТЬ ПРОЦЕСС ФАЙЛОВОГО ОБМЕНА

Хочу рассказать о внедрении в АО «МСП Банк» решения в сфере файлообмена, позволяющего обеспечить передаваемые файлы необходимой защитой, гарантировать конфиденциальность информации, контролировать и управлять процессом обмена.

Существенное увеличение объема информационных потоков в нашем кредитном учреждении между различными категориями пользователей, как между сотрудниками в пределах банка, так и между сотрудниками и клиентами сделало обмен файлами неотъемлемой частью современных бизнес-процессов. В этой связи возникает необходимость постоянного анализа ресурсов транспортировки данных в контексте обеспечения информационной безопасности, снижение рисков утечки конфиденциальной или другой важной информации.

В ходе этой работы мы обратили внимание на процесс обмена информацией с новыми контрагентами — юридическими лицами, которые еще не являются клиентами нашего банка.

В стандартном случае клиенту необходимо передавать в банк несколько десятков документов различных форматов: pdf, docx, jpeg, png. В совокупности объем этих документов составляет порядка 50 МБ, что превышает допустимый размер почтового вложения. При этом клиенты могли передавать документы в банк тем способом, который выбирали сами, в основном через Яндекс Диск, Облако Mail, Dropbox, FTP-серверы и другие средства.

Такой способ передачи информации не позволял просто запретить использование облачных или недоверенных сервисов, что создавало условия для не-

контролируемой утечки данных, снижало контроль за их обменом, повышало риск вирусных заражений.

Для минимизации угроз, эффективного управления и контроля всего процесса файлообмена, потребовалось создание единого канала получения документов от юридических лиц в рамках работы с новыми клиентами, т.е. внедрение специализированного решения, которое бы соответствовало требованиям информационной безопасности и стало для пользователей доступным и понятным на интуитивном уровне, без дополнительного обучения.

При выборе подходящего решения, с которыми предстояло работать пользователям, немаловажную роль мы отводили анализу влияния требований информационной безопасности на удобство его использования и функциональность, старались найти баланс в классическом треугольнике «Безопасность — Функциональность — Удобство».

С учетом всех этих обстоятельств было выбрано решение Secret Cloud Enterprise от российской компании Secret Technologies, ведущей разработки своих продуктов с 2012 года, специалисты которой успешно реализовали десятки проектов в области информационных технологий и информационной безопасности в различных отраслях.

Решение Secret Cloud Enterprise позволило гибко организовать контролируемый процесс файлового обмена, основанный на следующем алгоритме действий:

- ♦ внутренний пользователь запрашивает загрузку документов у клиента (контрагента) по внешней ссылке;
- ♦ клиент (контрагент) загружает документы по предоставленной ссылке.

При этом количество документов ограничено, контрагент не может перегрузить систему;

- ♦ производятся обязательные проверки получаемых документов:
 - проверка по белому списку типов файлов — контрагент может загружать только документы (не допускается наличие исполняемых файлов, медиа-файлов и т.д.);
 - антивирусная проверка файлов — для противодействия проникновения вредоносного программного обеспечения;
 - проверка на архив с паролем — если файл является архивом с паролем, файлы внутри невозможно проверить, такой архив должен быть заблокирован для загрузки.
- ♦ пользователь получает файлы, прошедшие проверки;
- ♦ передача файлов от пользователя вовне проверяется в системе через карантин вручную (файлы также могут проверяться на DLP-системе), т.к. это не является стандартным действием в рамках процесса;
- ♦ все события файлового обмена записываются в журнал и могут передаваться в систему лог-менеджмента.

Принятое решение стало эффективным инструментом для обеспечения безопасного файлообмена и удовлетворяет потребностям нашего кредитного учреждения. Цель достигнута — процесс функционирует, требования ИБ выполнены, пользователи довольны функциональностью и удобством. Дерзайте, и Вы добьетесь поставленной цели!



Владимир ВЕРЕЩАГИН
аналитик
ООО «Код Безопасности»

ПЯТЬ ВОПРОСОВ

ПРО ВИРТУАЛИЗАЦИЮ И ЕЁ ЗАЩИТУ

Несмотря на то, что существует острая потребность в отечественных информационных системах, и необходимые технические решения прорабатываются уже много лет, всё равно бытует несколько заблуждений по поводу сертифицированных средств виртуализации и особенностях их применения.

Первое заблуждение связано с тем, что если операционная система сертифицирована по требованиям защиты информации, то и все программные продукты, которые в ней есть, — тоже сертифицированы. Например, если есть калькулятор в составе системы, то он тоже прошёл контроль на отсутствие вредоносных программных закладок и что испытательная лаборатория проверила его реальные возможности на соответствие описанным в документации. В действительности, чтобы проверить код, который создавался разработчиками пять лет, надо потратить сравнимое количество времени на тестирование и изучение его работы. Поэтому проверяется даже не столько сама операционная система, сколько эффективность системы защиты, которая контролирует все возможные процессы, файлы, каналы, память, межпроцессные взаимодействия. Если такая проверка проходит успешно, то можно быть уверенным (в определённой степени, конечно), что операционная система, имея вредоносную закладку в одном из модулей, не сможет её реализовать, т.к. защитой будет перехвачено обращение к памяти, к файловой системе, к другому процессу и определено по политике безопасности — есть ли у данного модуля пра-

во на выполнение действий с объектом, или же такое право отсутствует.

Создание массовых операционных систем российского производства не пошло по пути первооткрывателей и изобретателей из-за отсутствия на это, в первую очередь, времени для разработки. В результате чего стали появляться один за другим дистрибутивы российских операционных систем: Alt Linux (на базе Mandrake Linux), Astra Linux (на базе Debian Linux), Заря (на базе CentOS Linux), ROSA Linux (на основе Mandriva Linux), MCBC (на основе Red Hat Enterprise Linux), Эльбрус (на базе Debian Linux), Аврора (на основе Ubuntu) и многие другие, уже даже отсутствующие на рынке. В части систем виртуализации такой подход тоже актуален.

Второе заблуждение кроется в том, что если какая-нибудь хорошо работающая система (например, Red Hat Enterprise Linux) прошла сертификацию (под названием MCBC), то её можно использовать также хорошо, как и в оригинальном виде. Как выясняется на практике — это не совсем так. Изменённая на свой лад система защиты, ограниченная в обновлениях и установке новых пакетов операционная система, с необходимостью сохранения целостности компонентов, не имеющая тестирования с теми сертифицированными продуктами, которые как раз и нужны, — создают сначала для проектировщика пользовательской системы, а потом и для самого пользователя множество трудно разрешимых и неразрешимых задач. За счёт этого стоимость введения в эксплуатацию продукта чаще всего вырастает, и время введения тоже. Но

при этом, если создавать и проектировать вдумчиво (с учётом особенностей и совместимости), то можно выстроить очень надёжную и безопасную систему.

Вопрос первый: можно ли купить систему виртуализации с сертификатом ФСТЭК?

На сегодняшний день есть одно сертифицированное средство аппаратной виртуализации (гипервизор), разработанный всероссийским институтом экспериментальной физики города Саратова. Сертификат ФСТЭК № 4056.

А так как количество экземпляров ограничено тремя сотнями, то перейти на него удастся только ряду проектов, проводимых в госкорпорации «Росатом», под эгидой которой работает саратовский институт экспериментальной физики.

Остальные гипервизоры, включая ESX/ESXi компании VMware, Hyper-V фирмы Microsoft или же KVM от консорциума фирм Intel, HP, Red Hat и IBM сертификацию не проходили. В т.ч. и разработчики операционной системы Astra Linux сообщают, что платформу виртуализации они не сертифицировали, но уверенно защищают.

Таким образом, фактически, сертифицированных систем виртуализации сейчас на рынке нет. В том числе и потому, что Федеральная служба по техническому и экспертному контролю не так давно выпустила новые требования (утверждены Приказом № 131 от 30.07.2018 г.) к разработке безопасного программного обеспечения и они предполагают детальный разбор заимствованного исходного кода уже даже не испытательными лабораториями, а в первую очередь производителями.

И, если саму систему виртуализации сертифицировать довольно сложно, то защиту информации к ней много проще. И они есть на рынке.

Вопрос второй: можно ли покупать иностранные программы, если нужно использовать российские?

Национальная программа «Цифровая экономика» не предполагает 100% перехода на отечественные продукты даже в госструктурах. Более того, к 2024 году планируется, что они должны будут использовать программные продукты не менее, чем на 90% российского производства.

Фактически это означает, что как минимум 9% продуктов могут быть иностранного производства. Например, если один гипервизор компании VMware будет поддерживать работу 98 виртуальных машин, работающих с гостевыми российскими операционными системами Astra Linux, ROSA, Alt Linux, Эльбрус и другими, а сам будет защищён средством vGate, то доля зарубежной продукции составит 1%. Что более чем соответствует требованиям законодательства.

Вопрос третий: какая система виртуализации более производительна — VMware или KVM?

Ответ на этот вопрос — тот редкий случай, когда лучше привести таблицу со значениями (таблица 1).

Из таблицы видно, что последние версии KVM в чём-то уступают VMware, но это скорее информация для проектировщиков. Экономистам будет интереснее узнать цену вопроса.

Программный продукт	vSphere 6.7	ПК «Брест»
Производитель	VMware	РусБИТех
Аппаратный гипервизор	ESXi	KVM
Средство управления гипервизором	vCenter	Virtual Manager
Стоимость		
для 6 процессоров	\$ 576,96 ¹	
ОС СН + 25 ВМ	–	380 000 ² руб.
дополнительные 25 ВМ	–	150 000 руб.
тех. поддержка на 1 год		~ 100 000 руб.
СЗИ НСД vGate Standard	389 075 руб.	0
СЗИ НСД vGate Enterprise	533 075 руб.	0
СЗИ НСД vGate Enterprise Plus	857 075 руб.	0

¹ Включает техническую поддержку на 1 год, средство управления vCenter и работу 3-х серверов до 2-х процессоров на каждом

² В стоимость входит ОС СН Astra Linux 1.6 ФСТЭК. Отдельно она стоит 24 900 руб. + техническая поддержка для сервера на год 62 100 руб.

Таблица 2

Финансовый вопрос: какая защищённая система наиболее выгодна по цене?

Всё зависит от того какую защиту использовать. KVM как таковой много дешевле, чем продукты компаний VMware или Microsoft, потому что может распространяться и бесплатно. Но защита к ней будет стоить денег и довольно больших.

Возьмём, к примеру, виртуализацию на базе защиты Astra Linux и на базе vGate. Производитель Astra Linux выполняет расчет стоимости, зависящий от числа виртуальных машин, не обращая внимание на производительность сервера. VMware считает в процессорах, не обращая внимание на количество виртуальных машин (таблица 2).

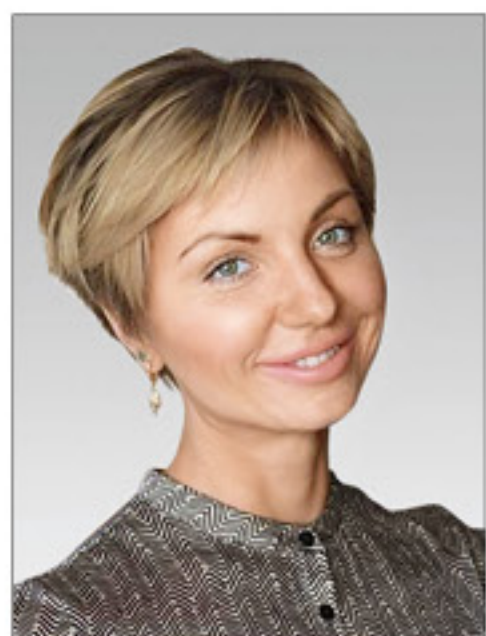
Не так просто сравнить что дороже, но можно это сделать так: если у пользователя есть 3 сервера, на которых он собирается запустить по 250 виртуальных машин, то за vSphere + vGate он заплатит максимум 900 тыс. руб. А за БРЕСТ + Astra Linux 5,2 млн руб. При этом, используя продукт VMware он может увеличить количество машин ещё на 2322 единицы. А с Astra Linux нет, потому что каждый сервер KVM более 250 штук не поддерживает. И платить в РусБИТех надо не за процессор, а за виртуальную машину. И тогда ему понадобится поставить дополнительно ещё ~9 таких серверов с Брестом. Каждый, получается, примерно по 1,7 млн руб. А вместе получается 20 млн рублей.

Вопрос перспективы: стоит ли в ближайшие годы ожидать сертифицированную систему виртуализации KVM?

С точки зрения разработчиков защищённых ОС — скорее всего нет. Т.к. продукты виртуализации они не развивают сами, а пользуются результатами консорциума, включающий в себя IBM, Red Hat, Intel, HP и другие компании. И в то время как последние вкладывают средства для увеличения производительности и оптимизации в работе виртуальной инфраструктуры, российским разработчикам на это ресурсов не хватает. И если они могут обеспечить работу новой версии в защищённом исполнении, то нет необходимости вкладывать деньги в пересертификацию.

Программный продукт	vSphere 6.7	RHEV 4.3
Производитель	VMware	Red Hat
Аппаратный гипервизор	ESXi	KVM
Количество ВМ на гипервизоре	1024	250
Количество [виртуальных] ядер/поток	768	768
Количество [виртуальных] ядер/поток в 1-й ВМ	256	384
Оперативная память гипервизора, Тб	16	12
Оперативная память на 1 ВМ, Тб	6	4
Средство управления гипервизором	vCenter	Red Hat Virtual Manager
Число управляемых ВМ	35 000	4000
Число управляемых гипервизоров	7000	400

Таблица 1



Татьяна СТАНКЕВИЧ
менеджер по продукту
ООО «Код безопасности»,
кандидат технических наук

ЗДОРОВО-е ПИТАНИЕ В ОБЛАКЕ

ЗДОРОВАЯ И БЕЗОПАСНАЯ ИНФОРМАТИЗАЦИЯ
ИЛИ КАК СЕБЯ НИ В ЧЁМ НЕ ОГРАНИЧИВАТЬ

В последние годы ФСБ России, ФСТЭК России, Центробанк были озабочены вопросами практического обеспечения информационной безопасности, а результатом их деятельности стали изменения и расширение основополагающей нормативно-правовой базы, регламентирующей это направление. Итак, требования к бизнесу становятся всё жёстче, штрафы существеннее (например, 405-ФЗ от 02.12.2019 года устанавливает штраф для юридического лица за первичную утечку персональных данных (ПДн) в размере от 1 до 6 млн руб., а за повторную — от 6 до 18 млн руб.). И в таких условиях должны существовать не только субъекты крупного, но и среднего, среднего бизнеса, ведь именно они, зачастую, используются как промежуточные звенья для проникновения в инфраструктуру денежных или обладающих важными данными игроков. Как же быть, если субъект критической информационной инфраструктуры (КИИ), оператор ПДн или субъект, чья информационная система отнесена к категории «государственная» (взаимодействует с государственной) не может по каким-либо причинам (малые бюджеты, нехватка квалифицированных сотрудников, сложности с арендую-

емыми площадями и пр.) развернуть необходимую и достаточную систему информационной безопасности? Ответом является использование защищённых облаков.

ВИРТУАЛИЗАЦИЯ — ЭТО НЕ ОБЛАКО

В своей рабочей деятельности нам часто приходится сталкиваться с ошибочным убеждением, что виртуализация — это и есть облако. Несмотря на то, что технологии виртуализации являются ключевыми для облачных сервисов, между облаками и виртуализацией нельзя ставить знак равенства: просто развернув гипервизор на сервере, вы ещё не получите облако.

Публичные и частные облака появляются там, где пользователю доступны автоматическое предоставление сервисов и масштабирование инфраструктуры. При этом частное облако, в отличие от публичного, предполагает, что ресурсы используются одной ор-

ганизацией и полностью изолированы от других, а это позволяет обеспечить более высокий уровень безопасности и надёжности системы в целом. Если эту самую изоляцию дополнить наложенными сертифицированными средствами защиты информации, то такое облако может стать полноценной заменой собственной инфраструктуры для предприятий, подпадающих под российское нормативно-правовое регулирование в области информационной безопасности.

Можно провести аналогию для виртуализации и облака на понятном для всех примере. Молодая пара увлечена правильным питанием и дотошно следит за калорийностью съеденного. У них строго определено время приёма пищи и просчитана энергоёмкость. У неё фитнес-рацион, который готовит компания «Женская радость», у него — рацион набора массы от компании «Брутальный мужчина», и если за завтраком кто-то из них не наел-

Несмотря на то, что технологии виртуализации являются ключевыми для облачных сервисов, между облаками и виртуализацией нельзя ставить знак равенства: просто развернув гипервизор на сервере, вы ещё не получите облако

Проблема небольших банков, мелкого ритейла, медицинских организаций, связанная с непосильными инвестициями в соответствие нормативке, сводится к аренде ресурсов в облаке

ся своей порцией, то придётся жить с чувством голода до обеда (а может и до ужина); он не претендует на её порцию, она не лезет к нему в тарелку. Пища есть, но она от конкретного производителя и ограничена по калорийности. Так и с виртуализацией: ресурсы выделены, но они строго ограничены. Масштабирование возможно только при условии закупки дополнительных вычислительных мощностей (перехода нашей пары на более калорийный рацион или выбора другого поставщика).

В отличие от виртуализации, ресурсы облака не ограничены. Здесь примером послужит человек, который абсолютно ни в чём себе не отказывает, ест всё подряд, когда захочет и сколько захочет. Вспоминается анекдот: «Ты же говорил, что увлекаешься здоровым питанием, а сам ешь всё подряд. — Да! А разве это неЗДОРОВО?» Т.е. в облаке, если израсходованы ресурсы одного виртуального сервера, то нагрузка переносится на менее загруженный, а процессорные ресурсы, оперативная память, дисковое пространство между этими серверами перераспределяются автоматически.

БЕЗОПАСНОСТЬ ПРЕВЫШЕ ВСЕГО

Однако, несмотря на то, что виртуализация и облако — это разные сущности, обеспечение информационной безопасности является актуальным для обеих. На сегодняшний день существует ряд продуктов, которые решают задачи защиты среды виртуализации, и, следовательно, облаков от специфичных угроз. При этом часть таких угроз может быть нивелирована организационными мерами, а часть только техническими, например, угроза выхода процесса за пределы виртуальной машины.

Стоит отметить, что несмотря на возможность защиты информационных ре-

сурсов организационными мерами, существует и человеческий фактор, когда, в силу усталости или невнимательности, ответственный за безопасность может упустить и не выполнить ряд требований регулятора. Но даже если ничего не было упущено, то изменение регуляторных норм потребует и обновления предпринятых ранее организационных мероприятий, что повлечёт пересмотр отдельных устоявшихся бизнес-процессов компании. Применение же технических средств избавит бизнес от этих операций, поскольку задача выполнения требований регулятора является прерогативой конкретного вендора, а сами изменения воплотятся в обновлении эксплуатируемого продукта и не затронут корпоративных процессов и регламентов.

ОБЛАКА — КАТАЛИЗАТОР ЭКОНОМИКИ

По сути, переход или начало работы в облаках для малого и среднего бизнеса — это возможность. Возможность для нового бизнеса быстрее окупить себя, а функционирующего — сократить текущие расходы, повысив эффективность производственной деятельности, и соблюсти при этом все законодательные требования. Т.е. облака являют собой некий катализатор развития экономики страны.

А если наш мелкий и средний бизнес подпадает под действие законов 152-ФЗ, 187-ФЗ (а ведь сегодня огромное число субъектов КИИ находятся в руках частного бизнеса), приказов ФСТЭК, как быть в таком случае? Ответ — выбирать операторов IaaS, SaaS, PaaS, которые могут предоставить в аренду облака, соответствующие требованиям нормативно-правовых актов Российской Федерации, что подтверждено результатами аттестации. Таким образом, проблема небольших банков, мелкого ритейла, медицинский орга-

низаций, связанная с непосильными инвестициями в соответствие нормативке, сводится к аренде ресурсов в облаке.

Сегодня рынок IaaS, PaaS, SaaS стимулирует формирование новых бизнес-моделей: компании арендуют инфраструктуру или сервисы у облачного оператора, внося годовой или месячный платеж за пользование, а облачный оператор, в свою очередь, сам инвестирует в закупку всего необходимого или имеет договора на аренду программно-аппаратного обеспечения также на основе периодических платежей в адрес поставщиков, что удобно во всех смыслах и первым, и вторым, и третьим.

На текущий момент времени мы совместно с партнёрами ведём работу над созданием нового продукта — защищённого частного (рисунок 1) и публичного облаков, которые смогут быть аттестованы под обработку ПДн, а также субъекта ГИСов и КИИ. В таких облаках будут соблюдены все требования российского законодательства в части обеспечения информационной безопасности. Сам продукт на основе абонентской платы будет предоставлять компаниям в пользование выделенные ресурсы, ограниченные сущностями, вошедшими в аттестацию облака, включая все их разнообразие и вычислительные мощности.

ЧТОБ И ПОЛЬЗОВАТЕЛЮ, И ВЕНДОРУ БЫЛО ХОРОШО

Глобальная информатизация нашей жизни требует определённых действий и в направлении автоматизации защиты облачных инфраструктур, поскольку все причастные могут наблюдать насколько они становятся сложными и масштабными. А эта сложность приводит к тому, что администратору(ам) облака, да и корпоративному центру обработки данных становится нереально отслеживать ежедневный рост информационно-технологической виртуализированной инфраструктуры и контролировать корректность настроек средств обеспечения её безопасности. И, руководствуясь принципом: вендор знает, как настроить разработанное им программное обеспечение (ПО), но не знает, что конкретно нужно пользовате-

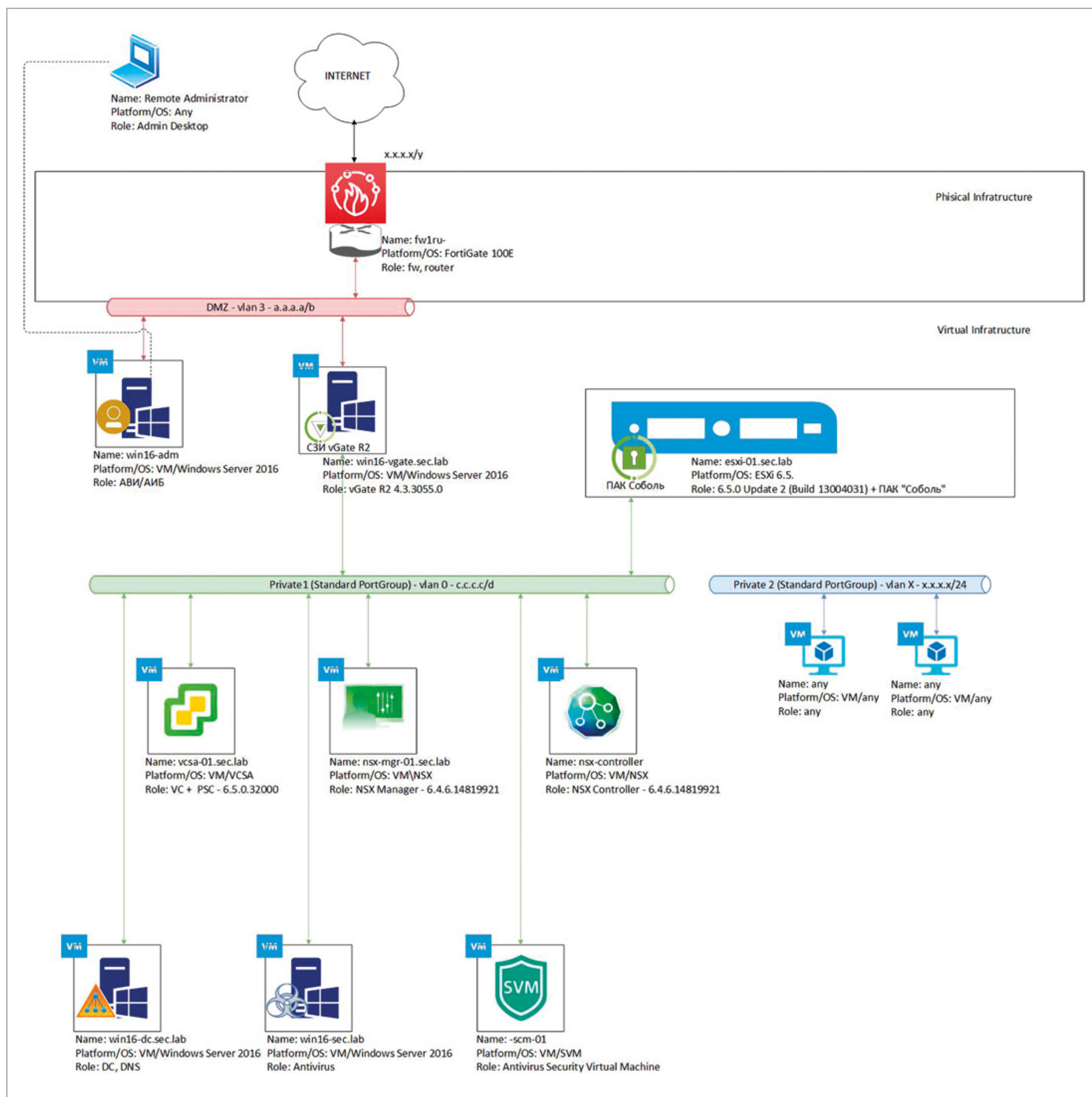


Рисунок 1. Защищённое частное облако

лю; пользователь знает, что ему нужно, но не знает, как это настроить в приобретённом ПО, — мы видим выход в автоматизированном выполнении ряда функциональных возможностей ПО.

Для нашего решения по защите среды виртуализации, которое войдёт в новый продукт защищённых облаков, одним из приоритетных направлений развития мы видим machine learning (ML). Эта технология позволит нам

по результатам выполненных сканирований виртуальной инфраструктуры представлять администраторам облака актуальную информацию о ней и предлагать наиболее подходящие конфигурации ПО защиты (на основе имеющихся в своей базе данных либо генерируемых алгоритмами ML), а человек, на своё усмотрение, будет решать, что применить в действие, а что отклонить.

* * *

И, в завершение, хотели бы пригласить всех желающих в нашу правильную облачную демо-зону! Мы уверены, что Вы останетесь довольны возможностями и условиями подобного подхода к развитию или модернизации информационно-технологической инфраструктуры Вашего предприятия.



Иван ЛОПАТИН
технический эксперт
АО «ДиалогНаука»

СИСТЕМА ПОД КОНТРОЛЕМ

АВТОМАТИЗАЦИЯ КОНТРОЛЯ РАБОТОСПОСОБНОСТИ SIEM-СИСТЕМ

Сейчас трудно представить себе отдел информационной безопасности, в арсенале которого нет SIEM-системы для выявления инцидентов информационной безопасности и оповещения.

В эпоху развивающейся эпидемии множество компаний стараются подключить к своим SIEM-системам как можно больше региональных источников — для контроля за всеми действиями пользователей в сети. Большинство крупных компаний переводят своих подчинённых на удалённую работу из дома, что неминуемо увеличивает нагрузку на коммуникационное оборудование и другие сервисы. Все эти действия неминуемо увеличивают поток событий, направленный на SIEM-системы, мощностные ресурсы которых не безграничны.

Для контроля за состоянием SIEM-системы необходимо иметь штат сотрудников, которые должны на постоянной основе снимать метрики и ана-

лизировать их изменения, чтобы увеличивающийся поток событий не вывел из строя всю систему. Сбор и анализ метрик является сложной и кропотливой работой, требующей определённых знаний пороговых значений, таких как: количество tcp-соединений с ОС, количество соединений с базой данных, состояние потоков в jvm, утилизация памяти правилами и многие другие, чтобы можно было в любое время получить реальную картину нагрузки всех компонентов SIEM-системы.

Системным администраторам и инженерам, ответственным за SIEM-систему, приходится вручную анализировать и делать выводы о её работоспособности. Зачастую по тем или иным проблемам приходится обращаться к производителю за поддержкой, где, проходя через ряд стандартных вопросов и действий, вендор предлагает ряд решений для стабилизации ситуации, которые не всегда приводят к моментальным резуль-

татам. Бывает и так, что специалисты вендора сильно загружены и не дают ответы на вопросы так быстро, как бы того хотелось.

Некоторые проблемы приводят даже к полной остановке сервиса или остановке приёма событий SIEM-системой. На рисунке 1 приведён пример, как SIEM система ArcSight была перегружена большим количеством tcp-соединений и её сетевой интерфейс был не готов принять такой объём сессий.

Для эффективного мониторинга своей SIEM-системы вы должны обратить внимание на мониторинг следующих метрик:

- ♦ метрики нагрузки на корреляционное ядро;
- ♦ метрики нагрузки на агрегационное ядро;
- ♦ метрики работы внутренних ресурсов базы данных;
- ♦ метрики работы базы данных;
- ♦ метрики поступающего потока событий;

- ♦ метрики состояния работы операционной системы;
- ♦ метрики состояния работы дисковых накопителей;
- ♦ метрики утилизации процессорного времени;
- ♦ и др.

Сейчас мы постараемся на примере SIEM-системы ArcSight показать, как те или иные метрики сказываются на её работе.

НАГРУЗКА НА КОРРЕЛЯЦИОННОЕ ЯДРО

Создание некорректных правил корреляции и их применение на большом потоке событий могут привести к ряду проблем, таких как:

- ♦ очереди в корреляционном ядре в части «застревающих» потоков (thread-ов), попавшие в статусы WAITING или SLEEP по той или иной причине;
- ♦ высокая утилизация памяти в базе данных CORR-E и JVM (java virtual machine);
- ♦ увеличение времени выборки событий из базы данных из-за переполнения буфера или превышения количества потоков к ней.

ОПРЕДЕЛЕНИЕ НАГРУЗКИ НА АГРЕГАЦИОННОЕ ЯДРО

Настройка агрегации событий является необходимой и обязательной процедурой для снижения нагрузки, но выставление неправильных значений ведёт к:

- ♦ недостижению порога событий или времени агрегации;
- ♦ превышению порога по поступлению событий или времени.

Неправильно настроенная агрегация также расходует ресурсы SIEM-системы или ее компонентов и в пиковых значениях нагрузки может привести к просадкам производительности.

ОПРЕДЕЛЕНИЕ РАБОТЫ ВНУТРЕННИХ РЕСУРСОВ БАЗЫ ДАННЫХ

Создавая внутренний контент (правила, фильтры, списки/листы), мы не задумываемся о нём, а иногда и вовсе забываем, что создавали. Неучтённый, забытый контент, а именно правила, листы и другие компоненты также потребляют ресурсы и способны пагубно отразиться на производительности

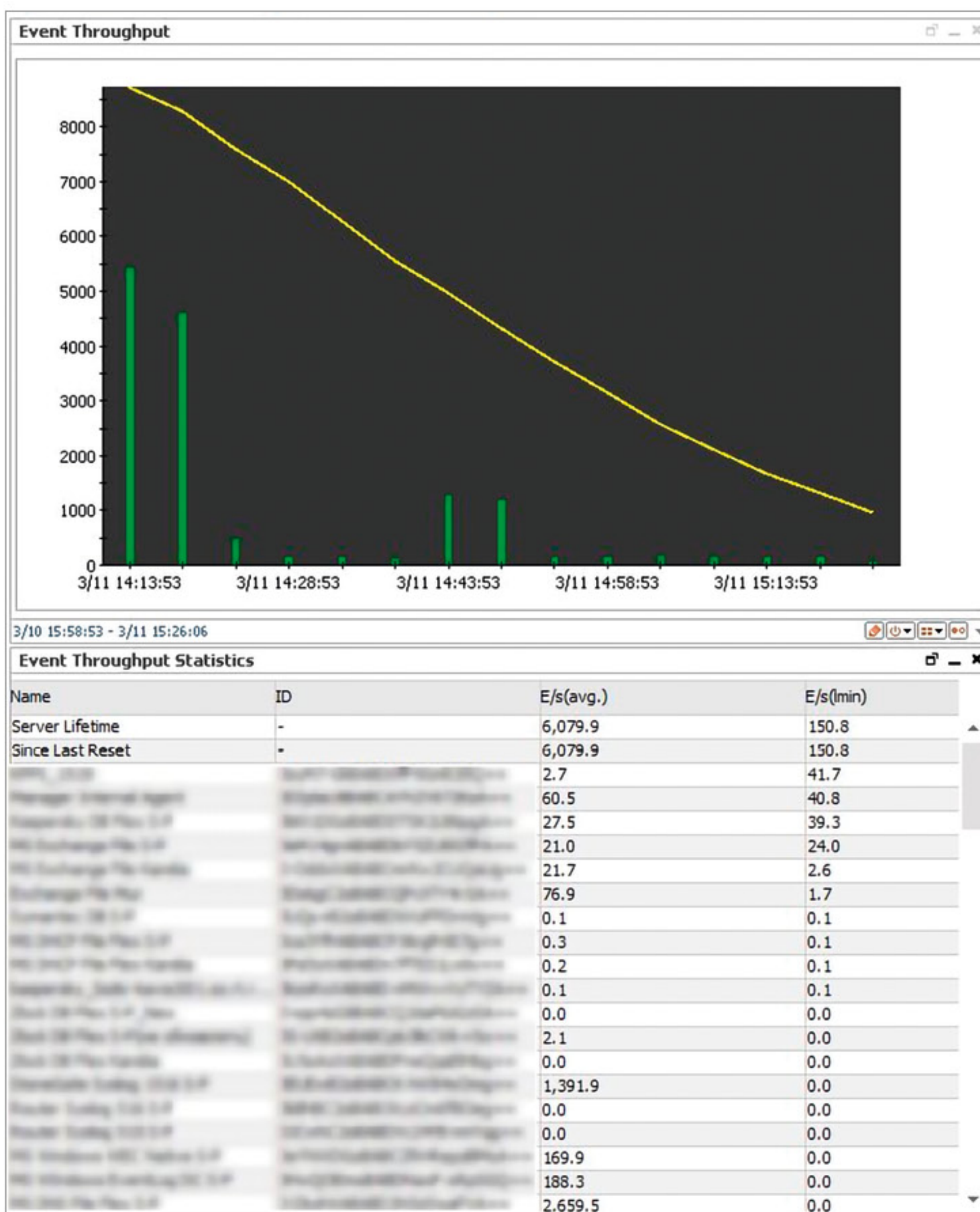


Рисунок 1. Перегрузка SIEM-системы ArcSight большим количеством tcp-соединений

SIEM-системы. Мы приведём два примера, которые снижают производительность SIEM системы ArcSight:

1. Переполненные активные листы — это происходит в случае указания неправильного TTL (time to live — время жизни событий) в активных листах при количестве поступающих записей в лист больше, чем освобождающихся событий по истечении времени.

2. Правила корреляции с большим показателем «Partial Matches» — говорит о необходимости пересмотра правила корреляции.

Все описанные выше метрики и параметры подтолкнули нас к созданию программного комплекса по анализу работоспособности SIEM-систем для

увеличения скорости реакции на изменившиеся метрики и снижения собственных трудозатрат.

КОРОТКО О НАШЕЙ СИСТЕМЕ

Система анализа работоспособности SIEM состоит из набора компонентов, которые позволяют ей эффективно контролировать метрики и события:

- ♦ модуль сбора событий — обладает механизмами сбора событий и метрик, как в агентском режиме, так и без него;
- ♦ модуль обработки и обогащения событий — обладает механизмом парсинга событий SIEM-систем и обогащения их необходимой информацией для дальнейшего реагирования;
- ♦ база данных — необходима для хранения и анализа метрик, а также

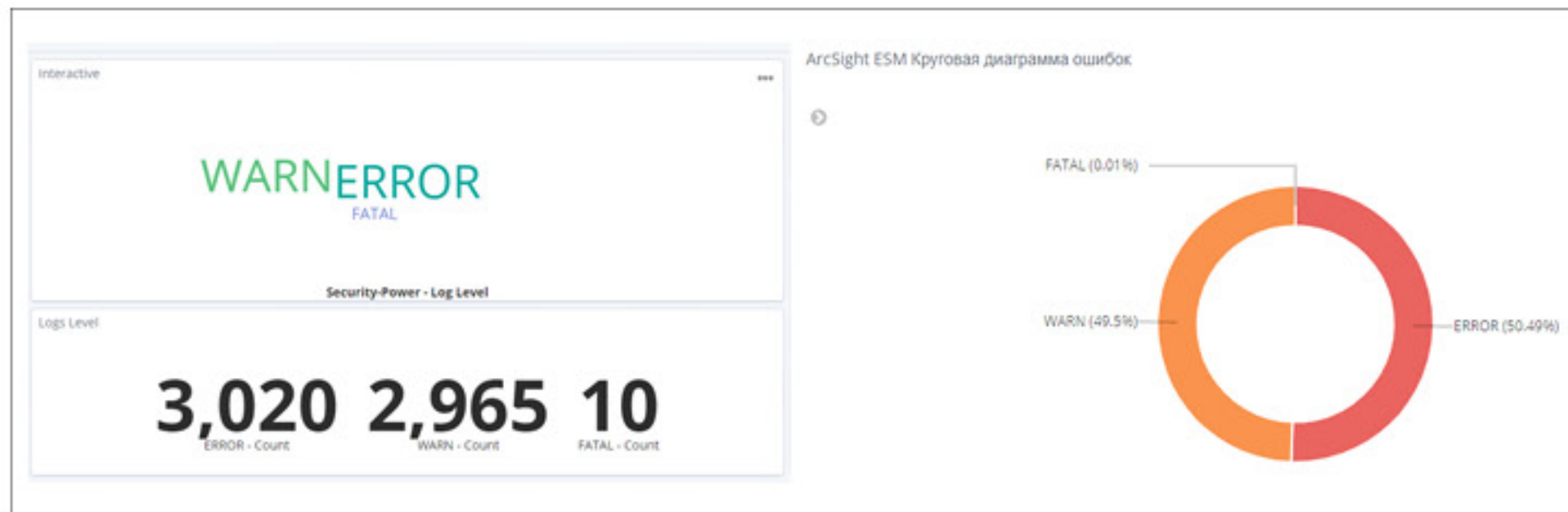


Рисунок 2. Визуализация количества ошибок

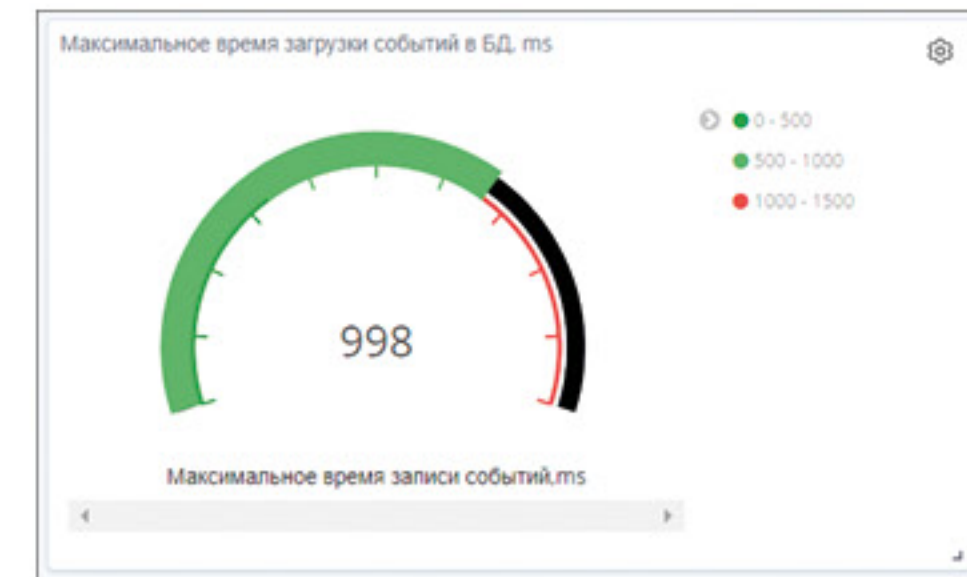


Рисунок 3. Визуализация скорости записи в базу данных событий ИБ

оперативной оценки состояния архитектуры. База данных включает в себя визуализацию метрик и критичных событий, а также итоговый дашборд, который займёт достойное место в SOC;

♦ визуализация:

- визуализация всех ошибок с возможностью поиска по каждой из них (рис. 2);
- визуализация скорости записи в базу данных событий информационной безопасности (рис. 3);
- компоновка метрик на одном дашборде (рис. 4);

♦ работа с оповещениями:

- регистрация поступающих оповещений в отдельный интерфейс (рис. 5);
- рекомендации по решению выявленных проблем (рис. 6).

Необходимость в мониторинге сервисов всегда стояла не на последнем месте, а в непростое эпидемиологическое время только возрастает. Необходимость контролировать работоспособность систем из любой точки планеты и реагировать на инциденты — основная задача любого руководителя IT или ИБ направления.

* * *

Наша команда более 10 лет занимается исследовательской работой по минимизации трудозатрат для анализа работоспособности SIEM-систем. Нами была разработана отечественная система анализа работоспособности SIEM-систем, которая переросла в продукт, который мы можем предложить нашим клиентам и заказчикам. Наше решение позволит сократить время реакции на инциденты работоспособности и повысить производительность SIEM.



Рисунок 4. Компоновка метрик на одном дашборде

Title	Severity	Tasks	Observables	Assignee	Date
#337 - ESM ERROR Security-Power ESM	M	1 Task	0	E	02/25/20 10:45
#336 - ESM ERROR Security-Power ESM	M	1 Task	0	E	02/25/20 10:45
#334 - ESM ERROR Security-Power ESM	M	1 Task	0	E	02/25/20 10:19
#303 - MySQL FATAL Security-Power MySQL	M	1 Task	0	E	02/24/20 18:33

Рисунок 5. Перечень поступающих оповещений

Рисунок 6. Визуализация оповещения и пути его решения



НА НОВЫЙ УРОВЕНЬ

ВЫШЕЛ XII УРАЛЬСКИЙ ФОРУМ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВОЙ СФЕРЫ»

С 17 по 21 февраля 2020 года при участии государственных регуляторов в области информационной безопасности состоялся XII Уральский форум «Информационная безопасность финансовой сферы». Организатором мероприятия выступил Банк России, оператором — Медиа Группа «Авангард».

В мероприятии приняли участие более 650 человек. Большинство составили руководители и ведущие специалисты департаментов ИБ в банках, некредитных финансовых организациях и платёжных системах, представители российских и зарубежных регуляторов, компаний-разработчиков и интеграторов решений и услуг в сфере защиты от киберугроз, образовательных учреждений и СМИ. В деловой программе приняли участие представители руководства Банка России, а также Генеральной прокуратуры РФ, МВД России, Минкомсвязи Рос-

сии, Минобрнауки России, Минфина России, Роскомнадзора, ФСБ России. Участниками ряда дискуссий, заседаний и круглых столов стали представители международных организаций и центральных банков зарубежных стран.

Благодаря открытию новой конференц-площадки Free Zone программа форума проходила двумя полноценными потоками. Это позволило обсудить значительно больше ключевых тем, провести серию мастер-классов и демонстраций новых технологий для решения задач служб ИБ. Помимо основной программы в ходе форума состоялись встречи представителей российских и зарубежных регуляторов финансовой отрасли стран БРИКС и ЕАЭС, которые были посвящены международному сотрудничеству в борьбе с киберпреступностью.

В заключительный день Уральского форума впервые был проведён Молодёжный день. Его участниками стали

команды учащихся по специальности «Информационная безопасность» из 10 вузов со всей страны. Участники Молодёжного дня прослушали курс лекций, продемонстрировали свои навыки в формате киберучений и представили свои решения, направленные на противодействие кибермошенникам.

ЗНАЧИМОСТЬ ИБ РАСТЁТ

Представители Банка России сделали ряд важных анонсов и заявлений о мерах регулятора, направленных на повышение киберустойчивости российских финансовых организаций, развитие безопасных цифровых финансовых сервисов и укрепление банковской системы страны. Предлагаем вашему вниманию некоторые из наиболее значимых заявлений.

Заместитель Председателя Банка России Дмитрий Скобелкин назвал развитие цифровой среды и высокую скорость развития финансовых технологий



В мероприятии приняли участие более 650 человек



Сессия, посвященная взаимодействию организаций финансовой сферы и правоохранительных органов



Параллельный поток программы форума на новой конференц-площадке Free Zone

факторами, которые повышают значимость информационной безопасности финансового рынка в наше время.

По словам зампреда, развитие цифровой среды — это непрерывное появление и внедрение новых цифровых технологий. В отношении некоторых из них Банк России уже устанавливает требования по информационной безопасности — это единая биометрическая система, система быстрых платежей и платформа Маркетплейс.

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД

Базовый стандарт по информационной безопасности должен соблюдаться в любой кредитной организации, но при этом необходимо понимать, что каждый банк обладает своей специализацией, банки отличаются по размерам и масштабам деятельности. И в зависимости от этого должна развиваться ИБ.

Банк России будет пропагандировать риск-ориентированный подход к безопасности. Одна из форм такого подхода — проведение киберучений. «Если мы будем видеть проблемы, которые возникают у участников киберучений, это станет предметом для дальнейших наших действий», — сказал Д. Скобелкин. При этом он отметил, что речь не идет о санкциях со стороны регулятора. Под риск-ориентированным подходом подразумевается наблюдение за банками, совместная работа над профилактикой проблем и недопущение их реализации.

«Регулирование и информационная безопасность — это единое целое. Мы, безусловно, будем учитывать риски информационной безопасности в надзорных рисках. Это станет одним из основных и очень важных направлений, которые мы будем совместно с надзорным блоком развивать», — сказал Д. Скобелкин.

Первый заместитель Председателя Банка России Дмитрий Тулин дал свою оценку взаимодействию по вопросам обеспечения ИБ в рамках Центрального банка: «Я представляю блок, который в целом отвечает за комплексную оценку риск-профиля каждой кредитной организации, что включает в себя оценку киберустойчивости,



Первый заместитель Председателя Банка России Д. В. Тулин

комплаенс-риски. И мы в данном случае очень тесно взаимодействуем как одна команда. Потому что все аспекты деятельности участников финансового рынка могут сказаться на их финансовой устойчивости, — подчеркнул Д. Тулин. — У нас общие подходы и главный заключается в том, что это некарательные меры».

КИБЕРРИСКИ — ТРАНСНАЦИОНАЛЬНАЯ ПРОБЛЕМА

Решить проблему киберрисков в отдельно взятой стране или группе стран практически невозможно. Поэтому Банк России настроен на то, чтобы в его мероприятиях участвовало максимальное число иностранных гостей, представителей зарубежных регуляторов, специальных организаций, которые занимаются проблематикой информационной безопасности.

«Мы со своей стороны принимаем самое активное и непосредственное участие в международных форумах, которые проводятся Всемирным банком, Базельским комитетом и иными международными организациями», — отметил Дмитрий Скобелкин.

В настоящее время практически со всеми партнёрами стран ЕАЭС подписаны договора об обмене информацией, налажена хорошая практика взаимодействия. Зампред Банка России выразил надежду на то, что в этом году будут



Заместитель Председателя Банка России Д. Г. Скобелкин

завершены все подготовительные мероприятия и подписаны все соглашения в рамках стран БРИКС.

ВЫСОКОТЕХНОЛОГИЧНЫЙ, ОБРАЗОВАННЫЙ РЕГУЛЯТОР

Топ-менеджеры Банка России из разных департаментов в ходе очередной сессии обсудили, что должен делать регулятор, чтобы оставаться высокотехнологичным, образованным, хорошо знающим и глубоко понимающим все процессы, происходящие на финансовых рынках и тем самым способствовать решению всех актуальных задач совместно с участниками рынка.

Для изучения всех инноваций в рамках ЦБ был специально создан Департамент финансовых технологий. Департамент национальной платёжной системы также работает в коллаборации с технологическими партнёрами.

Директор Департамента национальной платёжной системы Банка России Алла Бакина уверена, что регулятору необходимо не только оценивать все процессы, происходящие на внутреннем рынке, но и анализировать мировые тенденции, видеть общие тренды.

Начальник Управления анализа и регулирования в сфере финансовых технологий Банка России Дмитрий Дубынин отметил, что технологическое развитие всегда происходит быстрее, чем развитие регулирования, тем не менее, Центробанку необходи-

мо своевременно реагировать на появление новых технологий. У банка есть для этого специальная ассоциация, которая работает с рынком, рабочие группы по разным проектам, а также такой механизм, как регулятивная песочница.

Заместитель директора Департамента обработки отчётности Банка России Станислав Короп добавил, что Центробанк сильно продвинулся в области сбора и обработки отчётности. Так, в 2018 году банк ввёл для некоторых своих подконтрольных организаций новый стандарт отчётности — XBRL.

СОВЕРШЕНСТВОВАНИЕ ЗАКОНОДАТЕЛЬСТВА

На XII Уральском форуме Банк России представил ежегодный отчёт по операциям без согласия клиента. Первый заместитель директора департамента информационной безопасности Банка России Артём Сычёв привёл всю соответствующую статистику, рассказал о наиболее распространённых способах хищения — лидерство по-прежнему сохраняется за хищениями через системы ДБО.

А. Сычёв рассказал о тех мерах, которые регулятор собирается предпринять, чтобы «статистика всё-таки улучшалась, а не скатывалась в пропасть. Прежде всего это совершенствование законодательства». В проработке сейчас находятся два законопроекта: Закон



Дискуссия «Будущее финансовой сферы: безопасное, удобное, доступное»

о блокировках сайтов и Закон об обмене информацией между телеком-операторами и банковскими организациями. Продолжается развитие нормативной базы.

Другая важная мера — повышение финансовой грамотности. «Мы нацелены на то, что в эту работу активно будем вовлекать финансовые организации. Они и сейчас обязаны это делать, но более широкое их участие — это один из наших приоритетов», — подчеркнул А. Сычёв.

НЕОБХОДИМОЕ ВЗАИМОДЕЙСТВИЕ

Представители Банка России, Генеральной Прокуратуры и МВД в ходе форума много говорили о необходимости взаимодействия финансовых организаций и правоохранительных органов. Несмотря на неутешительную статистику по итогам прошлого года, такое взаимодействие позволяет увеличить число пресечённых правонарушений. Так, в 2019 году департамент ИБ заблокировал в 5 раз больше фишинговых ресурсов, чем в 2018 году — более 10 тыс. Заблокированы также более 1100 ресурсов, распространяющих вредоносное ПО и более 13 тыс. телефонных номеров, с которых мошенники пыта-

лись получить доступ к пользовательским данным.

Ещё одной бедой современного цифрового общества стали финансовые пирамиды, когда сомнительные инвестиции, в том числе криптовалютные, привлекаются через интернет, причём организаторы пирамид, как и прежде, обещают участникам солидный заработок «на халяву». О методах противодействия такому виду мошенничества рассказал глава департамента Банка России по противодействию недобросовестным практикам Валерий Лях.

ТЕМАТИЧЕСКИЕ СЕССИИ

В рамках форума состоялось много содержательных тематических сессий, посвящённых различным вопросам информационной безопасности.

На одной из них речь шла о построении эффективного центра мониторинга событий информационной безопасности (Security Operations Center). Аналитик центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар» Алексей Павлов показал примеры правильных и неправильных задач, которые организация ставит перед собственным или аутсорсинговым SOC.

SOC может выполнять как функции только мониторинга или реагирования, так и полного цикла расследования. Для его эффективной работы специалистам SOC необходим диалог с подразделениями заказчика, отвечающими за бизнес и ИТ.

Другая сессия была посвящена идентификации и аутентификации пользователя в банковских системах. Опытом применения в своём банке аутентификации и электронной подписи поделился заместитель начальника департамента защиты информации АО «Газпромбанк» Сергей Горленко. Заместитель генерального директора компании «Аладдин Р.Д.» Алексей Сабанов представил аутентификацию как основу доверия online-транзакциям.

«СБП: безопасность или иллюзия?» — этот вопрос стал центром обсуждения ещё одной тематической сессии. К системе быстрых платежей как к системе национального масштаба предъявляются максимальные требования безопасности. Чтобы их выполнять, используются самые современные и актуальные международные практики по обеспечению ИБ. Безопасность в системе заложена на всех возможных уровнях: на транспортном, прикладном, системном.

Две специализированные сессии были посвящены технологиям распределённого реестра и современным методологиям разработки ПО. Большинство участников высказали мнение, что при выборе между процессами гибкой разработки и классического waterfall организациям нужно уметь совмещать у себя эти подходы.

«МНЕНИЕ ОТРАСЛИ БУДЕТ УСЛЫШАНО»

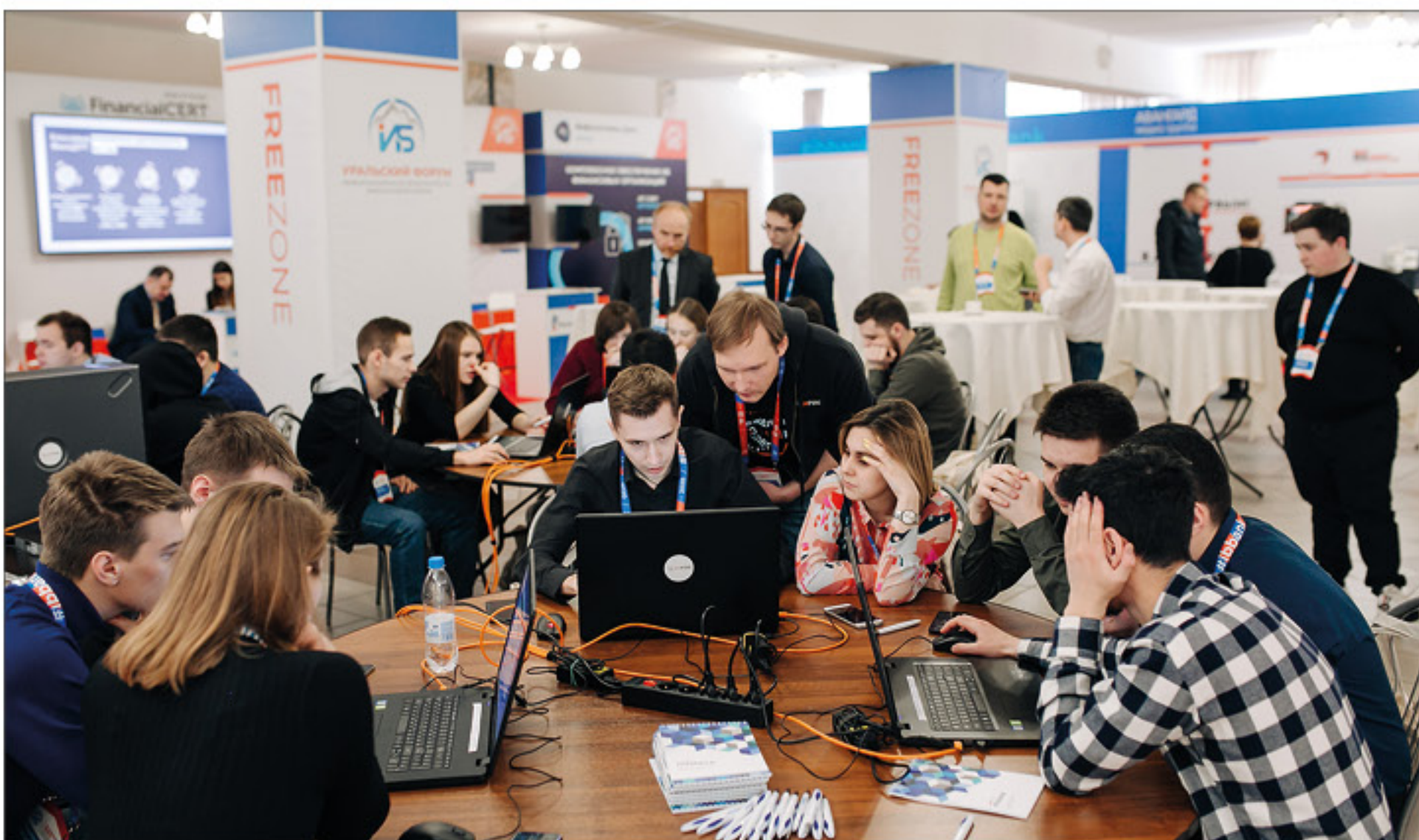
В заключении третьего дня форума бизнес-консультант по ИБ Алексей Лукацкий подвёл своеобразный итог всех прошедших выступлений. По его убеждению, сегодня концепция ИБ-аудита регулятора меняется в сторону непрерывного мониторинга, проверки реализуются с помощью разных каналов, к которым подводится законодательная база: пентесты, анализы защищённости, киберучения, информирование ФинЦЕРТа об инцидентах и рисках. Меняются и ключевые показатели, по которым будут оцениваться финансовые организации, не только кредитные, — для того, чтобы у них не было возможности манипулировать отчётностью, завышая свой уровень оценки ответственности. Появляются новые механизмы отчётности, связанные с анализом данных об инцидентах, «бумажная» составляющая сдвигается на второй план.

«Далеко не все довольны теми большими нормативными изменениями, которые готовит Банк России. Наверное, это объясняется тем, что мы сейчас находимся на переходе от комплаенс-ориентированного подхода к ИБ в сторону риск-ориентированного, и появление новых полномочий регулятора как раз означает появление новых документов, которые раньше ничем и никем не закрывались. К счастью, различные формы взаимодействия с регулятором позволяют нам надеяться, что мнение отрасли будет услышано в новых нормативных актах или в обновлениях существующих, которые готовит ЦБ», — резюмировал спикер.

Важнейшие события и выступления Уральского мероприятия широко освещались в ряде федеральных, региональных и отраслевых СМИ.



В рамках международной программы Уральского форума прошла встреча рабочей группы подразделений ИБ национальных и центральных банков стран ЕАЭС



В заключительный день Уральского форума впервые был проведён Молодёжный день



Традиционные «Банковские битвы» в рамках спортивного дня Уральского форума

iFin-2020

КЕЙСАМИ ФИНТЕХА СТАЛИ ПОДХОДЫ И МЕТОДОЛОГИИ

Почти сотня докладов, представленных на Международном форуме iFin-2020 «Электронные финансовые услуги и технологии», вращалась по большей части по орбитам сегодняшнего внимания Центробанка — ДБО, СБП, ЕБС, маркетплейс. Кибербезопасности была посвящена отдельная секция, а на других секциях она так или иначе представлялась в ходе анонсов компетенций участников и достоинств продуктов, ими предлагаемых. Было представлено даже «железо», позволяющее оптимизировать в ИТ-сервисах учёт требований ИБ за счёт шифрования на уровне L1.

На финальной дискуссии о технологиях, которым предстоит определять лицо кредитно-финансовой сферы в ближайшие пять лет, эксперты единодушно признали, что технологии безопасности — это краеугольный камень цифрового и дистанционного банка сегодня и завтра. Специально был упомянут такой важный аспект, как удобная, но надёжная идентификация, аутентификация и авторизация клиентов и персонала. Это задача, которая ещё не нашла окончательного решения.

СИСТЕМНЫЙ ФИНТЕХ

Большая часть из того, что представлялось на iFin-2020, либо успешно внедрено в крупных банках, либо предлагается к внедрению как решение (продукт),

тщательно выверенное с точки зрения взглядов регулятора на соблюдение нормативных требований. Поэтому для краткого обозначения места, занимаемого этим форумом в экосистеме отечественного финтеха, вполне уместно позаимствовать термин из политического лексикона: «системный».

По меткому замечанию одного из участников, идеологическое давление регулятора на форум оказалось столь высоко, что положения ЦБ были вынесены на рекламные фронтоны стендов компаний в качестве безусловно безотказного инструмента привлечения заказчиков.

Звучали на форуме и голоса «оппозиционеров». В ходе дискуссий высказывались мнения о высокой требовательности регулятора, рассказывались душещипательные истории, как некоторые банки вынуждены урезать «бюджет развития» для финансирования работ в сфере комплаенса.

Но является ли регуляторная жёсткость Центробанка самоцелью или это вынужденная мера? Скорее мягкий рыночный инструмент для выправления «перегибов на местах» в части игнорирования требований ИБ и укрепления устойчивости финансовой системы.

СБП СДЕЛАЕТ БАНКИ РАВНЫМИ

На финальной дискуссии о технологиях, которым предстоит определять

лицо банков, генеральный директор iDSystems, облачившись в каску, предрёк смерть пластиковым картам. И хотя зал скептически отнёсся к такому прогнозу, экспертный «президиум» положительно оценил влияние на отечественный рынок системы быстрых платежей.

Сравнивая СБП с «пластиком» и обсуждая технологии не только в контексте бизнес-задач банков, но и оценивая их в плане надёжности, возможности масштабирования и удобства модернизации инфраструктур, эксперты отметили перегруженность современной инфраструктуры платёжных карт «костылями» и «надстройками» на контрасте с известным изяществом инфраструктуры СБП, выстроенной на новой площадке.

Эксперты были также единодушны в своих надеждах на появление суперприложения, объединяющего интерфейсы к набору сервисов для квалифицированного потребителя. Сначала дебатировался лишь вопрос, кто должен быть владельцем суперприложения, — банк, государство или финтех-компания? Сошлись на том, что скорее банк, ибо сегодня банк — это символ доверия, в нём хранится самое ценное для квалифицированного потребителя — деньги.

Следует отметить, что Форум уделил достойное внимание не только лучшим внедренческим «кейсам» финтеха. Были широко представлены современные подходы к выбору архитектуры приложений, инструментария и технологиям работы ИТ-команд, включая Open API и Open Source банковских приложений.

А подведение итогов iFin-2020 на финальной дискуссии включило в число трендов финтеха использование современных методологий для оптимизации процессов обновления и развития ИТ-инфраструктуры банков.



Фото: forumifin.ru

MADE IN RUSSIA 2020

О МИФАХ И ИЗДЕРЖКАХ ЛОКАЛИЗАЦИИ

Следом за дискредитацией идей Реестров «отечественного»... (см, например, BIS Journal № 1/2020, стр.109) настал черёд критически осмыслить пригодность стратегий «локализации» для решения задач импортозамещения.

МИФ, ЗАБЛУЖДЕНИЕ, ЛОКАЛИЗАЦИЯ!

На конференции Made in Russia 2020 заместитель генерального директора компании «Т 8» развенчал ряд мифов и заблуждений, которые под вывеской достоинств т.н. «локализации» («быстро», «недорого»...) позволяют тормозить развитие отечественных разработок и производства после их развала в ходе «заколачивания гвоздей в крышку гроба коммунизма» 90-х. Если коротко резюмировать сказанное, то локализация позволяет в лучшем случае получать оборудование «позавчерашнего дня» и не способствует развитию компетенций разработчиков и рабочих.

В противовес локализации господдержка научно-производственных центров (НИЦ) позволяет, как продемонстрировал в своём докладе представитель «Т 8», создавать конкурентную на отечественном и мировом рынке продукцию для телекома и измерительной техники.

ПАРАД КОНЦЕПЦИЙ

Положительные примеры создания современного отечественного оборудования привёл на конференции представитель ООО «НТЦ ПРОТЕЙ», одновременно предложив и стратегию вывода такой продукции на отечественный рынок в рамках концепции сетей Private LTE/5G. Для отечественных производителей телеком-оборудования частные корпоративные сети — это

хорошая возможность для демонстрации «большим» операторам возможностей своей техники, а для корпораций и ведомств — шаг на пути к обретению технологической независимости в «дискриминационно-санкционном» мире и к обеспечению информационной безопасности в мире технологических бэкдоров и АНБ-закладок.

Готовность выйти за «красные флажки» стратегии «локализации» и поддерживать процессы импортозамещения на основе работы НИЦ продекларировали менеджеры Сколково и Ростелекома. Ими были представлены гладко написанные «маршрутные карты» и сказаны толково выверенные фразы.

Проверить обещания Сколково в части создания отечественного оборудования на основе открытых стандартов Open RAN возможно удастся во вполне обозримые сроки, измеряемые считанными годами.

Ростелеком представил гораздо более перспективные планы по части развития оптоэлектронных и квантовых технологий, расплывчатые в части конкретики конечных результатов и, к тому же, измеряемые десятилетиями в части сроков. Но озвучены эти планы были в весьма компетентных выражениях и уверенных тонах.

СТОЛКНОВЕНИЕ С РЕАЛЬНОСТЬЮ

Возвращаясь же к «локализации», уместно вспомнить достаточно известное правило: «Выбирая позор между войной и позором, получишь и войну, и позор».

Сдав без боя производство отечественных телевизоров и «самое важное из искусств» — телевидение, Россия сначала столкнулась с тотальной войной в сфере культуры и идеологии,

а теперь ещё и с другого рода провокацией. В стране тихой сапой было произведено веерное отключение «интеллекта» телевизоров Самсунг, в отношении которых в информационной системе корейской компании числится несоответствие между регионом фактической эксплуатации и регионом, в котором, по мнению информационной системы компании, эта техника должна бы эксплуатироваться.

Оставляя «за скобками» анализ юридической «чистоты» подобной акции южнокорейской компании, заместитель генерального директора МНИТИ обратил внимание слушателей на то, что телевидение на территории страны выполняет не только развлекательные функции, но и является важным элементом системы оповещения населения о критических ситуациях.

Разрешив локализацию производства иностранных телевизоров, законодатели и исполнительная власть новой России не только создали условия для потери технологической независимости страны по целому ряду направлений, но и ослабили информационную безопасность страны (темпы роста безработицы и потери квалифицированного персонала остались за рамками доклада).

* * *

Не был услышан на Made in Russia 2020 лишь компетентный и конкретный голос государства. А он весьма важен. Ибо ухватившиеся за штурвал управления экономикой России не выходят за рамки полуторавековой давности постулатов о рыночной экономике с конкуренцией и приматом прибыли. Современный же капитализм, с которым приходится конкурировать российским инженерам, комфортно чувствует себя в рамках откровенного монополизма и государственного протекционизма и позволяет устанавливать символические цены, ориентируясь на стратегические цели технологического доминирования.

Локализация позволяет в лучшем случае получать оборудование «позавчерашнего дня» и не способствует развитию компетенций разработчиков и рабочих

РЕГУЛЯТОР И ПУСТОТА

В ТОПЕ ТЕМ — БЕЗОПАСНОЕ ПРОГРАММИРОВАНИЕ

В определённые времена возникают темы, которые проходят общей нитью через множество разных по своей проблематике ИТ&ИБ-конференций. В последние годы это была, например, тема «обращения» с КИИ в свете требований 187-ФЗ. Постепенно, благодаря активной просветительской работе ФСТЭК и Центробанка, понимание этого вопроса вышло на должный уровень и работы двинулись по накатанной колее. Сегодня в топ тем подняты вопросы «безопасного программирования». Этой проблематикой весьма озабочен регулятор, и эта

озабоченность передаётся рынку, что продемонстрировала, например, дискуссия на конференции «Информационная безопасность 2020: новые технологии — новые риски».

РЕГУЛЯТОРЫ ХОТЯТ КАК ЛУЧШЕ

Это мероприятие представило в некотором смысле «репрезентативную выборку» рынка. Было, что называется, «каждой твари по паре»: выступили с докладами представители ЕВРАЗ и Росводоканала, были сообщения от пары организаций финансово-инвестиционной направленности, выступили пред-

ставители НИИ Восход и ДИТ Москвы, рассказали о своих продуктах и услугах несколько компаний, чей бизнес связан с финансовым «здоровьем» ИБ-бюджетов организаций.

В ходе финальной дискуссии обсудили, как водится, регуляторов, которые планомерно обузывают бурсацкую ИТ-вольницу, направляя её в русло обычной для развитых стран технической и социальной регуляторики. И вот в ходе этой дискуссии и были озвучены опасения в связи с активизацией работ по внедрению «нормативки» в сфере программирования. Некоторых экспертов возбудило то обстоятель-

«КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ» 2020

ЦИФРОВЫЕ ТЕХНОЛОГИИ
КАК КОЛЛЕКТИВНЫЙ ОРГАНИЗАТОР

Главный вывод по итогам конференции «Корпоративная безопасность»: корпоративная безопасность превращается в функцию, за которую ответственен весь персонал, а не только департамент или служба с таким же названием. Превращение идёт посредством информационных технологий, которые многократно усиливают возможности каждого конкретного сотрудника, но отнюдь не подменяют собой людей.

ОПЫТ НЕ В ТОПЕ

При этом опытом внедрения предиктивной ИТ-аналитики в интересах корпоративной безопасности делились не

столько представители банков из списка TOP-10 или телекомов (уверенно занимающие в общественном сознании лидирующие позиции в ИТ-инновациях), сколько эксперты из промышленности (Концерн «Калашников», Группа ЧТПЗ, Группа ГАЗ, Нестле Россия) и ритейла (OZON, OBI Россия, O'Key). Эти компании больше известны своей профильной деятельностью, однако, как оказалось, их «тылы» надёжно прикрыты щитом безопасности на базе ИТ.

МЫ ОДНОЙ КРОВИ

Некогда «социологи» сферы безопасности небезосновательно находили разни-

цу между «ибэшниками» и «безопасниками» и в дресс-коде (джинсы одних и деловые костюмы других), и, что более важно, в менталитете — инновационный ИТ-технократизм одних и консерватизм других, базирующийся на инструкциях, крепких замках и простых человеческих связях в силовых структурах.

В этом году конференция продемонстрировала складывающуюся синергию здравого смысла жизненного опыта и предиктивной аналитики Больших Данных, циркулирующих и хранящихся в ИТ-инфраструктуре предприятий.

Инструкции, оказывается, вполне возможно перевести в логику «искус-

ство, что финансовый регулятор выбрал курс на теснейшее сотрудничество с ФСТЭК.

Этим государственным мегарегулятором 11 февраля 2019 года утверждена методика выявления уязвимостей и недекларированных возможностей в ПО. И фактически под эгидой ФСТЭК актуализируется ГОСТ Р 56939–2016, формализующий общие требования к разработке безопасного ПО, а также готовятся ГОСТы, призванные стать руководствами по разработке безопасного ПО, по оценке безопасности разработки такого ПО, по управлению безопасностью ПО при заимствовании программных компонентов.

ЖЁЛТЫЙ ГЛАЗ ОЖИДАНИЯ

Для agile-ориентированных команд, разрабатывающих финтех-приложения для отечественных банков, бирж и инвестиционных компаний — это жёлтый сигнал светофора, который указывает на угрозу постановки заслона перед идеологией «непрерывных изменений» и выпуска релизов с трёх-четырёхзначными обозначениями версий.

ственного интеллекта», жизненный опыт подкрепить машинным обучением, а связи в силовых структурах — аналитикой данных из социальных сетей.

Деловые костюмы собравшихся на конференции руководителей служб безопасности не мешали им уверенно рассуждать о возможностях управления разными аспектами безопасности своих корпораций (экономической, информационной, физической, кадровой) с помощью аналитических инструментов, надстроенных над DLP-системами или на худой конец — на основе Excel-аналитики данных, собранных технологией RPA из «персональных» ИТ-систем бухгалтерии, кадровой службы и других «удельных княжеств» компании.

За этим явлением ощущается кропотливый евангелизм лидеров отечественного рынка ИТ&ИБ.

Регуляторы планомерно обуздывают бурсацкую ИТ-вольницу, направляя её в русло обычной для развитых стран технической и социальной регуляторики

О том, что agile остаётся обычной практикой, свидетельствовали и доклады на iFIN 2020, и выступления и дискуссии на другой конференции — «Информационные технологии в финансовых институтах», которая собрала 27–28 февраля весьма сильный состав экспертов.

И если спикеры iFin — это вендоры, весьма откровенно заинтересованные в быстром обороте продаж своих программных продуктов, то за спинами выступавших на конференции 27–28 февраля маячили самые что ни на есть конечные потребители современных финтех-поделок — ВТБ, Ростелеком, Яндекс.Деньги, Альфа-Капитал и Альфа-Банк, UBS, Нордеа Банк, БКС Брокер, ТрансКапиталБанк, Металлинвестбанк, Банк Уралсиб, Банк «Открытие»... Проще было бы сказать, что из

законодателей финтех-моды не было только Сбербанк.

«ПОЧТИ» VS «ВСЕГДА И ПРАВИЛЬНО»

В контексте темы agile vs ГОСТ весьма поучительным был доклад представителя Альфа-Капитала на конференции «Информационные технологии в финансовых институтах». Илья Батай поделился наблюдениями различий опыта и подходов к работе «айтишников» 90-х, одинаково хорошо владевших знаниями о бизнесе и знаниями в ИТ, и нынешних «аджайл»-финтехов, основным конкурентным преимуществом рассматривающих короткий «time-to-market» своих разработок. Г-н Батай предложил интересное определение различия между классическим банковским и финтех-сервисом: «Фин-

Что, впрочем, не позволяет не заметить и определённых недостатков упомянутого евангелизма.

ДЕНЬГИ НЕ ГЛАВНОЕ

В первую очередь заразительности очень модной (и столь же очень сомнительной) мантры о необходимости общения безопасников с бизнесом на языке бизнеса, мыслящего в координатах «максимизации прибыли» и «снижения костов». В связи с этим, по мнению некоторых гуру, безопасность должна ежечасно доказывать бизнесу свою нужность. Такая парадигма необоснованно порождает у отечественной безопасности своеобразный комплекс вины за своё существование.

Деловой «язык» бизнеса был однобоклен лишь во времена Маркса, а нынче, в обществе с развитой социальной культурой, бизнес для своей «рукопожатости» вынужден использовать более

широкий набор правил. В банковской сфере, например, регулятор сегодня успешно доносит до курируемой им части бизнеса обязательные требования в сфере безопасности, не только не сочетающиеся с готовностью преступить любые законы за «300% прибыли», но и твёрдо пресекающие такую готовность в зародыше.

* * *

Остаётся пожелать, чтобы корпоративная безопасность, как явление более широкое, чем безопасность кредитно-финансовой сферы, получила бы столь же заботливого регулятора. Хотя бы в виде развития программ MBA учебными треками, формирующими социально ответственный (а не только монетарный) подход к управлению корпоративной безопасностью.

И хотя пока ряд руководителей бизнеса довольствуется качеством уровня «почти», регулятор, похоже, выбрал курс на высокое качество уровня «всегда и правильно»

тех — это почти всегда и почти правильно, но быстро, а классический банк — это и всегда, и правильно, но медленно».

И хотя пока ряд руководителей бизнеса довольствуется качеством уровня «почти», регулятор, похоже, выбрал курс на высокое качество уровня «всегда и правильно».

Об этом же, кстати, свидетельствовал и доклад на той же конференции представителей Нордеа Банка, которые рассказали о реализации проекта по созданию отказоустойчивой ИТ-инфраструктуры в соответствии с требованиями регулятора. Они представили ещё один пример того, сколь широко ЦБ охватывает своим вниманием разные аспекты обеспечения надёжной работы банковской системы России. Одним из элементов проекта оказалась методология работы банка в условиях полного отказа всей ИТ-инфраструктуры.

МИФЫ О СОТРУДНИЧЕСТВЕ

Наиболее полно в начавшемся 2020 году вопросы «безопасного» программирования были освещены на ТБ Форуме в ходе конференции «Актуальные вопросы защиты информации». Ключевые темы, вызвавшие особый интерес публики — «Основные направления совершенствования деятельности по технической защите информации», «Нормативное правовое регулирование вопросов создания отечественной радиоэлектронной продукции», «Перспективы создания средств защиты информации на базе отечественной радиоэлектронной продукции», «Инструментальные средства и технологии выявления уязвимостей в программном обеспечении».

Последний доклад был представлен директором Института системного программирования РАН и вызвал смешанные чувства. С одной стороны, были системно изложены результа-

ты работ высокопрофессионального коллектива, позиционирующего себя как «ведущая научная школа в области анализа программ и кибербезопасности». С другой, несмотря на декларативное заявление об успешном опыте конструктивного взаимодействия регулятор&наука&бизнес, следов этого опыта в докладе обнаружить не удалось.

Хотя действий в этом направлении было предпринято немало. Лишь с 2019 годом связаны такие «события», как возникновение курсов по повышению квалификации сотрудников Испытательных Лабораторий, создание подкомитета 4 «Разработка безопасного программного обеспечения» в ТК 362 «Защита информации», совместное создание ФСТЭК России и ИСП РАН Центра компетенции в области кибербезопасности.

Тем не менее, повторюсь, ни в докладе «Основные направления совер-

шенствования деятельности по технической защите информации» ФСТЭК России, ни в упомянутом докладе директора ИСП РАН не обнаружено следов «опыта конструктивного взаимодействия» этих организаций. И это, наверное, можно понять. Такой опыт за один год не нарабатывается!

Более того, из некоторых фраз в ходе доклада директора ИСП РАН можно было сделать вывод, что учёные нашей страны лишь в общих чертах и лишь в режиме постфактум осведомлены о деятельности регулятора в сфере управления безопасностью ПО. И в этом не вина учёных. Проблема скорее в том, что процессы децентрализации управления в научно-технической сфере и промышленной политике подошли слишком близко к опасной черте, за которой — пустота. Та самая пустота, в которую уже проваливается мир отечественного компьютерного «железа». Почувствовать это позволяет красноречивый слайд, представленный на ТБ Форуме в докладе компании Крафтвэй (рисунок 1).

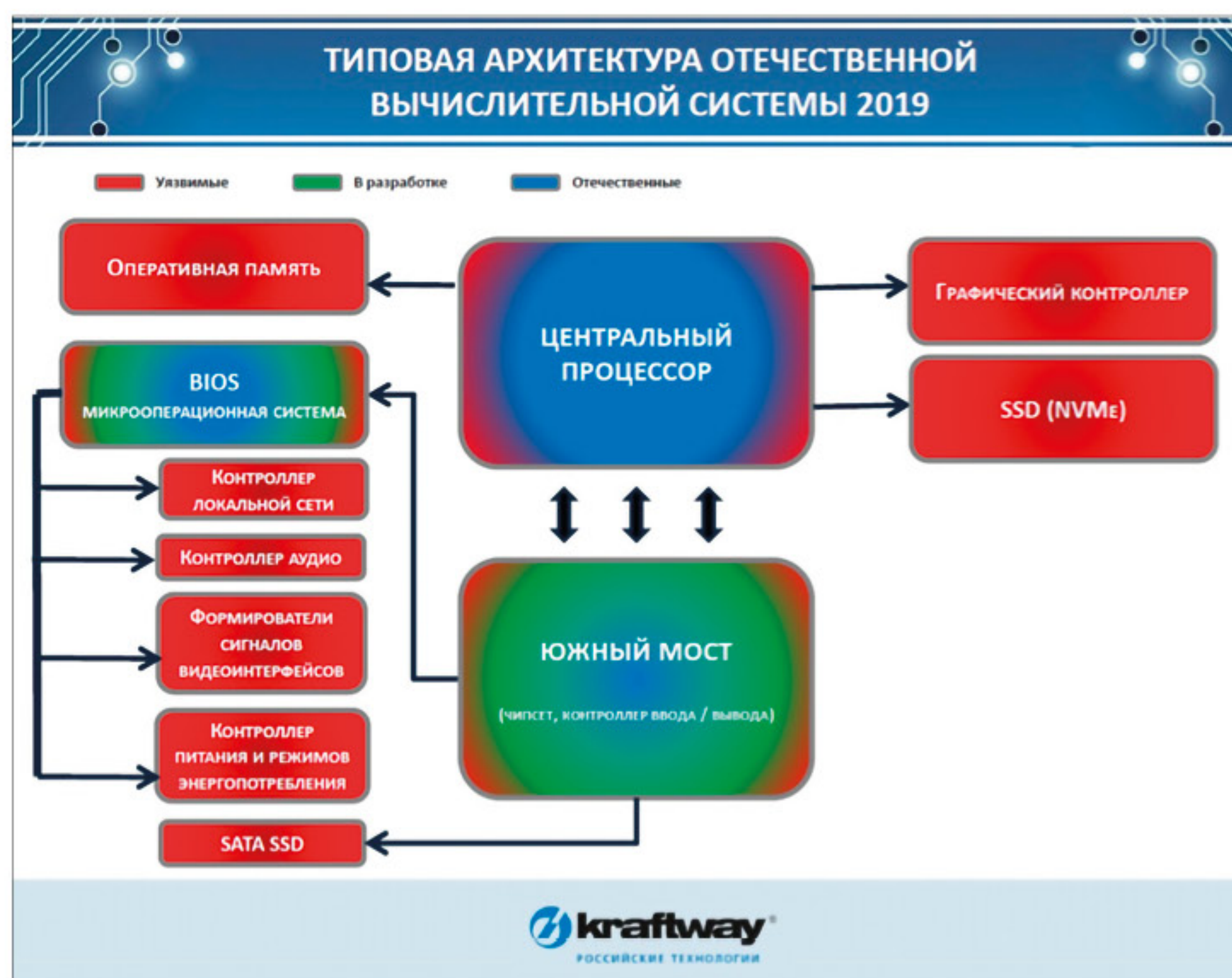


Рисунок 1. Типовая архитектура отечественной вычислительной системы 2019 (по версии компании Крафтвэй)

**Елена МЕЛАНИЧ**

первый заместитель Председателя Правления Ассоциации организаций в сфере наличного денежного обращения, инкассации и перевозки ценностей (АНДО), кандидат юридических наук, лауреат премии Правительства РФ

**Сергей КАСЬЯН**

генеральный директор Ассоциации организаций в сфере наличного денежного обращения, инкассации и перевозки ценностей (АНДО)

АНДО. НАЛИЧНЫЕ. НАДОЛГО!

Тотальная цифровизация в кредитно-финансовой сфере изменила угол зрения на товарно-денежные отношения и в первую очередь непосредственно на сами деньги. Сегодня деньги в общественном сознании связаны прежде всего с безналичными расчётами, всевозможными онлайн-сервисами, дистанционным банковским обслуживанием. Кредитные карты, айфоны, электронные кошельки заменили собой привычные бумажники, закладки и сейфы. Казалось бы,

традиционные деньги — и новенькие хрустящие купюры, и мятые замусоленные бумажки, и звенящая мелочь в карманах — навсегда уходят из нашей жизни, а с ними и грандиозная отрасль, обслуживающая эту, можно сказать, глобальную сферу. Но так ли это? Наш корреспондент беседует с руководителями Ассоциации организаций в сфере наличного денежного обращения, инкассации и перевозки ценностей (АНДО) Еленой Меланич и Сергеем Касьяном.

— Можно ли сказать, что упорные слухи о близкой кончине наличных денег не преувеличены. Можно ли их опровергнуть? И стоит ли?

Елена Меланич. Безусловно, цифровизация — это объективный фактор, она проникает во все сферы нашей жизни, в том числе и в сферу денежного обращения. Во многом благодаря ей оборот безналичных денег в стране постепенно растёт. Но если абстрагироваться от вполне понятного рекламного шума, который сопровождает этот процесс, и обратиться к языку цифр, то мы увидим, что на сегодняшний день безналичный и наличный денежный оборот в стране распределяется примерно поровну. В прошлом году безналичный оборот составил 51 процент, но в то же время оборот наличных в абсолютной массе подрос на 2–3 процента.

Сергей Касьян. По мнению многих специалистов, оборот привычных нам наличных денег гарантировано сохранится до 2035 года. А дальше вообще ничего нельзя загадывать, так как объективных данных недостаточно.

— А дальше посмотрим?

Сергей Касьян. Да, там посмотрим. Но даже 15 лет — это очень большой срок. И не нужно забывать, что страна наша огромная, разноплановая, основ-

ная её территория удалена от центров, во многих местах нет не то что интернета, электричества порой нет. И люди, которые там живут, ещё очень долго будут оперировать в основном наличными. Покупать и продавать за наличные, копить их на чёрный день... Для них наличные по-прежнему незыблемая основа жизни. Да и не только в отдалённых районах, в городах все розничные предприятия оперируют наличными в гигантских масштабах, зарплаты часто выдаются наличными...

Елена Меланич. И все эти деньги нужно обслуживать: инкассировать, привозить-отвозить, складировать, считать, зачислять на банковские счета магазинов, предприятий... И это делается каждый день, причём, все в большем объёме. Так что слухи о кончине наличных денег действительно сильно преувеличены.

— Что на сегодняшний день представляет из себя отрасль наличного денежного обращения? Каковы её масштабы?

Елена Меланич. Костяк отрасли — это организации, которые инкассируют наличные у своих заказчиков — крупных, средних и мелких банков, торговых предприятий, государственных и частных компаний... У всех, у

кого есть кассы, аппараты по приёму или выдаче наличных — от банкоматов до автоматов по продаже шоколада. Частные лица тоже нередко выступают заказчиками. Инкассаторы транспортируют деньги до кассовых центров, там эти деньги пересчитывают и зачисляют на банковские счета. Это основа. Из этих специализированных организаций и состоит наша Ассоциация. Но вокруг костяка существует множество смежных предприятий — технологические компании — вендоры, различные поставщики, торговые предприятия. Важнейшей силой отрасли является Банк России и другие регуляторы, как, например, правоохранительные органы...

— Как много людей в отрасли?

Сергей Касьян. Если учитывать заказчиков и смежников, то несколько миллионов. А что вы хотите? Почти всё взрослое население страны так или иначе имеет к ней отношение. Водители инкассаторских автомобилей, механики, ремонтирующие эти автомобили, работники Гознака и Монетного двора, полицейские и охранники, обязанные прийти на помощь инкассаторам, кассиры — их одних в стране, наверное, под миллион, операторы и ремонтники счётных машин, программисты, пишу-

Одной из задач АНДО является создание отраслевых стандартов. Базовый стандарт «Инкассация и перевозка ценностей» мы уже разработали в 2017 году, и он применяется на практике. В работе ещё больше десяти стандартов

щие программы для этих машин... Не говоря уж о простых гражданах, несущих наличные в тот или иной магазин, откуда эти деньги обязательно заберут инкассаторы.

— **А сколько людей в инкассаторских организациях?**

Сергей Касьян. Трудно сказать. В отрасли около тридцати крупных организаций. Все организации, входящие в Экспертный Совет Ассоциации, оказывают услуги на высоком профессиональном уровне. Из них две — Росинкас и Сбербанк — очень крупные. Они имеют несколько тысяч броневинов и десятки тысяч сотрудников, оказывающих услуги по всей нашей стране.

— **Ассоциация работает уже больше трёх лет и до этого три года подготовительного периода. Что сделано?**

Елена Меланич. Регулярные заседания Правления принимают важные решения для жизни Ассоциации. Ежемесячно мы проводим заседания Экспертного Совета, на который собираются руководители, ведущие специалисты и представители Банка России, других регуляторов нашей отрасли, обсуждаем плановые и актуальные вопросы. Собственно, стабильная работа и есть непрерывный процесс строительства отраслевого сообщества — объединения профессионалов. Результаты таких заседаний — это всегда несколько важных решений, несколько кирпичиков в архитектуру отрасли. Главное, по-моему, что у нас получилось — это создать атмосферу общего дела.

— **Расскажите, пожалуйста, подробнее.**

Сергей Касьян. Например, одной из задач АНДО является создание отраслевых стандартов. Базовый стандарт «Инкассация и перевозка ценно-

стей» мы уже разработали в 2017 году, и он применяется на практике. В работе ещё больше десяти стандартов. В том числе сейчас работаем над важным для цифрового контекста стандартом. В чём его суть? Сегодня счетно-сортировальные машины (ССМ) работают в разных программных форматах, которые часто не стыкуются с внешними (смежными) системами. Это вынуждает банки тратить значительные материальные и кадровые ресурсы на обработку полученных данных, составление отчётов и передачу их по инстанциям. Создание стандарта, унифицирующего интерфейсы взаимодействия ССМ с внешними системами — системами сбора данных о результатах обработки банкнот, системами удалённого мониторинга качества работы ССМ, системами роботизированной подачи и изъятия банкнот, системами видеоаналитического контроля процессов обработки и др. — позволит решить сразу много задач. В первую очередь, снизит затраты на разработку, внедрение и эксплуатацию интегрированных систем, сопряжённых с ССМ, а также повысит эффективность и надёжность работы этих систем.

Елена Меланич. Также мы работаем над стандартом по идентификации пачек банкнот и другими стандартами, которые позволят автоматизировать процессы инкассации.

— **По сути ваша Ассоциация стала инициативным центром отрасли. Что мешает ей получить статус саморегулируемой организации?**

Елена Меланич. В нашем Уставе это заложено, и вообще это одна из наших организационных целей. Однако есть проблема: отрасль относится к сфере финансового рынка, а в федеральном законе «О саморегулируемых органи-

зациях в сфере финансового рынка» саморегулирование в сфере инкассации не отмечено.

Сергей Касьян. В нашем случае это, конечно, казус. По базовому закону «О саморегулируемых организациях» 2007 года государство передаёт таким организациям определённые полномочия, чтобы эффективно развивать ту или иную отрасль, пробудить инициативу снизу, максимально задействовать творческий и соответственно экономический потенциал страны. Таким образом развитие отраслей идёт гармонично и полноценно, и одновременно резко сокращаются расходы государства на отраслевое управление, координацию и контроль. Наша Ассоциация именно с такими задачами и создавалась.

— **Будем надеяться, что это временная трудность и она будет преодолена. Скажите, а какие возможности получит Ассоциация с получением статуса саморегулируемой организации? Как вы им распорядитесь?**

Елена Меланич. Собственно, все направления нашей работы обозначены, и работа по ним уже активно ведётся. Статус саморегулируемой организации предоставляет дополнительные права и обязанности, чётко распределяет полномочия между всеми отраслевыми силами. А такое положение должно способствовать прогрессивному развитию. Возможно, статус саморегулирования позволит решить и такие сложные задачи как «тротуарный риск».

— **Сейчас всё чаще идёт разговор о повышении культуры работы. Важно ли это для Ассоциации?**

Елена Меланич. Да, Ассоциация старается формировать общеотраслевую культуру. Мы рассматриваем её как особый стратегический инструмент, который помогает ориентировать организации отрасли на общие цели, мобилизовать инициативу и облегчать продуктивное общение, направленное на принятие конструктивных решений.

— **Спасибо!**

Беседовал Игорь Некрасов

КТО ПОД МАСКОЙ?

«СЛОВЕСНЫЙ ПОРТРЕТ» МОШЕННИКОВ,
СПЕЦИАЛИЗИРУЮЩИХСЯ НА ЮРИДИЧЕСКИХ ЛИЦАХ

В последнее время много говорят о социальной инженерии, о том, как мошенники «разводят» клиентов банков — физических лиц. Но не стоит забывать, что преступники также атакуют и юридических лиц. Если верить отчёту ФинЦЕРТа, таких немало. Так кто же они — эти мошенники, крадущие деньги у организаций? Кто под маской?

ВНЕШНЕЕ МОШЕННИЧЕСТВО

Внешнее мошенничество совершается лицом или группой лиц, целенаправленно атакующими юридические компании. Мошенники рассылают фишинговые письма для последующего заражения АРМ с банк-клиентом. Зачастую сотрудник компании, отвечающий за банк-клиент, сам «помогает» мошенникам, т.к. не соблюдает правила информационной безопасности, предоставляемые Банком, в частности, оставляет носитель ключевой информации воткнутым в USB-порт, хранит логин и пароль в системе, не имеет антивируса, использует удалённый доступ для работы в системе и т.п.

Мошенники, взломав АРМ компании, могут достаточно долго наблюдать за системой, дожидаясь удобного случая для списания всех денежных средств со счёта. А потом, войдя в интернет-банк, меняют пароль, создают платёжные поручения на «своих» получателей, подписывают их ключом электронной подписи, который оставил воткнутым в USB-порт бухгалтер, и выводят денежные средства, отправив платёжные поручения в Банк. Как правило, мошенники, дробят остаток на счёте и несколькими платежами выводят всю сумму.

Второй способ, которым пользуются мошенники для вывода денежных средств, это подмена реквизитов получателя в платёжном поручении. Они не взламывают банк-клиент, а ждут, когда бухгалтер зайдёт в систему, создаст легитимные платёжные поручения и перед подписанием ключом электронной подписи, подменяют реквизиты получателя, номер счёта, ИНН и Банк получателя, создавая видимость, что бухгалтер отправил платежи по верным реквизитам. Такое мошенничество может пересекаться с внутренним мошенничеством. Например, бывший сотрудник, увольняясь, получает до-

ступ к АРМ с банк-клиентом или заражает его вредоносным ПО, или сотрудник ИТ, оставляя себе лазейки, удаленно подключается к АРМ с банк-клиентом с домашнего компьютера и совершает платежи.

Получается, что лица, совершающие такие мошенничества, технически подкованы, владеют вредоносным ПО, необходимым для заражения АРМ. Имеют данные об обороте денежных средств и уровне защищённости атакуемой компании, могут иметь инсайдера внутри компании. Долго наблюдают за компанией, готовятся и ждут подходящего момента для атаки.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ У ЮРИДИЧЕСКИХ ЛИЦ

Методы социальной инженерии мошенники начинают применять с момента, когда компания планирует открыть счёт в Банке и ищет людей, которые окажут в этом помощь. В Интернете достаточно много сайтов фирм, которые оказывают помощь компаниям в подготовке документов и открытии счёта. Не все фирмы добросовестные, многие из них мошенники.

Как их распознать? Как правило сайты таких фирм односторонние, без точного указания адреса местонахождения, без адреса электронной почты, но с контактными номерами телефонов. Директор компании, «клюнувший» на крючок фирмы, сам передаёт мошенникам учредительные документы и свои персональные данные. Мошенники заверяют документы, нотариус обычно у них в доле, открывают счёт в банке, получают комплект документов на банк-клиент, разводят директора на пополнение счёта и осуществляют платежи без его ведома.

Так же мошенники орудуют на разных интернет-площадках, чаще на avito, разводя индивидуальных предпринимателей и компании малого бизнеса. ИП и директора малых предприятий



Артем ПРОХОРОВ
эксперт ИБ

В Интернете достаточно много сайтов фирм, которые оказывают помощь компаниям в подготовке документов и открытии счёта. Не все фирмы добросовестные, многие из них мошенники



ищут там различные фирмы-поставщики для своего бизнеса и... попадают на мошенников. Мошенники, войдя в доверие, предлагают товары или услуги и, вводя предпринимателей в заблуждение, сообщают реквизиты для перечисления денежных средств. Получив деньги, мошенники пропадают.

Иногда мошенники взламывают почту «своих» клиентов, т.к. клиенты не соблюдают рекомендации Банка по информационной безопасности, и реализуют схемы, о которых сказано выше. Известны случаи, когда мошенники звонили ИП, представлялись сотрудниками Банка и, имитируя работу кол-центра, вынуждали совершить платежи на подставных получателей.

Таким образом, мошенниками, использующими данные методы, являются организованные группы людей, в которых заранее расписаны все роли, составлены схемы и просчитаны ходы в краже и выводе денежных средств. Мошенники психологически подготовлены, знают методы и средства воздействия на «жертву», разбираются в рыночных отношениях, обладают техническими навыками. Таких сложно вычислить, т.к. все их контакты — это контакты подставных лиц, а получателями являются фирмы-однодневки, либо подставные физические лица.

ВНУТРЕННЕЕ МОШЕННИЧЕСТВО

Внутреннее мошенничество — это мошенничество, совершаемое внутри компании лицами, связанными с данной компанией. Этими лицами могут быть: сотрудник, отвечающий за всю бухгалтерию и финансы (бухгалтер, соучредитель, директор и т.д.), ИТ-специалист (системный администратор, сотрудник технической поддержки и т.д.) или увольняющийся сотрудник. Сотрудник, отвечающий за бухгалтерию и финансы, имея на руках все необходимые документы и доверенность от генерального директора, может спокойно, без ведома директора, открыть счёт в Банке, получить носитель с ключами электронной подписи на имя директора и спокойно проворачивать свои схемы с выводом средств со счёта фирмы.

Либо же директор сам (а часто так и бывает) доверяет сотруднику носитель с ключами электронной подписи для подписания платёжных поручений при осуществлении переводов. И так получается, что директор не знает о «тёмных» схемах этого сотрудника. ИТ-сотрудник под видом настройки или установки обновлений легко может получить доступ к АРМ с банк-клиентом и необходимым аутентификационным данным. Имея всё необходимое, он спокойно создаёт, подписывает и направляет платёжные поручения на подставных получателей или, подменив реквизиты получателя в уже созданных платёжных поручениях, делает так, чтобы их подписал и отправил бухгалтер. Случается, что увольняющийся сотрудник, например, ИТ, директор или бухгалтер, напоследок перечисляют на свой счёт деньги компании.

Лица, совершающие внутреннее мошенничество, мотивируют свои действия тем, что хотят больше денег, делают назло своим руководителям, пытаются таким образом рассчитаться со своими долгами...

* * *

Таким образом, можно составить общий портрет мошенника, атакующего юридических лиц. Под «маской» оказывается организованная группа лиц с распределёнными ролями, обладающая техническими, психологическими и финансовыми навыками. Эти люди имеют необходимые инструменты для взлома, обладают инсайдерской информацией, умеют скрывать следы своей деятельности. И — главное — имеют терпение месяцами выжидать удобного случая для вывода денежных средств.

ВЫУЧЕННЫЙ ИНСАЙД

КОГДА УЩЕРБ КОМПАНИИ НАНОСЯТ
ЛОЯЛЬНЫЕ СОТРУДНИКИ

Крупные компании всё чаще выявляют сотрудников, которые своими действиями создают угрозу информационной безопасности, причём лишь незначительная часть из них делает это по незнанию. Все остальные действуют с полным пониманием того, что нарушают инструкцию.

Среди понимающих нарушителей можно встретить два основных мотива, которые побуждают их поступать неправильно. Как ни парадоксально, эти мотивы прямо противоположны друг другу: одни нарушают, чтобы получить личную выгоду, другие — чтобы создать больше ценности для компании.

ИНСАЙДЕРЫ И ИНСАЙДЕРСКИЕ УГРОЗЫ

Сотрудника, который своими действиями или бездействием, умышленно или неосознанно причиняет вред организации, в которой работает, называют *инсайдером*. Этот человек имеет доступ к информационной системе и может совершать различные действия в отношении одного или нескольких информационных активов компании.

Например, он может отправить письмо с информацией о планируемой сделке конкурентам и сорвать её, либо некорректно начислить проценты за обслуживание клиенту, который негативно настроен к банку, в результате чего клиент переведёт свои средства в другую финансовую организацию.

В зависимости от действий, которые выполняет или не выполняет инсайдер, различают три основных типа *инсайдерских угроз*¹:

- ◆ Злоупотребление доступом.
- ◆ Обход защиты.
- ◆ Ошибки в настройке прав.

Злоупотребление доступом означает, что сотрудник, имеющий соответствующие его должности права использования различных систем,

использует их таким образом, что прямо или косвенно наносит вред компании. Это самая сложная в обнаружении угроза, поскольку обнаружить её техническими средствами практически невозможно — инсайдер имеет вполне легитимный доступ к системе и действует, находясь в рамках предоставленных ему полномочий.

Обход защиты предполагает, что инсайдер использует различные технические средства, чтобы добиться своей цели.

Ошибки в настройке прав приводят к тому, что инсайдер получает доступ к ресурсам, которые не требуются ему для выполнения служебных обязанностей. Обнаружив такую ситуацию, он не только не сообщает об этом в отделы ИТ или ИБ, а напротив, пользуется ситуацией для своих целей.

Рассмотрим, как выглядит инсайдерская атака.

МОДЕЛЬ ИНСАЙДЕРСКОЙ АТАКИ

Наиболее наглядный и исчерпывающий вариант моделирования инсайдерской атаки предложили британские исследователи², выделив четыре основных компонента (рисунок 1):

- ◆ Катализатор инсайдерской угрозы;
- ◆ Характеристика исполнителя (инсайдера);
- ◆ Характеристика атаки / инсайдерской угрозы;
- ◆ Характеристика организации / условия реализации инсайдерской угрозы.

Катализатором инсайдерской угрозы является поворотное событие, «переломный момент», который подталкивает потенциального инсайдера стать действующим инсайдером. К катализаторам можно отнести:

- ◆ события внутри компании (увольнение, ссора с работодателем или коллегами, столкновение с несправедливостью и т.п.);
- ◆ события в личной жизни инсайдера (семейные проблемы, проблемы со здоровьем, появление новых возможностей и т.п.).



Ольга ЛИМОНОВА
психолог
ООО «Антифишинг»



Андрей ЖАРКЕВИЧ
редактор
ООО «Антифишинг»

¹ S. M. Bellovin, The Insider Attack Problem: Nature and Scope. Springer, 2008, ch. in [71].

² J. R. C. Nursey, O. Buckley, P. A. Leggy, Michael et al, «Understanding Insider Threat: A Framework for Characterising Attacks», IEEE Computer Society, 2014.

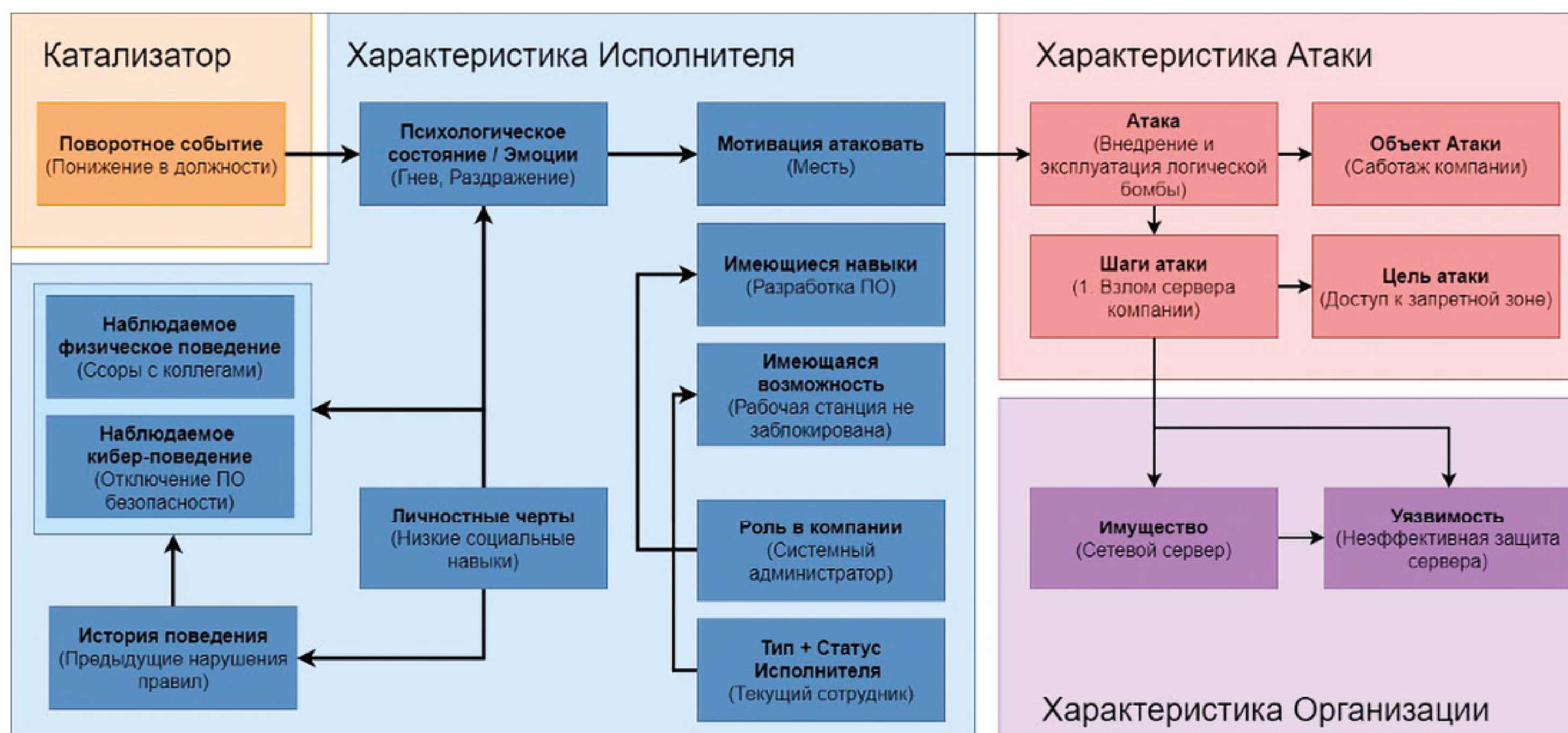


Рисунок 1. Модель инсайдерской атаки

Характеристика исполнителя представляет собой совокупность личных особенностей инсайдера, таких как личностные черты, психологическое состояние, поведенческие паттерны, мотивация, профессиональные навыки и статус в компании.

В Характеристику атаки входят опасные действия, которые может совершить инсайдер, сознательно или случайно. Данные характеристики определяют объект и цель самой атаки.

И последний компонент — Характеристика организации, в которые входят активы, предметы, представляющие ценность для компании и интерес для инсайдера, а также уязвимости, слабые места в активах или средствах контроля, защищающих их.

Данная модель ценна тем, что позволяет спроектировать любой тип инсайдерской угрозы и составить характерологические портреты для выявления потенциальных инсайдеров, а также сценарии их действий в рамках организации.

ХАРАКТЕРИСТИКИ КЛАССИЧЕСКИХ ИНСАЙДЕРОВ

Чтобы успешно выявлять и профилировать инсайдеров внутри компании, нужно понимать мотивирующие факторы, черты личности и особенности наблюдаемого поведения сотрудников.

Злонамеренные инсайдеры — это классический тип инсайдеров, чьи действия направлены на нанесение умышленного ущерба компании.

Мотивирующими факторами здесь являются:

- ♦ месть — в 56 %–86 % случаев;

- ♦ финансовая выгода;
- ♦ неудовлетворённость политикой компании (идеологические причины);
- ♦ нереализованные ожидания — плохие отношения с коллегами, отсутствие продвижения по службе, понижение в должности, уменьшение ответственности;
- ♦ стрессовые события, например, введение организационных санкций;
- ♦ желание перенести информацию на новое место работы;
- ♦ желание угодить в случае вербовки знакомыми или родственниками;
- ♦ наличие долгов;
- ♦ наличие проблем, связанных с наркотиками.

Основные цели злонамеренных инсайдерских атак — саботаж (47 % случаев) и финансовая выгода от кражи информации (42 % случаев).

Общие черты злонамеренных инсайдеров, которые оказываются статистически значимыми:

- ♦ мужчины, большинство из которых на момент атаки не состояли в браке;
- ♦ средний возраст от 35 до 45 лет. Связь между личной и профессиональной жизнью в этот период имеет наибольшее значение, на этот период приходится пик разводов и карьерных перемен;
- ♦ 38 % были арестованы ранее;
- ♦ около 50 % инсайдеров на момент атаки работали в компании, причём эта доля выше при кражах информации. Оставшаяся часть — бывшие сотрудники;
- ♦ более 50 % работали в организации на технических должностях.

Психологические черты, которые обычно свойственны злонамеренным инсайдерам, это:

- ◆ серьёзные психические расстройства — приступы паники, наркотическая и алкогольная зависимость;
- ◆ низкие социальные навыки;
- ◆ склонность к эскалации конфликтов;
- ◆ постоянное недовольство чем-либо в работе;
- ◆ проблемы с управлением гневом, агрессивность;
- ◆ макиавеллизм, нарциссизм, психопатия («Тёмная триада»);
- ◆ интровертность, самоизолированность от коллектива;
- ◆ социальная и личная разочарованность;
- ◆ этическая гибкость;
- ◆ низкая лояльность;
- ◆ чувство собственной правоты в сочетании с гневом, направленным на власть;
- ◆ отсутствие эмпатии.

Считается, что наличие у сотрудника сразу нескольких психологических особенностей из перечисленных говорит о его потенциальной опасности.

Наблюдаемое поведение злонамеренных инсайдеров:

- ◆ прогулы;
- ◆ ссоры с коллегами;
- ◆ трудности с соблюдением правил на рабочем месте;
- ◆ неадекватные реакции на стресс;
- ◆ плохая результативность;
- ◆ в 46 % случаев коллеги, знакомые, члены семьи и друзья обладали информацией о предстоящей атаке, но не признавали серьёзность заявлений и игнорировали необычное поведение.

Таким образом, поведение классических злонамеренных инсайдеров обладает набором вполне конкретных характеристик, которые позволяют выявить их с достаточной степенью достоверности. Однако помимо классических инсайдеров, совершающих вредоносные действия, отслеживается тенденция к появлению другой разновидности опасных для организации сотрудников — *выученных инсайдеров*.

ВЫУЧЕННЫЕ ИНСАЙДЕРЫ

Выученный инсайдер — это вполне лояльный к компании сотрудник, который в силу собственных убеждений нарушает требования информационной безопасности, что может привести и во многих случаях приводит к утечкам конфиденциальных данных, финансовому ущербу и другим проблемам. Главное отличие выученного инсайдера от классического злонамеренного состоит в том, что он совершает эти дей-

Выученные инсайдеры

не появляются на пустом месте.

Их рождение — результат наложения организационных особенностей на личностные качества сотрудников

ствия, искренне считая, что таким образом помогает организации достигать лучших результатов.

Выученные инсайдеры не появляются на пустом месте. Их рождение — результат наложения организационных особенностей на личностные качества сотрудников. Рассмотрим, как происходит формирование выученного инсайдера.

Пугливый новичок

Сотрудник только принят на работу. Он в восторге от того, что его выбрали, что прошёл все круги собеседований и проверку службы безопасности. Впереди — стабильная зарплата за усердный труд на благо развития бизнеса.

На коллег смотрит с уважением и опасением. Из всех сил старается не ударить в грязь лицом, показать себя с лучшей стороны, ведь испытательный срок — как экзамен, только растянутый на долгие три месяца.

Каждый назначенный учебный курс и направленный на ознакомление нормативный документ пристально изучается. За разъяснением непонятных моментов он пытается обратиться к коллегам, но в основном от него отмахиваются, либо недоумённо пожимают плечами — не задумывались, не помнят, не обращали внимания на такие тонкости, в работе не требуется.

Постепенно новичка всё больше загружают работой, времени вникать в детали не остаётся, он убеждается, что для выполнения плана всё это и в самом деле не требуется, а если и требуется, то очень редко, так что лучше позвонить ещё одному клиенту, сделать дополнительную отметку в CRM, чтобы улучшить свои ключевые показатели эффективности. Так пугливый новичок переходит на следующий этап развития, который можно назвать «Сомневающийся боец».

Сомневающийся боец

Сотрудники, успешно продержавшиеся испытательный срок и не испугавшиеся огромного объёма свалившейся на них разнообразной работы, из пугливых новичков превращаются в бойцов. У них рождается сомнения по поводу бизнес-процессов, в которых им приходится участвовать. Поскольку они не видят ситуацию целиком, им начинает казаться, что принятые

в банке процедуры страдают излишним формализмом, это мешает бизнесу и в конечном счёте сказывается на их эффективности, а значит, они получают премию меньше, чем если бы всё работало как часы.

Эти сомнения бродят у них в сознании, изредка принимая форму недовольства, осторожно высказываемого на командообразующих мероприятиях, в спортбарах и других заведениях с алкоголем. Озвучивать их на совещаниях, где подводят итоги месяца или квартала, они пока не решаются, поскольку не набрали достаточно опыта, чтобы их мнение принимали во внимание.

Уверенный воин

Систематическое применение обходных процедур для ускорения решения вопросов стало привычной частью бизнес-процессов, заменив регламенты безопасности, содержащиеся в нормативных актах. Воин бизнеса ловко раскручивает воронку продаж и спокойно идёт на нарушения, поскольку совершенно уверен, что время — деньги, победителей не судят, поэтому ему никто ничего не скажет, если он будет выполнять и перевыполнять бизнес-план.

На общих собраниях воин свободно высказывается по поводу ненужных формальностей, мешающих достижению целевых финансовых показателей, и временами даже получает поддержку со стороны руководства.

Убеждённый инсайдер

На этой стадии сотрудник, как правило, уже вырастает по карьерной лестнице до руководителя среднего звена или даже топ-менеджера. Приобретённые им навыки пренебрежения безопасностью становятся не просто нормой жизни, а обычаем бизнес-практики. Подчинённые получают рекомендации придерживаться нормативных актов банка, но не до фанатизма, чтобы не парализовать работу.

С коллегами, отвечающими за информационную безопасность, проводятся доверительные беседы, цель которых — убедить пойти навстречу и не обращать внимания на «незначительные» нарушения, «ведь все решают общую задачу».

ВЫУЧЕННЫЙ ИНСАЙД В «ДИКОЙ ПРИРОДЕ»

Рассмотрим реальную историю превращения вполне лояльных сотрудников в инсайдеров.

В крупном банке из ТОП-3 имеется нормативный акт, с которым ознакомлены все сотрудники. В соответствии с ним сообщать клиентам процентную ставку по электронной почте или



по телефону строго запрещено, поскольку такая информация относится к разряду банковской тайны, и её передача по открытым каналам связи недопустима.

Условия привлечения или размещения средств — это один из самых распространённых вопросов, которые клиентские менеджеры получают от действующих и потенциальных клиентов. Изменение ключевой ставки ЦБ РФ мгновенно создаёт поток запросов на корректировку действующих ставок по кредитам и депозитам.

Чтобы ответить клиенту, сотрудник должен согласовать новую ставку с ответственными подразделениями, а для отправки сообщения придётся использовать защищённую почту, либо распечатать письмо на фирменном бланке, подписать у руководителя, зарегистрировать в системе электронного документооборота, заказать такси и отвезти клиенту.

Если бы клиентский менеджер работал с одним-единственным клиентом, такую схему работы с большой натяжкой можно было бы



назвать уместной и оправданной. Однако в реальности каждый клиентчик взаимодействует с десятками организаций, поэтому он просто не может себе позволить роскошь действовать по такой процедуре. И даже защищённый документооборот или банк-клиент не всегда спасает положение.

Чтобы не попасть под санкции службы ИБ, клиентчики поступают проще: они фотографируют согласованную ставку на смартфон и отправляют её клиенту в WhatsApp или другой мессенджер. Обнаружить такие действия служба безопасности в общем случае не может, поэтому никаких последствий не бывает.

Клиент доволен, сотрудник тоже — он сэкономил рабочее время и сохранил хорошие отношения с бизнес-партнёром.

По идее ситуация выглядит как вин-вин — в плюсе как клиент, так и банк. Но если взглянуть глубже, обозначаются проблемы:

1. Сотрудник привыкает к мысли, что нормативные акты по безопасности — это что-то мешающее реальной работе, а поэтому можно и

нужно использовать все средства, чтобы решить вопрос наиболее простым способом.

2. Клиент привыкает, что взаимодействие с банком происходит не по правилам, а в соответствии с его требованиями, поэтому попытки вернуть взаимодействие в рамки регламента неизбежно встретят сопротивление.

3. Воодушевлённый мыслью, что всё делает правильно, сотрудник будет всё шире использовать практику обхода ограничений, поскольку он работает, чтобы принести максимум пользы в единицу времени.

Фактически у вполне лояльного сотрудника развивается отношение к ИБ, свойственное скорее для инсайдера. В конечном счёте это неизбежно приведёт к инциденту, виновником которого будет данный лояльный сотрудник.

Особая опасность такого выученного инсайда состоит в том, что сотрудник уверен в своей правоте, поэтому менее подозрителен и внимателен. А ещё он неизбежно будет применять свои «навыки» и после перехода в другую организацию, создав инсайдерские угрозы на новом месте.

ВЫЯВЛЕНИЕ ВЫУЧЕННЫХ ИНСАЙДЕРОВ

Учитывая риски, которые создают выученные инсайдеры, а также степень влияния на менее опытных сотрудников, крайне важно своевременно выявить их присутствие в организации и создать понимание того, каким образом можно спрогнозировать их появление.

Среди наиболее характерных качеств выученного инсайдера можно выделить следующие:

- ♦ высокий уровень лояльности к организации;
- ♦ большой опыт работы;
- ♦ трепетное отношение к решению бизнес-задач;
- ♦ пренебрежение любыми ограничениями, мешающими достижению бизнес-целей;
- ♦ хорошие показатели исполнения плана;
- ♦ дружеские отношения с клиентами и коллегами;
- ♦ уверенность в том, что небольшие нарушения ради достижения цели вполне допустимы.

Если задуматься, эти качества можно обнаружить у каждого успешного клиентского менеджера. Однако далеко не все они становятся выученными инсайдерами. В чём же дело?

Наиболее вероятной причиной такой трансформации является многократное положительное подкрепление нарушений правил безопасности, которое сотрудник получал в течение своей трудовой карьеры. Если бы этот путь к вершине прервался на начальном этапе, и потенциальный инсайдер получил наказание за несоблюдение правил, у него бы сформировалось другое отношение к требованиям ИБ.

Вторая причина состоит в том, что во многих случаях соблюдение всех нормативных документов действительно вступает в конфликт с интересами бизнеса. Однако в этом случае проявление лояльности должно состоять скорее в том, чтобы инициировать пересмотр устаревших требований и разработки удобных и безопасных процедур, а не в том, чтобы допускать систематические нарушения, оправдывая себя тем, что «по правилам работать невозможно».

КАК ИЗБЕЖАТЬ?

Учитывая риски, которые создают инсайдерские действия лояльных сотрудников, необходимо принимать максимум возможного для предотвращения или снижения вероятности появления выученных инсайдеров.

Среди таких мер необходимо отметить:

1. Систематическое отслеживание исполнительской дисциплины.

2. Внезапные проверки соблюдения требований ИБ.

3. Показательные наказания сотрудников, нарушивших регламенты.

4. Проведение реинжиниринга бизнес-процессов для выявления ИБ-процедур, затрудняющих взаимодействие с клиентами и снижающих эффективность достижения плановых показателей. Процессы, которые не принимают во внимание удобство исполнения и эффективность, скорее всего, приведут к распространению небезопасных рабочих практик, то есть к появлению выученных инсайдеров.

5. Привлечение потенциальных выученных инсайдеров к разработке новых процедур обеспечения безопасности при выполнении бизнес-задач.

6. Обязательную проверку биографической информации при найме сотрудников.

7. Психологическое тестирование при найме на работу с использованием:

- ♦ пятифакторного опросника личности (Big-5);
- ♦ теста «Тёмная Триада» (SD 3).

8. Включение в учебную программу по ИБ курса по выявлению инсайдерской угрозы среди коллег. Важно, чтобы сотрудники знали, что делать, если они наблюдают чужое небезопасное поведение.

9. Внедрение в корпоративную систему мотивации поощрения персонала к бдительности и внимательности к угрозам, которые могут исходить от других сотрудников.

10. Создание программы помощи уязвимым сотрудникам. Если сотрудники сталкиваются с какой-либо формой личного кризиса, рекомендуется поощрять сотрудников обращаться за помощью. Обратная связь, полученная от лиц, совершивших акты шпионажа, свидетельствует о том, что раннее вмешательство могло бы предотвратить эти действия.

* * *

Инсайдеры и инсайдерские угрозы — сложное и многогранное явление, исследования которого ведутся во всём мире. Выученный инсайдер опасен ничуть не меньше, чем злонамеренный, поскольку его действия создают риски для компании, среди которых могут быть как репутационные, так и финансовые. Именно поэтому руководству кредитных учреждений следует выделить ресурсы для выявления потенциальных выученных инсайдеров и предотвращения их появления.

У самого выхода Польшаев схватил Остапа за рукав и пролепетал:
— Я ничего не утаил. Честное слово. Я могу быть спокоен. Правда?
— Полное спокойствие может дать человеку только страховой полис, — ответил Остап, не замедляя хода. — Так вам скажет любой агент по страхованию жизни. Лично мне вы больше не нужны. Вот государство, оно, вероятно, скоро вами заинтересуется.

«Золотой телёнок», Ильф и Петров

БОРЬБА С ИНСАЙДОМ В СТРАХОВАНИИ

РЕАЛЬНЫЕ КЕЙСЫ — НЕ ДОГМА,
А РУКОВОДСТВО К ДЕЙСТВИЮ

Страховой бизнес в мире и России даёт хлеб сотням тысяч, а может быть, и миллионам людей. Некоторым из них, вовсе не топ-менеджерам, он даёт не только возможность заработать на жизнь, но и завершить карьеру вполне обеспеченным человеком, уволиться и уехать в светлое будущее на новеньком Бэнгли.

Отдав работе в страховании в сфере ИБ годы, могу с убеждением сказать, что основная угроза в страховании — это не мифические хакеры, а собственные сотрудники, иными словами инсайд.

СПЕЦИФИКА РЫНКА

Страховой бизнес имеет собственную неповторимую структуру: тысячи сотрудников, 80 процентов которых имеют прямое или косвенное отношение к продажам, к «живым деньгам». Армия агентов, быстрорастущее слабоконтролируемое ИТ, массивные базы данных, легко конвертируемые в деньги. Всё вышперечисленное осложняется подходом «ты здесь хозяин, а не гость, тащи с работы каждый гвоздь», т.е. менталитетом.

Схемы обмана страховой компании возникли ещё в ранние годы становления рыночной экономики и с тех пор активно растут и развиваются.

Я расскажу об основных схемах внутренних мошенничеств, с которыми довелось столкнуться на практике, а также о методиках их выявления и предотвращения. Описанные далее кейсы не претендуют на полноту, однако, по моему мнению, отражают наиболее критичные проблемы инсайда в страховой компании. Конкрет-

ные технические решения находятся за рамками данной статьи и потребуют отдельного описания. Некоторые из схем на текущий момент могут потерять актуальность в деталях, хотя и остаются рабочими в целом.

Но прежде чем перейти к практическим кейсам, хотелось бы привести основные тезисы, фундамент, который, по моему мнению, поможет коллегам из ИБ по счастью работающим в страховании (безумный вал проблем даёт не только головную боль, связанную с их решением, но и возможности профессионального роста).

DLP-система ваш главный друг — полноценно внедрённая, правильно настроенная DLP-система даёт возможность выявлять нездоровые схемы на самом раннем этапе их появления.

Видимость бизнес-процессов — для чёткого понимания бизнес-процессов и их странностей исключительно важно видеть происходящее в деталях, иметь возможность оценивать данные системно.

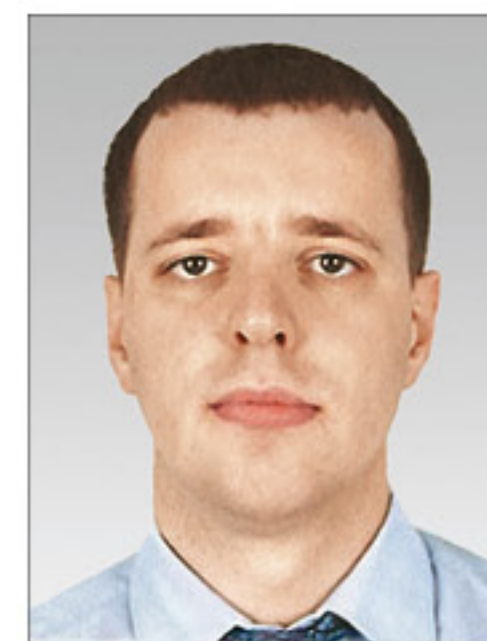
ДАМ-система — дополнит DLP, даст возможность привязать частное к общему.

РАМ-система — заранее отпугнёт нечистых на руку партнёров, создаст базу для расследования в будущем.

И наконец, информационную базу для расследования происходящего в мельчайших деталях даст грамотно настроенное **логирование всех ИТ-систем**.

ТИПИЧНЫЕ КЕЙСЫ

Утечка пролонгаций. Информация об утечках персональных данных постоянно появляется



Александр ПАЛЬЦЕВ
начальник
отдела ИБ
АО Русагротранс

	A	B	C	D	E	F	G
1	НОМЕР	ФИО	ТЕЛЕФОН	ПРЕМИЯ	ДОГОВОР		УБЫТКИ
2	002-2111-PP	Пархоменко Сергей Владимирович	89167384665	34016.44	03.01.2019	2/30/2020	0
3	012-6131-HP	Кузьмин Алексей Александрович	89064526816	61739.8	03.01.2019	2/30/2020	0
4	122-776-PP	Ким Екатерина Викторовна	9258842254	105431.65	03.01.2019	2/30/2020	0
5	091-2211-PP	Уланова Екатерина Юрьевна	89166344877	52593	03.01.2019	2/30/2020	1
6	100-8890-PP	Дмитриев Денис Юрьевич	89164488378	85582.91	03.01.2019	2/30/2020	0
7	002-66227-PP	Горский Сергей Павлович	9160222345	97446.34	03.01.2019	2/30/2020	0
8	091-8871-PP	Мельниченко Денис Юрьевич	9654332324	28111.68	03.01.2019	2/30/2020	0
9	002-99881-HP	Курпатова Анна Борисовна	9175556773	55545.62	03.01.2019	2/30/2020	0
10	122-00091-PP	Гладких Павел Юрьевич	89193344344	36201.06	03.01.2019	2/30/2020	0

Рисунок 1. Фрагмент продаваемой базы (все данные вымышленные)

в СМИ. Так, например, согласно данным МФИ софт¹, в 2017 году на открытых пиратских форумах в интернете для приобретения были доступны 5,7 млн записей данных россиян, клиентов страховых компаний.

Наиболее распространённым товаром на чёрном рынке в страховании являются так называемые базы пролонгации — ежемесячные нарезки данных клиентов, которым по окончании месяца необходимо продлевать договора страхования, обычно моторного страхования — КАСКО, ОСАГО (рисунок 1).

Приведённая база разбивается на сегменты с «уникальными» клиентами в каждой.

Каждый сегмент, на какой-то процент, в зависимости от честности продавца, разбавляется неуникальными данными или мусором, обычно на 10–20% повышая прибыль продавца. Стоимость одного сегмента базы начинается обычно от 20 000 рублей. Процесс разбавления информации аналогичен разбавлению наркотиков, хорошо известному нам по кинематографу.

Каждое появление подобной базы больно бьёт по бизнесу, так как наиболее вкусные, высокомаржинальные клиенты уходят из компании, казалось бы, без причины.

Разумеется, утечки информации затрагивают репутацию компании, имеют серьёзные последствия со стороны закона.

Решение. Проблему решает тесное взаимодействие с оперативными сотрудниками безопасности и компетентными органами, подкреплённое информационной поддержкой ИБ.

Выставленные на продажу базы выкупаются и анализируются на признаки, позволяющие понять источник информации. По опыту, большинство продаваемых на рынке баз получены не через «слив», а лишь являются агрегирован-

ными, переформированными (насыщенными из других источников) данными партнёров — автосалонов, агентов, брокеров. Система даёт сбой там, где защита наиболее слаба.

В том случае, когда в данных имеются признаки целевого слива, информация анализируется на предмет поиска потенциального источника — сотрудника, департамента, партнёра.

Тот факт, что базы должны быть актуальны и привязаны к конкретному периоду пролонгации не только делает базы востребованным товаром, но и оставляет чёткий след, ведущий к инсайдеру.

Продуманный стек политик DLP-системы, при условии её комплексного внедрения, даст достаточно информации для восстановления схемы слива в деталях, а чёткое понимание инцидента позволит скорректировать политики компании либо устранить техническое несовершенство информационных систем.

Занижение мощности в моторном страховании. Случаются ситуации, когда, например, люксовый внедорожник согласно данным страхового полиса оснащён двигателем в 60 л.с или, например, грузовой Камаз имеет грузоподъёмность 2 тонны. Нередко владелец авто оказывается зарегистрирован в регионе, имеющем заниженные коэффициенты ОСАГО.

Во внутренних информационных системах при этом, явно некорректные данные полиса будут подтверждены скан-копиями документов. Стоимость полиса для клиента значительно снижается, а разница либо делится с клиентом, либо присваивается без его ведома.

Клиент часто выявляет несоответствие страхового полиса реальности уже после попадания в ДТП. И несмотря на то что верховный суд признал подобные полисы действительными², головной боли клиенту не избежать.

¹ <https://www.vedomosti.ru/technology/articles/2017/09/27/735622-poyavilis-dannie-strahovih-kompanii>

² <https://rg.ru/2017/12/21/vs-raziasnil-chto-neverne-dannye-ne-delaiut-polis-osago-nedejstvitelny.html>

Решение. Тот факт, что введённые в информационные системы полисы проходят внутренний контроль, заставляет агента или штатного продавца изменять скан-копии документов транспортного средства, подгоняя их под полис.

Как показывает практика 90 % подделок скан-копий выполняется штатными сотрудниками непосредственно на рабочем месте незамысловатыми средствами — графическим редактором Microsoft Paint, либо через сайты конвертирования JPG-PDF. Наиболее искушённые «специалисты» используют практику пересканирования, изменяя документы в процессе.

Системный анализ баз данных позволяет массово выявлять автомобили, имеющие странности, отличающие их от заводских показателей.

DLP-система, при правильной настройке, даёт возможность выявить подделку скан-копий документов авто ещё до загрузки в информационные системы компании.

Автоюризм. Проблема ставшая актуальной для страховых компаний в последние годы. Приводит к значительным убыткам компании, и, что более важно, разрушает доверие клиентов.

Юридические конторы, опирающиеся на аффилированных экспертов, зачастую с поддержкой в судах, специализируются на судебных процессах против страховых компаний, обычно в моторном страховании. Так, по данным портала asn-news со ссылкой на PCA, общая сумма возмещений по решению суда в 2017 году достигла 37,4 млрд руб., что составило 18,2 процента от общего объёма страхового возмещения³.

Наиболее типичный пример — истребование УТС (Утрата Технической Стоимости) по формальным признакам по ранее урегулированным убыткам. Для претензий выбираются убытки, находящиеся на крайнем сроке закрытия производства. Задача автоюриста заключается в поиске ранее урегулированного убытка, с высокими шансами победы в суде при наличии «своей» экспертизы, выход на контакт с клиентом и заключение цессии. Разумеется, для выполнения экспертизы необходим максимально полный комплект документов по убытку, фото материалы.

Основная прибыль автоюриста генерируется затребованием УТС транспортного средства, которая увеличивается с течением времени. Расчёт обычно строится следующим образом: 5–6 тыс. руб. — договор цессии, 2–3 тыс. руб. получает сотрудник «в полях», обзванивающий клиентов и заключающий цессию, 10 тыс. уходит эксперту. Прибыль же может составлять до 300 000 тыс. руб. в самых успешных случаях.

В передаче информации по клиентам часто оказываются замешаны партнёры компании, которым делегируется процесс урегулирования убытков. Нередко и внутренние сотрудники юридического департамента не против заработать на афере.

Решение. Тщательный контроль использования УЗ внутренних систем позволяет выявить сотрудников, интересующихся делами, к которым не имеют служебного отношения.

РАМ-система с поддержкой нормативной базы заранее отпугивает нерадивых партнёров, даёт основу для расследования инцидентов в будущем.

В последнее время прибыльность схемы уравновешивается строгостью наказания, уже появились механизмы привлечения аферистов к уголовной ответственности.

Закладки. Наличие во внешних веб-сервисах так называемых закладок довольно редкая проблема, которая, тем не менее стала появляться всё чаще во многих сферах бизнеса.

Закладка — это заложенная в информационных системах компании недокументированная функция, через которую уже уволенный сотрудник или партнёр может сливать информацию по клиентской базе «на лету», со всеми удобствами присущими интернету.

Так, например, на внешнем b2b может быть размещён скрипт поиска произвольной информации по клиентам. Закладка, попав в релиз сервиса, становится его частью на годы вперёд, даёт возможность построить бизнес-паразит на базах компании.

Решение. Продуманный, документированный процесс SDLC (жизненный цикл разработки программного обеспечения) сдержит нечестных сотрудников разработки, предотвратит добавление вредоносного кода.

Анализ работы информационных систем, их обращений к базам данных выявит нелогичные или необоснованные обращения.

В ЗАВЕРШЕНИЕ

Подводя итог, повторю основные моменты и фундамент, опираясь на который, можно успешно противостоять инсайду в страховании:

- ♦ полная видимость технических аспектов работы бизнес-процессов;
- ♦ контроль действий сотрудников и партнёров на рабочих местах и в информационных системах;
- ♦ пошаговое изучение инцидентов, применение опыта (тех самых Lessons Learned) для выявления цельной картины и предотвращения инцидентов в будущем.

³ <http://www.asn-news.ru/news/65933>

«ПРЕДОТВРАЩАТЬ ИНСАЙДЕРСКИЕ ИНЦИДЕНТЫ — ЗАДАЧА НЕПРОСТАЯ. НО И НЕ ФАНТАСТИЧЕСКАЯ»



Лев МАТВЕЕВ
председатель
совета директоров
«СёрчИнформ»

83 % представителей банков признают, что инсайдерские угрозы создают больше рисков, чем внешние. Несмотря на это в банках по-прежнему часто недооценивают важность внедрения ПО для защиты от внутренних угроз. Почему директивы ЦБ не мотивируют изменить ситуацию? Как выглядит система защиты банка, данные клиентов которого невозможно купить в даркнете? Рассказывает председатель совета директоров «СёрчИнформ» Лев Матвеев.

— В этом году вы выпустили исследование¹ с громким выводом, что банки и медкомпании теряют данные чаще всего. Исследование рисует довольно суровую картину. Так ли все страшно?

— Главный неутешительный вывод, что банки в лидерах среди компаний, которые теряют персональные данные. Это 47 % всех утечек, в два раза больше, чем в среднем по другим отраслям. Конечно, это опасная тенденция, ведь банки собирают и хранят наиболее чувствительные данные о россиянах.

— Больше утечек, потому что активнее выявляют?

— В этом есть правда. Банки больше другого бизнеса уделяют внимание защите данных, есть жесткое регулирование. Поэтому общий уровень защиты от киберрисков выше. Но это справедливо только в плане защиты от внешних мошенников. Вопрос инсайдерских рисков не закрыт. Мне придется долго перечислять слабые места документов ЦБ в подтверждение этому тезису. Для краткости обобщу: стандарты в плане защиты от внутренних рисков даны рамочно, а контроль исполнения даже этих неполных требований не описан. Получается, что необходимость защиты от инсайдеров не директива, а рекомендация.

Результат налицо: сервисы по вербовке инсайдеров в банках работают в русскоязычном сегменте даркнета практически открыто, мож-

но купить данные и владельца платиновой карточки, и пенсионной. Каждый сталкивается с угрозой стать жертвой мошенника. Это ненормальная ситуация.

— А сами банки — они мотивированы по рекомендациям ЦБ применять защитное ПО?

— Малая часть «сознательных банков» — безусловно да. Но кто-то рассуждает: «За это не штрафуют. Пронесет». Добавим к этому, что клиенты банков не предъявляют гражданские иски по фактам утечек, хотя, уверен, и до этого дойдет рано или поздно.

Но ведь утечки — это только вершина айсберга. Инсайдеры часто и сами организуют схемы, которые наносят клиентам (а через них и банкам) прямой финансовый ущерб. Сотрудники снимают деньги со счетов, о которых клиент, вероятно, забыл; подменяют телефонные номера в карточках клиентов, чтобы незаметно вывести средства; открывают счета, чтобы «прогонять» по ним деньги. Из самого безобидного, что встречали наши аналитики, — сообщения «по дружбе» о том, сколько денег на счете у бывшего мужа.

Все это выливается в большие хлопоты, ведь новости о сливах и махинациях сотрудников все чаще просачиваются в СМИ и создают имиджевый ущерб, банкам приходится обращаться в суд, чтобы наказать инсайдера — 31 % это делают.

— Но ведь банки себе не враги, чтобы создавать хлопоты по расследованиям, судебным тяжбам...

— Конечно, в банках хорошо осознают риски. Но в вопросах защиты организации часто находятся в иллюзии контроля, ставя ИБ-решения в недостаточном объеме. Например, обеспечивают DLP-системами 2 тысячи ПК из 10 тысяч. Логика такая: «мы контролируем 10–20 % персонала на самых критичных местах». Это луч-

¹ <https://searchinform.ru/research-2019/>

Стандарты в плане защиты от внутренних рисков даны рамочно, а контроль исполнения даже этих неполных требований не описан

ше, чем ничего, но в целом это неверная практика. Закрывать парадную дверь, оставляя при этом открытым черный ход и окна заодно — так себе стратегия.

Предотвращать инциденты — задача хоть непростая, но и не фантастическая. А ведь есть образцы ответственной работы, вы это можете видеть по предложению в даркнете — данные некоторых банков очень сложно или невозможно купить.

— **Давайте тогда поговорим о том, какой должна быть образцовая организация защиты данных?**

— В выстраивании защиты от инсайдерских рисков нужен комплексный подход. Достаточно двух элементов: качественное ПО и профессиональная служба безопасности. Просто поставить программу и забыть — нельзя, с ней нужно работать.

Что касается защитного ПО. DLP-система контролирует перемещение информации, документов и файлов по всем популярным каналам — от корпоративной почты и флешек до мессенджеров и облачных хранилищ. Это также программа для расследований, чтобы собрать информацию по случившемуся или готовящемуся нарушению. Как мы видим из материалов судебных дел против инсайдеров-нарушителей, данные из DLP-систем постоянно фигурируют как доказательства.

Но в банках есть иные внутренние проблемы. Функционала DLP для их решения не хватает, нужны другие классы софта. DСАР — для аудита файловой системы, программа классифицирует информацию по степени критичности, показывает, кто имеет к ней доступ. В случае с банками актуальнее всего задача по персональным данным. DAM-решение выявляет обращения и манипуляции с информацией в базах данных. Тут тоже далеко за примером ходить не нужно. Суды завалены историями, как сотрудники обращаются к карточкам клиентов, чтобы заменить номер телефона и незаметно для владельца счета вывести с него деньги.

Если в банке работает комплекс решений из DLP, DAM и DСАР, можно говорить о защите на основных уровнях: баз данных, файлов, каналов передачи информации.

— **Вы развиваете линейку своих продуктов именно в этом направлении?**

— Да, помимо нашего флагмана DLP-системы «СёрчИнформ КИБ» мы вывели на рынок систему файлового аудита «СёрчИнформ FileAuditor». Сделали это в прошлом году и очень вовремя, заказчикам была нужна отечественная разработ-

В вопросах защиты организации часто находятся в иллюзии контроля, ставя ИБ-решения в недостаточном объеме. Например, обеспечивают DLP-системами 2 тысячи ПК из 10 тысяч

ка, до нашего решения на рынке были представлены только зарубежные аналоги. В этом году мы готовим к релизу DAM-систему «СёрчИнформ DataBase Monitor». Она в автоматизированном формате будет фиксировать все изменения в базах данных — добавление, удаление, изменение информации.

Заказчики также внедряют наше ПО для автоматизированного профилирования сотрудников «СёрчИнформ ProfileCenter». Это продукт, который упрощает жизнь службам безопасности, потому что определяет группы риска, сильные и слабые стороны сотрудников, склонность к нарушению правил и т.п.

— **Как вы как вендор реагируете на кризис? Перестраиваете работу компании?**

— Мы делаем решения экономичнее, вендоры обязаны идти по пути оптимизации своего софта, особенно в нынешних условиях. Еще в прошлом году мы изменили архитектуру системы, и это позволило увеличить быстродействие DLP на 30% и расширить спектр решаемых задач — искать данные в очень больших сетях, например. Раньше для этого заказчикам приходилось выделять большие ресурсы: размещать дополнительные сервера, диски. Продолжаем работы по совершенствованию интерфейса, чтобы сложную аналитику можно было проводить в несколько простых действий. Дорабатываем механизмы работы с архивом, а это значит опять же, что заказчику можно будет снизить затраты на закупку СХД и другого «железа» для работы с данными из программы.

И главное, экономичен сам наш подход — комплексность решений, которые работают в бесшовной интеграции. Это позволяет снизить затраты на персонал — не нужно раздувать штат, чтобы каждый специалист работал с одной системой.

Но я всегда призываю не верить вендорам на слово, надо проверять программы в реальных условиях вашего банка. Каждый из продуктов доступен для тестирования в полном функционале, лучше всего ставить на тест весь комплекс решений, нагрузить их максимально и сделать выводы самостоятельно. Оставьте заявку у нас на сайте.

Оставьте заявку
на месяц бесплатного
тестирования на сайте:





**Сергей
МЕЛЬНИКОВ**

заместитель
генерального
директора
ООО «Лингвистические
и информационные
технологии», кандидат
физико-математиче-
ских наук

ОПРЕДЕЛЯЕМ АВТОРА

НОВЕЙШИЕ ТЕХНОЛОГИИ ПРОТИВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В BIS Journal № 3(34)/2019 мы публиковали статью «Задача по биометрии: кто написал txt?», посвящённую современным технологиям определения авторства текста. Сегодня предлагаем краткий обзор самых современных направлений использования этих технологий в насущных задачах ИБ.

В СОЦИАЛЬНЫХ СЕТЯХ

Одной из первых систем обнаружения скомпрометированных аккаунтов в социальных сетях стала система COMPA [1], предложенная в 2015 году. Она основана на простом наблюдении: пользователи социальных сетей со временем вырабатывают привычки, и эти привычки весьма стабильны. Типичный пользователь социальной сети, например, может утром проверить сообщения с телефона, а во время обеденного перерыва с настольного компьютера. Кроме того, его сетевое взаимодействие скорее всего ограничено умерен-

ным количеством социальных сетевых контактов (друзей).

Когда аккаунт попадает под чужой контроль, поток его сообщений имеет аномалии по сравнению с типичным поведением пользователя. COMPA строит поведенческий профиль для учётных записей социальных сетей, основанный на анализе сообщений, отправленных аккаунтом в прошлом. Каждое новое сообщение сравнивается с поведенческим профилем аккаунта. Если сообщение значительно отклоняется от профиля поведения, COMPA помечает его как возможно скомпрометированное. Возможности использования особенностей авторского стиля для обнаружения скомпрометированных аккаунтов изучались в целом ряде работ (см. обзор [2]).

Специалистами из лаборатории Линкольна Массачусетского Технологического института и Мичиганского университета предложен [3] фреймворк CAUTE (Compromised Account User Tweet Encoder), который на основе предыдущих

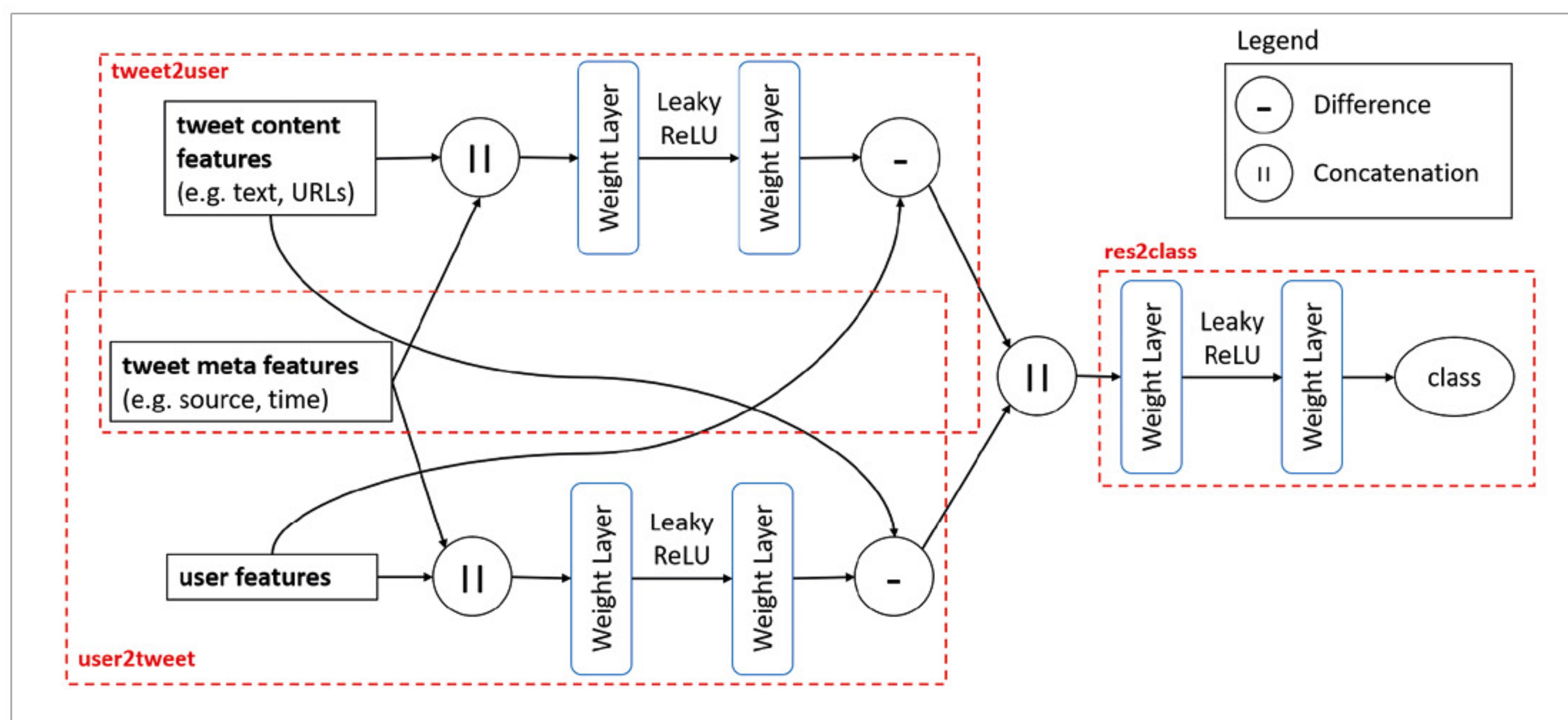


Схема работы фреймворка CAUTE (Compromised Account User Tweet Encoder) [3]

постов пользователя определяет, исходит новый пост от законного пользователя или его аккаунт уже скомпрометирован и захвачен кем-то другим. Фреймворк ориентирован на анализ материалов Твиттера. Используются глубокие нейронные сети, обучаемые на метаданных и текстах пользователя.

Качество этих и других разрабатываемых систем обнаружения скомпрометированных аккаунтов оценивается на тестовых базах сообщений. Изучаемыми характеристиками являются ошибки идентификации первого и второго родов (пропустить скомпрометированный аккаунт или принять истинный аккаунт за скомпрометированный) при следующих типовых параметрах тестовой базы: число аккаунтов около 2000, число твитов с каждого аккаунта — около 10.

БОРЬБА С ФИШИНГОМ

Фишинг с помощью электронной почты, при котором злоумышленник имитирует вызывающего доверие отправителя письма с помощью тщательно созданного сообщения и поддельных метаданных, предназначен для введения получателей почты в заблуждение. Его цель — обманом заставить жертв запустить вложение, содержащее вредоносный код, или открыть вредоносную ссылку. Такой подход иногда србатывает даже в хорошо защищённых сетях. Пользователям трудно отличить законные электронные письма от фишинговых без дополнительных защитных механизмов. Эти защитные механизмы, конечно, существуют, но могут быть неудобными для пользователей.

В ссылке [4] предложен автоматизированный подход к защите пользователей от фишинговых атак. Сначала строятся вероятностные модели как метаданных электронной почты, так и

стилометрических характеристик содержимого электронной почты. Затем последующие электронные письма сравниваются с этими моделями, чтобы обнаружить характерные признаки фишинговых атак. Возможны разные варианты реализации такого подхода, включая выполнение обучения и оценки моделей исключительно на принимающей стороне или отправителей, публикующих модели, которые могут быть проверены получателем дистанционно. В работе приводятся оценки точности предложенного подхода, рассчитанные на реальных наборах данных 20 пользователей электронной почты (до десятков тысяч писем у каждого).

ПРОТИВ ФАЛЬШИВЫХ ОБЗОРОВ

В настоящее время высокую популярность имеют сайты с публикациями мнений пользователей товаров и услуг. Одной из основных проблем является проблема нечестных публикаций, когда человеку (например, маркетологу) платят за то, что он пишет благоприятные отзывы для одного продукта или плохие отзывы для конкурента. В ссылке [5] предложен метод выявления такого типа нечестных оценок. Метод основан на технологиях определения авторства текста. Существо метода состоит в вычислении наборов попарных метрик близостей авторского стиля в текстах обзоров. Вычисленные расстояния позволяют указать группы обзоров, которые близки друг к другу по авторскому стилю, и, следовательно, могут быть нечестными. На реальных материалах обзоров отелей (число авторов — 40) достигнута точность по F1-мере более 0,66. Предложенный подход может быть использован для анализа случаев возможного мошенничества с отзывами пользователей.

ЛИТЕРАТУРА

1. Egele M., Stringhini G., Kruegel C., & Vigna G. (2017). Towards detecting compromised accounts on social networks. *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 4, pp. 447–460.
2. Barbon, S., Igawa, R., & Bogaz Zarpelão, B. (2017). Authorship verification applied to detection of compromised accounts on online social networks: A continuous approach. *Multimedia Tools and Applications*, 76(3), 3213–3233.
3. VanDam C., Masrour F., Tan P., & Wilson T. (2019). You have been CAUTE! early detection of compromised accounts on social media. In *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM '19)*. Association for Computing Machinery, New York, NY, USA, 25–32.
4. Duman, S., Kalkan-Cakmakci, K., Egele, M., Robertson, W., & Kirda, E. (2016). EmailProfiler: Spearphishing filtering with header and stylometric features of emails. In *Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference*. Vol. 1, pp. 408–416.
5. Layton, R., Watters, P., & Ureche, O. (2013). Identifying faked hotel reviews using authorship analysis. In *Proceedings — 4th Cybercrime and Trustworthy Computing Workshop, CTC '13*, pp.1–6.



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

«ПРОЧИТАЛ С ПРИСТРАСТИЕМ, И КОЕ-ЧТО НАШЕЛ...»

ПОГОВОРИМ О ПРОФСТАНДАРТЕ
«СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ (КИБЕР)
БЕЗОПАСНОСТИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ»

В 2018 году я уже писал на тему профессиональных стандартов и программ обучения специалистов по ИБ. Тогда завершение статьи было весьма приподнятое:

«Благодаря стандарту специальности мы знаем, кто мы есть.

Благодаря стандарту образования мы знаем, как нас надо готовить.

Благодаря обоим стандартам у нас есть, куда еще развиваться».

И вот новый Стандарт: «Специалист по информационной (кибер) безопасности в кредитно-финансовой сфере».

ПЕРВАЯ И ВТОРАЯ РЕАКЦИЯ

Первая реакция: УРА! Процесс идет, и это не может не радовать.

Первое впечатление: стандарт описывает примерно от 20 до 60% необходимых трудовых функций для обеспечения ИБ-организаций кредитно-финансовой сферы, документ проработанный, целостный, и, безусловно, является существенным шагом вперед в области стандартизации профессиональной деятельности в нашей не простой области.

Макет стандарта выполнен в полном соответствии с принятыми требо-

ваниями к таким документам, разделы проработаны, охват реальных потребностей довольно высок, описание трудовых действий могут быть положены в основу учебных программ и курсов, описания видов трудовой деятельности, единиц профессионального стандарта (трудовые функции, трудовые действия, необходимые знания и умения) разработаны с учетом квалификационных уровней. Во всем документе чувствуется рука специалистов по ИБ с практическим опытом.

Спасибо разработчикам.

Вместе с тем, вторая реакция после углубленного прочтения более сложная: есть много чего, над чем надо поработать.

ПРО БАЗОВЫЕ ОРИЕНТИРЫ

Начнем прямо с первых абзацев. Цитирую:

«Основная цель вида профессиональной деятельности:

Организация и обеспечение системы информационной безопасности в кредитно-финансовой сфере; реализация процессов информационной безопасности при осуществлении банковских и финансовых операций; проведение контроля состояния информационной

безопасности в информационной инфраструктуре организаций кредитно-финансовой сферы»

Прочитал и призадумался. А тому ли я учу наше молодое пополнение? Нас самих учили, что есть три понятия: Система информационной безопасности как совокупность организационных мер, Система менеджмента информационной безопасности как подсистема управления (менеджмента) организации в части информационной безопасности, и, наконец, Система обеспечения информационной безопасности, которая объединяет первые две. На рисунке 1 я попытался изобразить это более наглядно.

После этого возникает вопрос: а о чем идет речь в новом Стандарте? Похоже, авторам документа необходимо еще раз внимательно перечитать свои определения.

ПРО ТРУДОВЫЕ ФУНКЦИИ

Читаем дальше. Может, я сразу не всё понял и пойму через «Описание трудовых функций, входящих в профессиональный стандарт».

Описание начинается с «Методологического обеспечения информационной безопасности в организациях кредитно-финансовой сферы».

О, радость! Это именно то, чего не хватает в 75 % организаций кредитно-финансовой сферы. Теперь мы узнаем, какие должны быть специалисты по методологии ИБ!

♦ Методологическое обеспечение управления риском реализации информационных угроз в организациях кредитно-финансовой сферы

♦ Методологическое обеспечение защиты информации организаций кредитной-финансовой сферы

♦ Методологическое обеспечение защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы

♦ Методологическое обеспечение управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы

Ну... Наверное, такие знания специалистам по ИБ нужны. Но выделить хотя бы одну штатную единицу на это все сразу я точно не смогу. Это просто небольшая часть повседневной работы примерно 0,25 штатной единицы.

Вспомним цикл Деминга в редакции ГОСТ Р ИСО/МЭК 27001-2006 (рис. 2).

Сложить Цикл и раздел «Методологическое обеспечение» в единую систему у меня не получилось.

ПРО СООТВЕТСТВИЕ ПОТРЕБНОСТЯМ

Слова про процессное управление, разработку состава и структуры нормативно-распорядительной документации, основы поддержки актуальности этого самого методологического обеспечения, методологическую поддержку оценки эффективности обеспечения информационной безопасности на основе оценки риска информационной безопасности нашлись лишь в одном пункте *Трудовых действий*, на задворках, так сказать. А ведь это и есть основа деятельности руководителя ИБ. Если попробовать сделать экспертную оценку соответствия всех трудовых действий для функции *Методологическое обеспечение защиты информации организаций кредитной-финансовой сферы* с реальными потребностями малого/среднего (после 70) банка, получится вот такая диаграмма (рисунок 3).

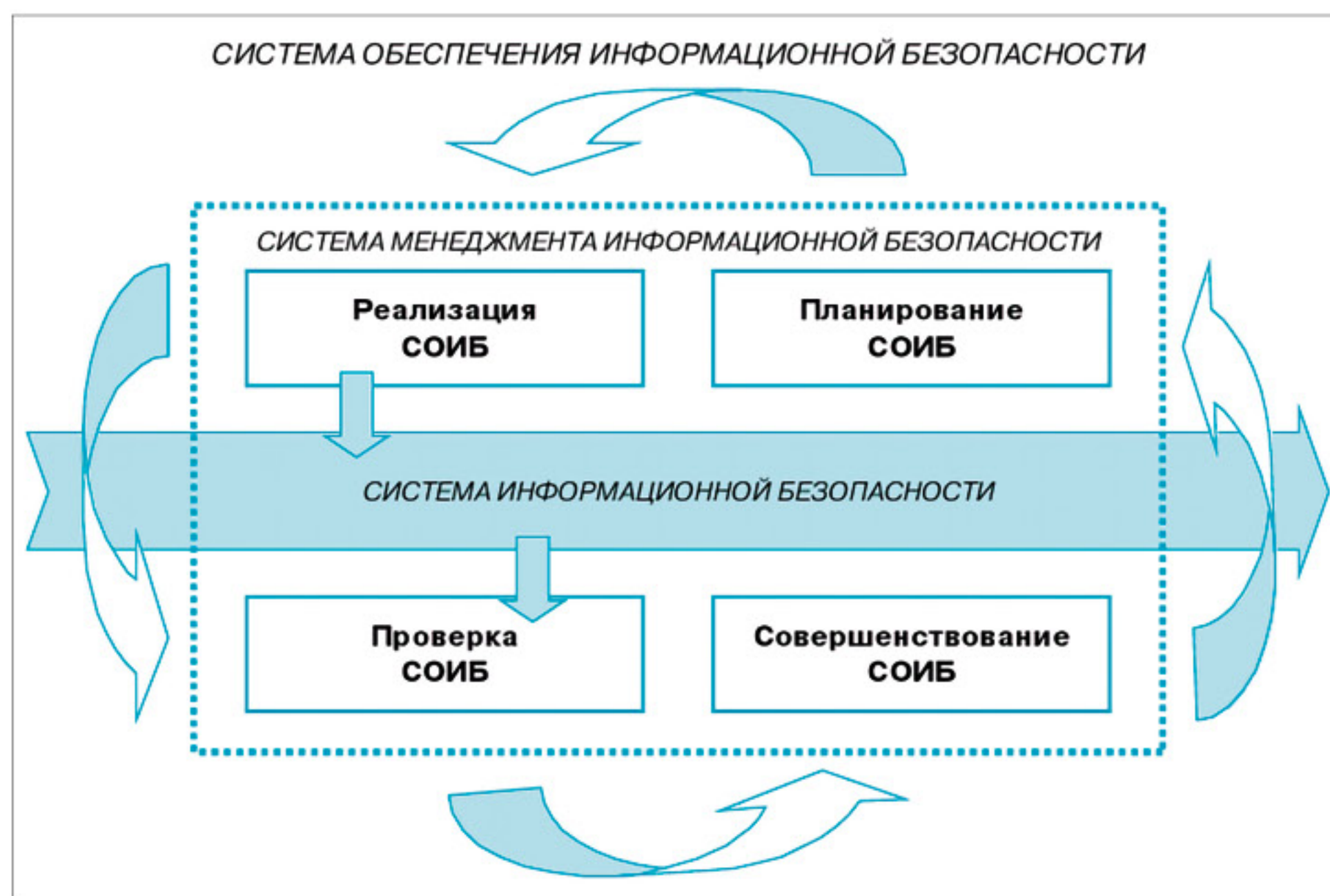


Рисунок 1. СОИБ=СИБ+СУИБ

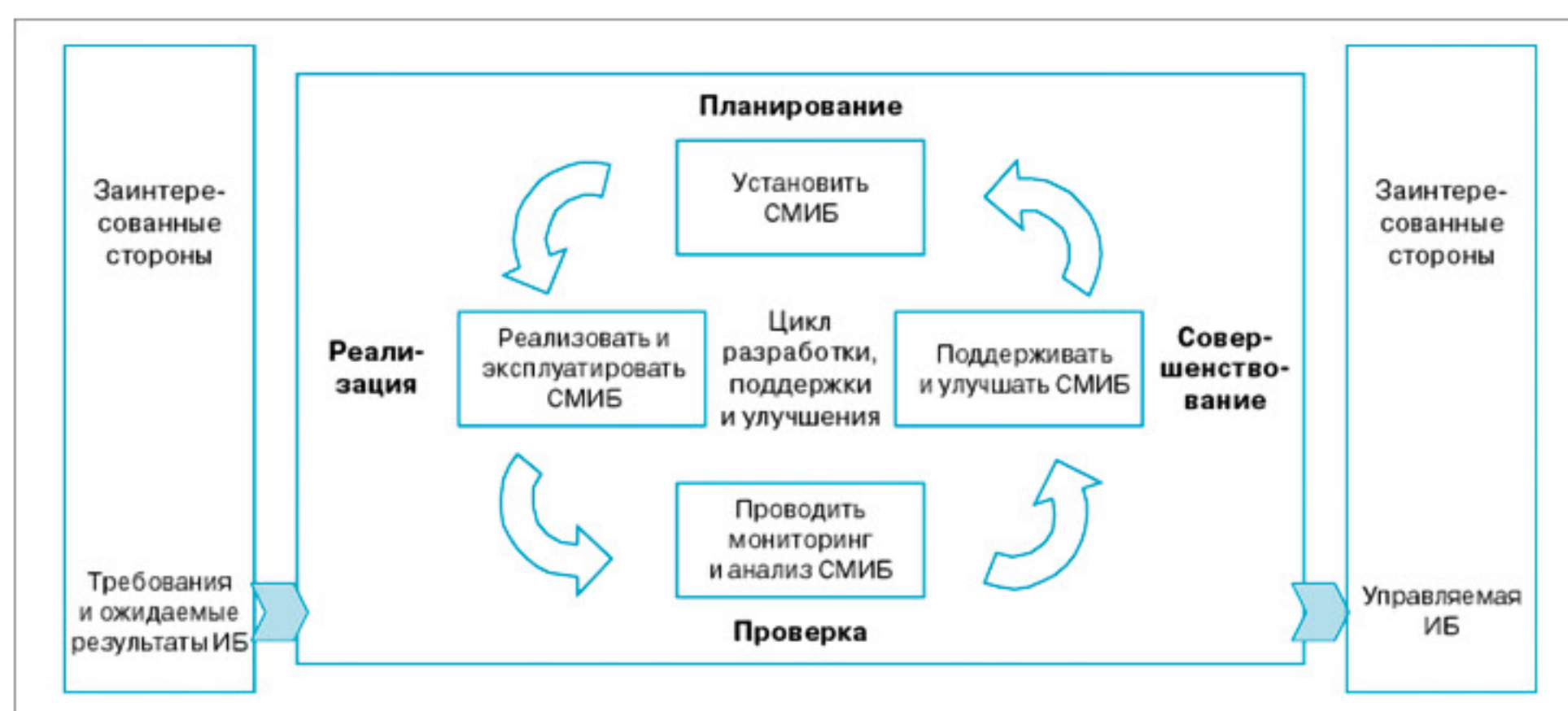


Рисунок 2. Цикл Деминга



Рисунок 3. Диаграмма соответствия трудовых действий потребностям

ПРО ДРУГИЕ СООТВЕТСТВИЯ

Идем дальше.

Реализация процессов информационной безопасности в информационной инфраструктуре организаций кредитно-финансовой сферы:

- ♦ Разработка состава технологических мер защиты информации при реализации основных бизнес и технологических процессов организаций кредитно-финансовой сферы

- ♦ Реализация технологических мер защиты информации при реализации основных бизнес и технологических процессов организаций кредитно-финансовой сферы

- ♦ Контроль применения технологических мер защиты информации при реализации основных бизнес и техно-

логических процессов организаций кредитно-финансовой сферы

Первый пункт сам просится в предыдущий раздел, но ему и здесь вполне уместно быть. Давайте вспомним, о чем здесь идет речь.

В соответствии с ГОСТ 57580.1–2017 в базовый набор мер входят такие направления деятельности по защите информации:

- ♦ Обеспечение защиты информации при управлении доступом
- ♦ Обеспечение защиты вычислительных сетей
- ♦ Контроль целостности и защищенности информационной инфраструктуры
- ♦ Защита от вредоносного кода
- ♦ Предотвращение утечек информации

- ♦ Управление инцидентами защиты информации

- ♦ Защита среды виртуализации

- ♦ Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств

- ♦ Управление системой ИБ

- ♦ Контроль отсутствия уязвимостей защиты информации в прикладном ПО АС и информационной инфраструктуре, предназначенной для размещения АС

Трудовые функции охватывают в разной степени эти направления (рис. 4).

РЕЗЮМЕ

Можно было бы и дальше продолжить подобное рассмотрение. Каждый это



Сергей ВИХОРЕВ

советник генерального директора
ООО «ИТ-Экспертиза»

*Кто хочет научиться летать,
тот должен сперва научиться
стоять, и ходить, и бегать,
и лазить, и танцевать:
нельзя сразу научиться полету!
Фридрих Ницше*

«МЫ ВСЕ УЧИЛИСЬ ПОНЕМНОГУ...»

ЭССЕ НА ТЕМУ СТАТЬИ В. А. ОКУЛЕССКОГО

«ПРОЧИТАЛ С ПРИСТРАСТИЕМ, И КОЕ-ЧТО НАШЕЛ...»

Прочитал статью уважаемого Автора. Прочитал и призадумался. Начать полемику? Да вроде и не с чем. Это твердая позиция Автора. Правильная она или нет? Не знаю, это позиция преподавателя. Спорить с преподавателем? Зачем. Поэтому решил просто высказать свою точку зрения. Так сказать, взгляд с другой стороны.

Начну вот с чего. Для кого нужен профессиональный стандарт? На мой взгляд, это четко определено в Трудовом Кодексе: «Характеристики квалификации, которые содержатся в профессиональных стандартах и обяза-

тельность применения которых не установлена, применяются работодателями в качестве основы для определения требований к квалификации работников с учетом особенностей выполняемых работниками трудовых функций, обусловленных применяемыми технологиями и принятой организацией производства и труда»¹.

Вот и получается, что прежде всего этот стандарт для работодателя, чтобы он смог правильно сформулировать те компетенции, которым должен обладать кандидат на вакантную долж-

ность. А еще он, наверное, потребует-ся самому претенденту, чтобы понять, достаточно ли его образования, знаний и навыков для работы в должности, на которую он претендует. Ну, и конечно, эти стандарты нужны учебным организациям для того, чтобы разработать актуальные программы и убрать разрыв между теоретическими знаниями и практикой. Обратите внимание, я поставил этот тезис на последнее место в ряду назначений стандарта.

Почему? Попытаюсь объяснить. Помните старый афоризм о том, что надо не рыбу давать, а удочку? На мой

¹ ТК РФ, ст. 195.3

может попробовать сделать сам для себя. Я бы отметил еще один момент, который бросается в глаза. Создается впечатление, что этот документ ориентирован в первую очередь на Банк России и очень крупные банки, и он совершенно не учитывает специфику работы малых и средних банков, хотя и предназначен для всех организаций кредитно-финансовой сферы.

* * *

Тем не менее, при всех шероховатостях, упомянутых выше, такой документ представляется очень нужным для формирования информационной безопасности как полноценной отрасли.



Рисунок 4. Диаграмма охвата базового набора мер

взгляд, специалисты по безопасности информации делятся условно на две группы: «стратеги» и «практики». Первые призваны формировать принципы и правила обеспечения защиты информации, вторые — реализовывать это в жизнь. Одним надо иметь очень широкий кругозор, иметь представление о многих новейших технологиях, методах и прочее (это удочка). Вторым требуются конкретные знания, чтобы администрировать те или иные средства защиты (это рыба). Это два совершенно разных направления обучения. В одном случае — это специальное (я бы сказал, среднее) техническое образование, в другом — воспитание стратегического мышления. «Мама всякие важны, мамы всякие нужны...»².

Стандарт в этом смысле не делает различия. Он формирует определенные требования к целому классу специалистов.

По своей сути, профстандарт пришел на смену существовавшему ранее классификатору должностей. И опять возвращаюсь к мысли: стандарт прежде всего важен для работодателей, а не для преподавателей. Профстандарт — это не программа обучения, это, скорее всего, путеводная звезда, вектор,

по которому надо идти преподавателю. А вот как двигаться в этом направлении — это как раз и есть искусство преподавателя.

Не секрет, что одна и та же трудовая функция для разных категорий должностей может иметь разный смысл. Все зависит от требуемой квалификации. А это должен определить уже именно работодатель с учетом особенностей выполняемых работниками трудовых функций: что он хочет получить от претендента. Задача претендента — удовлетворить требованиям работодателя. А как он получил необходимые знания и навыки — дело самого претендента. Это может быть и образование в вузе, и курсы повышения квалификации, и даже самообразование.

И тут встает вопрос: а какова роль стандарта для преподавателя, для образовательной организации? Оказывается, очень важная! Но сначала хочу вспомнить, как меня учили. Кто учил, всех уже и не упомяну, но особо в памяти остались профессора Н. С. Ярошенко, С. Д. Эйдельман, А. М. Страшкевич, легенда академик А. И. Берг и еще много других. И чему они учили? «Ручки крутить»? Нет. Они учили понимать ситуацию, они закладывали в нас базис, на котором можно строить любую трудовую деятельность.



Из альбома Жана Эффеля «Сотворение мира. Люди»

Вот и вывод: роль образования в реализации профстандарта — это необходимость формирования базиса, который позволит выполнять любые необходимые трудовые функции, нужные работодателю. Иногда это ограничивается только «кручением ручек», а иногда — стратегическим мышлением. И то и другое — нужно. И еще, не надо учить какой-то одной конкретной трудовой функции. Это тупиковый подход, приводящий к деградации развития личности и, в конечном счете, к деградации защиты информации.

² С. В. Михалков, «А что у вас?»



Марина БРОДСКАЯ
обозреватель BIS Journal

ТОЧКИ ОТСЧЁТА МНОЖАТСЯ

ЖИЗНЬ В КОЛЛЕДЖАХ ИБ ТЕЧЁТ ДОВОЛЬНО ИНТЕНСИВНО

Давно мы не обращались к теме среднего профессионального образования в сфере ИБ. А между тем колледжи успешно готовят специалистов среднего звена, на недостаток которых постоянно жалуется отрасль. И, если среди выпускников девятого класса идёт борьба за бюджетные места, то обладатели аттестатов о среднем образовании идут сюда по остаточному принципу — после неудачной попытки поступить в университет.

СИТУАЦИЯ

Обучение по специальности «Техник по защите информации» началось в техникумах и колледжах лет десять назад, позже для программ СПО был введён Федеральный государственный образовательный стандарт по направлению 10.00.00, унифицировавший подготовку кадров в области кибербезопасности. Чуть позже, в 2016–2017 гг., был отмечен и всплеск интереса к специальностям ИБ как со стороны колледжей, так и абитуриентов.

Подготовкой специалистов в области ИБ по программам СПО сегодня занимаются:

- ♦ колледжи, подчиняющиеся департаментам или отделам образования субъектов РФ;
- ♦ колледжи, входящие в состав крупных университетских комплексов;
- ♦ частные учебные заведения СПО, в т.ч. входящие в состав негосударственных университетов.

Поступившим на базе 9 классов придётся учиться 3 г. 10 мес., на базе 11

классов — на один год меньше. Приём в колледжи осуществляется на общедоступной основе — вступительные испытания не проводятся, конкурсный отбор организован по среднему баллу аттестата поступающего.

Однако, как показывает анализ текущей ситуации, не все учреждения среднего профобразования продолжают набирать учеников по специальностям 10.00.00. Хотя направление ИБ уже вошло в ТОП-50 самых востребованных профессий.

СТОЛИЦА

По данным Департамента образования и науки Москвы, городские колледжи предлагают абитуриентам 181 востребованную профессию и специальность. В пятёрку популярных направлений входят ИТ, программирование, ремонт автомобилей и строительные специальности, графический дизайн и гостиничное дело. Согласно информации сервиса Учеба.ру, лицензию на обучение по ИБ в Москве имеют 25 колледжей, однако далеко не все они ведут приём по направлениям 10.00.00.

Политехнический колледж № 8 им. дважды Героя Советского Союза И. Ф. Павлова ведёт очное обучение по направлению 10.02.05 («Обеспечение информационной безопасности автоматизированных систем») на базе 11 классов. В 2019 г. на бюджетные места по специальности приняты 50 человек. Правда, завершат учёбу из них немногие — в конце декабря 2019 г. на 3 курсе было 15 вакантных мест.

Колледж приборостроения и информационных технологий РТУ МИРЭА

принимает студентов на обучение по направлениям ИБ на базе 9 классов. На 2020/2021 учебный год по направлению 10.02.05 открыты 50 бюджетных мест, ещё 40 человек смогут учиться платно. В 2019 г. конкурс на 25 бюджетных мест составил 25,92 чел./место, на 65 платных — 6,26. Проходной балл на бюджет/платное — 4,947/3,722, средний балл — 4,998/4,259 (информация с сайта колледжа).

По данным приёма прошлых лет можно заметить, что в 2017 г. на специальность «Обеспечение ИБ АС» колледж принял 30 человек на платной основе. С 2018 г. начат приём за счёт средств городского бюджета. Число бюджетных мест растёт с каждым годом (15–25–50), впрочем, растёт и число платных мест (с 30 до 65 в 2018 г.). Вместе с ростом популярности направления, вырос и средний проходной балл — с 3,772 в 2017 г. до 4,259 (на платной основе) и 4,998 (на бюджет). Стоимость обучения — 120 тыс. рублей в год.

Причины популярности колледжа понятны — помимо качественного образования его выпускники получают возможность поступления в МИРЭА по внутренним экзаменам.

Московский колледж бизнес-технологий принимает абитуриентов по направлению 10.02.05. Открыты по 25 мест для каждой группы поступающих, проходной балл в 2019 г. для девятиклассников составил 4,23, для окончивших школу — 3,43. Стоимость обучения — 119 тыс. 900 рублей. Несмотря на невысокие проходные баллы, вакантных мест на 2–4 курсах не так уж и много — от 1 до 5.

Московский государственный образовательный комплекс в 2019 г. принял 25 студентов на базе 9 классов на обучение по направлению 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем». «Задача такого специалиста — обезопасить информацию в компании от утечек, потерь, злоумышленников и шпионов», — говорится на сайте колледжа. Среди потенциальных работодателей могут быть отделы обеспечения ИБ коммерческих организаций, банков и госучреждений, силовые ведомства, предприятия и учреждения телекоммуникационной сферы. Средний проходной балл на бюджет составил 4,22.

Московский приборостроительный техникум Российского экономического университета имени Г.В. Плеханова с 2017 г. работает по программе 10.02.05. В 2019 г. техникум принял 45 человек на бюджетные места и 10 — на платной основе. Конкурс составил 11,62 заявлений на бюджет и 14,2 — на обучение на коммерческой основе. Проходной балл — 4 для платников и 4,418 — для бюджетников. Приём на бюджетной основе ведётся только на базе девяти классов. Стоимость обучения — 112 200 руб.

Колледж декоративно-прикладного искусства имени Карла Фаберже ведёт обучение за счёт средств бюджета города Москвы по направлению «Обеспечение ИБ АС» на базе 9 классов. Для попадания на одно из 25 бюджетных мест нужен средний балл аттестата от 4,418, на 10 платных — ровно 4. Стоимость обучения — 130 тыс. рублей.

Колледж информатики и программирования Финансового университета при Правительстве РФ осуществляет обучение на базе 9 классов на бюджетной и платной основе. Выпускники колледжа заканчивают обучение по направлению 10.02.03, а последние три года идёт приём на специальность «Обеспечение ИБ АС». В 2019 г. был открыт приём на 50 бюджетных мест и 50 — на платной основе, стоимость обучения для первокурсников — 120 тыс. рублей. Впрочем, в процессе учёбы число вакантных мест увеличивается, а с ростом номера курса падает стоимость обучения.

В отличие от других бюджетных учреждений Москвы, где есть конкурс

Как сообщает сервис Учеба.ру, подготовку по ИБ ведут 95 колледжей в разных уголках страны, профессия входит в ТОП-50 востребованных специальностей

аттестатов, Колледж современных технологий имени Героя Советского Союза М. Ф. Панова похвастаться сильными студентами не может — сюда идут те, кто не прошёл в университеты. На направление «Обеспечение ИБ АС» после 11 класса было подано 44 заявления на 25 бюджетных мест, ещё 25 мест открыты для платного образования.

В рамках реализации специальности студенты осваивают одну рабочую профессию — Оператор электронно-вычислительных и вычислительных машин. Выпускники могут продолжить обучение по специальности в МГТУ ГА, МИРЭА или МИСиС. Средний балл поступающих в 2016–2018 гг. — 3,6. Стоимость обучения — 120 тыс. рублей в год.

Среди достижений колледжа — организация регионального этапа Всероссийской олимпиады профессионального мастерства по УГС 10.00.00 «Информационная безопасность».

Университетский колледж информационных технологий Московского государственного университета технологий и управления им. К. Г. Разумовского учит по специальностям 10.02.03 (ИБ АС) и 10.02.05 (Обеспечение ИБ АС). На 20 платных мест в 2019 г. было подано 52 заявления, зачислены 26 человек. Стоимость обучения — 114 тыс. рублей. По направлению 10.02.03 на конец декабря было 16 вакантных бюджетных мест на 4 курсе. В планах приёма 2020/2021 учебного года бюджетного финансирования направления ИБ не будет.

В РЕГИОНАХ

Как сообщает сервис Учеба.ру, подготовку по ИБ ведут 95 колледжей в разных уголках страны, профессия входит в ТОП-50 востребованных специальностей.

Ростовский-на-Дону колледж связи и информатики готовит техников по защите информации по специальностям 10.02.04 и 10.02.05 на базе 9 (бюджет и платно) и 11 (по 5 мест на направление, только на платной основе) клас-

сов. Конкурс на 25 бюджетных мест по каждой специальности превышает 3–4 человека на место, на платные места в 2019 г. зачислены более 30 человек по каждой специальности. Проходной балл на бюджет составляет 4,53 для ИБ телекоммуникационных систем и 4,61 для ИБ АС. Стоимость обучения 56 тыс. рублей в год.

Егорьевский техникум (Московская область) ведёт обучение по направлению 10.02.03 на базе 9 классов, за счёт бюджета тут учатся 27 человек на курсе. В сезоне 2019/2020 учебного года приёма по направлению не было. А Дмитровский техникум (г. Дмитров Московской области) уже не первый год принимает по 25 студентов на специальность «Организация и технология защиты информации» (10.02.01), обучение ведётся на бюджетной основе.

Санкт-Петербургская Академия управления городской средой, градостроительства и печати ведёт набор выпускников 9-х классов по направлению 10.02.01 и учит по специальности «Обеспечение ИБ телекоммуникационных систем». На первом курсе студенты изучают общеобразовательные дисциплины в объёме средней школы, а позже проходят подготовку по специальности. Желающих поступить и учиться в Академии много, однако уже на третьем курсе появляются вакантные места. По данным сайта колледжа, проходной балл в 2018 г. для поступающих девятиклассников составил 3,73. Стоимость обучения на очном отделении от 78 600 до 169 200 руб. (в зависимости от базового образования), на заочном — 41 400 рублей.

Колледж при Технологическом институте Северо-Восточного федерального университета имени М. К. Амосова принимает 25 бюджетников и 3 человек на платной основе. Полная стоимость обучения — 162 тыс. руб., для имеющих льготы — 63 тыс. рублей.

Продолжают учить студентов по направлению ИБ и в Аэрокосмическом

колледже Сибирского государственного аэрокосмического университета имени академика М. Ф. Решетнева. На базе 9 и 11 классов по направлению 10.02.04 принимают 35 бюджетников и 15 на платной основе. Ещё 25 желающих получить подготовку за счёт средств бюджета ждут на специальности 10.02.05. Платное обучение обойдётся в 103 600 рублей в год.

ЧАСТНЫЕ

По данным сервиса Поступи.онлайн, в России по программам 10.00.00 работают несколько частных образовательных учреждений СПО, что только подтверждает популярность направления у абитуриентов.

Частное образовательное учреждение СПО ИТ-Колледж «Мирбис» создан на базе Московской Международной высшей школы бизнеса МИРБИС, он готовит техников по защите информации по следующим видам деятельности:

- ♦ Эксплуатация подсистем безопасности АС.
- ♦ Применение программно-аппаратных средств обеспечения ИБ в АС.
- ♦ Применение инженерно-технических средств обеспечения ИБ.

Обучение ведётся на базе 9 и 11 классов, стоимость одного года учёбы — 300 тыс. рублей. Как сообщает сайт колледжа, помимо знаний, за эту сумму «в течение всего обучения студенты участвуют в Международной сертификационной Олимпиаде «Траектория будущего», в хакатонах, организуемых вендерами, в студенческом волонтерском движении и движении экспертов-студентов, в зарубежном проектном лагере «Траектория 360», в Международных саммитах и конференциях».

Колледж управления и производства (г. Москва) проводит обучение по направлению 10.02.05 и предлагает три формы обучения: очную, очно-заочную и заочную. Стоимость года учёбы — от 40 тыс. до 80 тыс. руб.

Частное учреждение СПО «Социально-технологический колледж» (г. Тула) проводит обучение по направлению 10.02.04 (Обеспечение ИБ телекоммуникационных систем) как по очной форме обучения (срок обучения 3 г. 10 мес.), так и по заочной форме (4 г. 7 мес.). Сто-



Тюменцы Виктор Легостаев и Дмитрий Титов (в центре) заняли первое место в компетенции «Информационная безопасность» на чемпионате по профессиональному мастерству Worldskills 2019. Источник: worldskills2019.com

имость первого семестра 2019/2020 учебного года — 17 тыс. для очной и 12,5 тыс. руб. для заочной форм обучения. Полная стоимость обучения ИБ в колледже — 154,5 тыс. для очников и 147 тыс. рублей для заочников.

Омский юридический колледж принимает абитуриентов на базе 9 и 11 классов на направление 10.02.01 «Организация и технология защиты информации». Колледж предлагает три формы обучения, стоимость — от 21 тыс. руб. в год (при заочной форме). По окончании колледжа выдаётся диплом о СПО государственного образца.

Также по направлениям 10.00.00 готовят специалистов частные учреждения системы среднего профобразования в Краснодаре (Факультет СПО Академии маркетинга и социально-информационных технологий), Калининграде (Балтийский информационный техникум, Бизнес-колледж), Владивостоке (Гуманитарно-коммерческий колледж Приморского крайпотребсоюза) и Ставрополе (Многопрофильный колледж).

ВСЮДУ ЖИЗНЬ

Организация жизни студентов колледжей во многом зависит от руководства учебных заведений. И при заинтересованности со всех сторон, студенты могут гордиться результатами учебного процесса.

Тюменцы Виктор Легостаев и Дмитрий Титов заняли первое место в

компетенции «Информационная безопасность» на чемпионате по профессиональному мастерству Worldskills 2019, который проходил в Казани в августе 2019 г. В нём участвовали более 1 тыс. 300 конкурсантов из 63 стран. Соревнования проходили по 56 компетенциям, объединённым в шесть блоков, в различных сферах производства.

В V Национальном чемпионате профессионального мастерства среди инвалидов и лиц с ограниченными возможностями здоровья «Абилимпикс» студент Краснодарского колледжа электронного приборостроения Алексей Иващенко стал первым в компетенции «Информационная безопасность», второе место занял студент Колледжа инфраструктурных технологий СВФУ Афанасий Павлов из Якутии. Всего в соревнованиях, организованных Министерством просвещения РФ, приняли участие 1800 человек из всех 85 регионов России.

Первые региональные соревнования по компьютерной безопасности среди школ и колледжей Свердловской области IsetCTF прошли в Екатеринбурге в 2019 г. За звание лучшего «белого хакера» боролись 47 участников из Екатеринбурга, Первоуральска и Новоуральска. Оценивал работу школьников искусственный интеллект. Победила команда Cheekibambonee из екатеринбургской гимназии № 35. Второе и третье место завоевали команды СУНЦ УрФУ «Гусь и гуси» и «Как называется наша команда».



Валерия МЕЩЕРЯКОВА

студентка факультета журналистики
МГУ им. М.В. Ломоносова,
студентка факультета журналистики
Университета Сорбонны

КАК ТАМ ВО ФРАНЦИИ?

НАШ КОРРЕСПОНДЕНТ В ПАРИЖЕ РАССПРАШИВАЕТ
МЕСТНЫХ СТУДЕНТОВ-ТЕХНАРЕЙ¹

Как там, во Франции? Как дела с техническим образованием? Сложно ли учиться по программе двойных дипломов? Почему у нас студенты не успевают работать и учиться одновременно, а во Франции без проблем? На один семестр я сама стала иностранным студентом и, конечно, воспользовалась возможностью порасспросить зарубежных «коллег». Но сначала поделюсь собственными открытиями:

- ♦ учебных пар тут меньше, чем в России, а сообществ по интересам больше.
- ♦ выходные — реально для отдыха, а не для учёбы (шок!).
- ♦ работодатели берут студентов на работу на один (один!) день в неделю и даже платят им за это.
- ♦ после окончания лицея (т.е. школьной программы) можно получить приличную высокооплачиваемую работу.

¹ Интервью сделаны до карантина. На момент выхода номера все школы и университеты во Франции закрыты, обучение и экзамены проводятся дистанционно.

ХАКИМ, 25 ЛЕТ

Алжир-Париж

Я приехал в Париж из Алжира пару лет назад. Чтобы вы лучше понимали, как я учусь, нужно ввести вас в курс дела. Как строится техническое образование во Франции?

Вузовская система предполагает окончание школы, затем лицея — это среднее образование. Дальше встает выбор, куда поступать: в государственный университет или Инженерную школу — Ecoles d'ingénieurs. В общей сложности и там, и там получение полноценного диплома занимает пять лет. В университете это Licence (бакалавриат) и магистратура. В Инженерной школе придется два года отмотать на подготовительных курсах и потом три года учёбы. В Алжире я окончил École d'ingénieurs, а здесь пришлось поступать в магистратуру. Но не беда: я учусь по программе alternance, которая позволяет все учебные часы уместить в три дня на неделе, а два дня я работаю инженером в компании Red Fabric. С жильём трудно: недавно у меня закончился контракт на аренду квартиры и теперь живу в colocation со знакомыми из Алжира — стараемся помогать друг другу, выручать в сложных ситуациях.



**ДАВИД И МИШЕЛЬ, 21 ГОД****Мехико-Париж**

Давид: Учился я в Испании во французской школе, и первые три года бакалавриата провёл там же, в Университете Бургоса. Потом перепоступил в Бордо, изучал прикладную математику и информатику в когнитивных науках, а в магистратуру поступил в Сорбонну VI. Вот, что думаю: в Испании требуют больше фактических знаний. Шаг влево, шаг вправо — и ты провалил экзамен. А здесь, во Франции, больше свободы, творчества. Иногда я подрабатываю репетитором: даю курсы по математике и статистике. Прошедший год был счастливым: ездил к другу в Мексику и встретил там Мишель. В Париж вернулся с ней.

Мишель: Да, правда, когда Давиду нужно было уезжать, я сделала визу *vacances-travail* на 1 год. Она позволяет непрерывно пребывать во Франции, а также даёт разрешение на работу. Сейчас работаю официанткой в ресторане рядом с Триумфальной аркой, 35 часов в неделю. Всё хорошо, только далеко от квартирки. Сегодня иду на собеседование на другую работу — хочу, чтобы оставалось время и на друзей, и на изучение языка.

**ВЯЧЕСЛАВ, 25 ЛЕТ****Екатеринбург-Париж**

В восьмом классе я переехал из Екатеринбурга во Францию, родителям предложили работу. Окончил здесь колледж и лицей по специальности физика и математика. Базовых знаний с восьмого класса мне хватило до самого поступления в Инженерную школу EFREI.

С пропусками занятий здесь жёстко: за весь семестр можно безнаказанно прогулять не больше десяти дней. Расписание состоит из лекций и пары практических работ в неделю, каждый день с 8 до 18. Расписание на официальном сайте школы выложено на весь год, но оно часто меняется: занятия то добавляются, то отменяются. На следующем курсе хочу выбрать специальность по кибербезопасности. Считаю, что на этом строится современное общество. Например, в прошлом году хакеры устроили атаку на госпиталь в Сан-Франциско, пришлось экстренно перевозить 3 тысячи пациентов. Таким образом, кибербезопасность полезна не только для защиты данных, но и для защиты жизни людей. На распределение по специальности — конкурс, пока что записаны 42 человека. Очень важно, что у нас будет возможность работать. Вакансию нужно искать самому, но учебный отдел помогает. К примеру, я могу взять стажировку в таких компаниях, как Airbus или Carrefour.



ДМИТРИЙ, 25 ЛЕТ**Санкт-Петербург-Тулуза**

Я учусь по программе двойных дипломов в ЛЭТИ и лаборатории IRIT в Тулузе. Какой-то специальной программы нет, потому и экзаменов никаких не было, отбора тоже. Дальше мы оформляли «соглашение о совместном руководстве» и согласовывали его содержимое между сторонами. Есть проблема: наши руководители владеют английским, а мы не владеем французским, поэтому наше общение происходит на английском. Защита, в соответствии с соглашением, будет тоже на английском. Однако подавляющее большинство людей из администрации или не говорит, или не хочет говорить на английском...

По сути я тут работаю над темой своей аспирантской, просто под руководством иностранных профессоров. В Европе не понимают, кто такой к.т.н. и д.т.н., зато они знают, кто такой PhD. Если вдруг станет интересно продолжить научную карьеру в Европе — без PhD¹ будет трудно. Так что для меня это скорее способ предоставить себе такую возможность, если она понадобится.

О местном бюрократизме: обычно люди не очень понимают кто и за что отвечает, потому приходится вместе с ними это выяснять и находить решение. При этом есть закономерность: молодые сотрудники обычно очень стараются и хотят помочь, даже если не всегда могут, в то время как более старшие сотрудники предпочитают ругань. Если говорить об особенностях бюрократии в России, то она становится реально сложной и напряжённой только в больших организациях (тот же ИТМО). Здесь у меня уже не раз были ситуации, когда для решения одного вопроса меня перенаправляли из отдела в отдел, чтобы на пересылке, скажем, пятой понять, что круг замкнулся, а вопрос так и не был решён. У нас даже была ситуация, когда документы пропали по пути из отдела в отдел...

Всё делается очень медленно: когда мы приехали, нам понадобился месяц, чтобы оформить нас в университете; 2 недели, чтобы оформить нас после этого в аспирантуре, и 2 дня после этого, чтобы оформить нас в лаборатории и активировать пропуск. Но что точно общее между нашими странами — решение вопросов удалённо довольно проблематично. Как правило, быстрее и эффективнее всё решается на месте.

Какого-то принципиального расписания у нас нет. Нам выделили кабинет в лаборатории IRIT. Сотрудники IRIT, как правило, его для аспирантов и используют. Ну или просто пьют в нём кофе (раньше здесь стояла кофемашина).

¹ PhD — это учёная степень, которую можно полностью расшифровать как Doctor of Philosophy. Это учёная степень, присуждаемая на Западе, а также в некоторых странах бывшего СССР, в частности в Казахстане и Украине. Является последней ступенью образования, поэтому иногда степень переводят как «доктор наук», однако наша докторская диссертация по требованиям более сложная и фундаментальная работа. То есть PhD — это где-то посередине между нашим кандидатом и доктором.



Встречи с руководителями назначаем по инициативе одной из сторон (или мы хотим что-то обсудить и пишем, или они хотят — соответственно пишут они). В среднем один раз в неделю. Вместе смотрим результаты работы, думаем, что делать дальше, планируем. Обычный научный процесс, периодически разбавляемый бюрократией — часто приходится просить человека, владеющего французским, нас сопровождать. Обязательных занятий у нас нет, хотя когда-то шла речь о возможных курсах французского языка. Для сравнения, в России у нас есть пары — как только решили сделать аспирантуру очередным этапом образования, ввели ряд обязательных к посещению занятий с экзаменами и зачётами.

Классный плюс: всегда можно договориться и отсутствовать пару будних дней, чтобы куда-нибудь съездить в путешествие, главное — заранее предупредить. Кстати, про путешествия, отсюда очень дешёво ездить по Европе, грех не воспользоваться такой возможностью. Также мы продолжаем активно работать с лабораторией в РФ: чтобы получать зарплату, учиться в ИТМО, получать стипендию и т.д. Правда, есть такой момент: наше отсутствие в течении года в России — не повод для автозачета занятий в ИТМО, поэтому нам необходимо продолжать обучение удалённо. Сам формат удалённого обучения никак не регламентирован и по сути заключается в том, что каждый лично пишет своим преподавателям и лично с ними договаривается.



**МАКСИМ, 25 ЛЕТ****Санкт-Петербург-Тулуза**

Я учился в ЛЭТИ по специальности информационная безопасность и после поступил в аспирантуру ИТМО. Выбрать профессию было просто — она должна была быть связана с IT, нужно было лишь выбрать область. Выбирал между обычным программированием и информационной безопасностью. Перед поступлением я просто промониторил уровень зарплаты в разных областях и выбор был очевиден. Кроме того, чтобы стать программистом, не обязательно идти в университет, ведь очень многие получают образование на онлайн-курсах или путём самообучения по паре книг — часто для начала этого хватает. А вот получить хотя бы минимальный багаж знаний по безопасности самому не получится. Как оказалось, я попал куда надо — рынок безопасности растёт очень быстро, а специалистов не хватает. Я уверен, это только начало тенденции и российской, и мировой. Преимуществ в двойном дипломе с точки зрения приобретённых знаний не много. Если найти хорошего научного руководителя и работать именно в R&D, то разницы между вузами нет. Аспирантура — это больше про взаимодействие аспиранта и научного руководителя, а не университетов.

Но для меня двойной диплом имел принципиальной значение. Как раз в то время, когда я задумывался о поступлении, прогремел Диссернет, и было обнаружено множество липовых диссертаций. И всё же ключевым моментом для меня стало понимание того, что степень кандидата наук в Европе работодатели не воспринимают всерьёз. Одним словом, PhD — это тот своеобразный гарант, что диссертация будет выполнена качественно. Поэтому я и шёл именно за двойной аспирантурой. Из дополнительных плюсов двойной диплом — это, конечно, возможность пожить в другой стране, увидеть европейский подход к обучению и более простое трудоустройство в зарубежную компанию.

Обучения в классическом понимании здесь нет. Если в России у аспирантов есть пары (их немного, но они есть) и показатели (написать N статей за полгода), то во Франции ничего этого нет. Ты просто работаешь с научным руководителем и выполняешь задачи которые он даёт — это и есть обучение. Решение о переводе на следующий год строится на основе отзыва руководителя о твоей работе. В конце обучения ты защищаешься, как и в России. Но если в России форма превалирует над содержанием, то во Франции на защите смотрят именно на содержание и суть работы.

Как и в России, тут всё зависит от специальности и научного руководителя. В моём случае 90% работы — это изучение алгоритмов, сбор данных и анализ. У геологов или, например, медиков аспирантура может проходить совсем по-другому.

Что удивило — бюрократии во Франции довольно много, но она не такая принципиальная как в России. Опечат-



ки в большинстве бумаг можно смело исправлять ручкой прямо перед принимающим. За подтверждение чего-либо подходят распечатки электронной почты, скриншоты переписки, чеки и прочие бумаги, которые в России даже не подумаешь представить как доказательство. Печати французы ставят только на очень важных документах (например, на соглашении о поступлении), а в 99% требуется только подпись. Франция напоминает коммунизм. Это и есть основная трудность. Например, сетевым магазинам нельзя работать после восьми вечера. А ещё им нельзя работать в воскресенье — есть такой закон. Поэтому, если вы прилетели в Тулузу в воскресенье, то будьте готовы поголодать. Это не распространяется на мелких предпринимателей, но их очень мало.

Другая большая проблема — это отсталость IT сферы. Например, в то время как у нас банкоматы учатся распознавать лица, во Франции банкоматы не принимают деньги и работают 5 часов в день со вторника по субботу. Интернет намного медленнее и намного дороже, чем в России. Гугл карты не работают и приходится пользоваться локальными, которые очень неудобны (возможно, французы просто запретили Гугл работать у них). В целом ощущение, что вернулся в 2005 год. Конечно, всё это относительно. Например, тут метро без водителей и вообще без персонала — всё работает автоматически, а улицы спроектированы так, что лужи или грязь не могут образовываться. Словом, жизнь во Франции в чём-то лучше, а в чём-то хуже. Тут зависит от человека и его привычек.



На набережной Гаронны в Тулузе

Ещё у меня есть возможность изнутри взглянуть на альтернативную систему образования и почувствовать её плюсы и минусы. Например, в России у учёных маленькая зарплата, но большие деньги с грантов. Во Франции большая зарплата, но деньги с грантов они не получают вообще. Во Франции полная нетерпимость к любому виду мошенничества — за списывание на экзамене отчисляют без разговоров. Ещё французы работают очень медленно, для них высокое качество важнее скорости. Есть гендерный аспект: девушкам немного проще получить грант или поступить. Сами институты очень автономны, например, полиция не может заходить на его территорию без разрешения и большинство проблем решаются непосредственно администрацией университета. Сама доступность образования во Франции — на уровне национальной идеи, и, как результат, поступить очень легко. Но так как очень много людей поступают даже без самых элементарных знаний, очень многих и отчисляют.

У университетов здесь хорошая материальная база, и получить доступ, скажем, к суперкомпьютеру проще, чем в России. В России необходимо либо чтобы в вашем вузе такой был, либо чтобы научный руководитель имел связи с теми, кто имеет к нему доступ. Во Франции все научные лаборатории объединены в научный центр CNRS, и вы можете запросить доступ к оборудованию другого института.

То же самое и с возможностью поработать со специалистами, которых по какой-то причине нет в вашем университете. Это, наверное, один из главных плюсов, так как вас обучают сразу два очень разных типа специалистов с разными критериями. Ну, и, конечно, просто возможность пожить в другой стране. Это скорее испытание, чем приятное времяпрепровождение, но опыт есть опыт.

Что успел понять о разнице менталитетов: русские очень индивидуальны и всегда говорят прямо, а французы любят решать проблемы сообща, и очень мягко говорят что что-то сделано плохо. Иногда это доставляет неудобства, так как приходится вытягивать из них хоть какую-нибудь критику. Но это в академической среде. В обычном бытовом плане мы похожи, и я удивлён, насколько сильно похожи. Всё-таки мы все европейцы. Разве что французы действительно любят вино, шарфы, багеты и вкусно поесть. Если бы я учился в Китае или Африке, то мог бы рассказать больше.

В плане ИБ: у французов направленность на частный сектор, в то время как в России — на государственный. Когда говоришь с французами о перспективах исследования, то в ход идут рассуждения о том, каким компаниям это будет полезно, в то время как в России все разговоры в основном о государственных структурах. Но в целом тенденции исследований похожи. Как-никак тренды исследований, связанных с безопасностью, во всём мире одни и те же.



СЛОВО О НАСТОЯЩЕМ РУКОВОДИТЕЛЕ

К 75-ЛЕТИЮ В. Г. МАТЮХИНА:

ЛУЧШИЕ ДЕЛОВЫЕ И ЧЕЛОВЕЧЕСКИЕ КАЧЕСТВА ДЛЯ
РЕАЛИЗАЦИИ КРУПНЫХ НАЦИОНАЛЬНЫХ ПРОЕКТОВ

Есть люди, которых принято считать «столпами общества». Они являют собою ту естественную скрепу, которой держится государство, общество, наука и техника. Они, как светочи, указывают путь к прогрессу, являют личный пример беззаветного и нравственного служения Делу, которое избирают для себя. Из этого малого числа и Владимир Георгиевич Матюхин, чей 75-летний юбилей мы отмечаем в нынешнем году.

Владимиру Георгиевичу судьба уготовила удивительный путь. Вырасти от рядового инженера до доктора технических наук, академика ряда российских и междуна-

родных академий, автора уникальных информационных систем общегосударственного масштаба — это не проехаться по гладкой накатанной колее служебного роста, за этим стоит самоотверженный труд и высочайшая требовательность, в первую очередь, к самому себе. Генералом армии Матюхиным сделано так много, что мы можем лишь кратко пробежаться по основным вехам его славной биографии, в которой очень многие свершения еще носят гриф «совершенно секретно». Но и то, о чем можно рассказать, украсило бы послужной список не одного десятка человек.

МАТЮХИН ВЛАДИМИР ГЕОРГИЕВИЧ, КРАТКАЯ БИОГРАФИЯ

Родился 4 февраля 1945 года.

В 1968 году окончил Московский энергетический институт по специальности «электронная техника», в 1973 году — механико-математический факультет Московского государственного университета им. М. В. Ломоносова по специальности «математика».

С 1969 года по 2003 год проходил военную службу в органах государственной безопасности. С момента образования в 1991 году Федерального агентства правительственной связи и информации при Президенте Российской Федерации до 1993 года возглавлял научно-исследовательский центр Агентства. С 1993 по 1999 год был заместителем Генерального директора ФАПСИ, с мая 1999 года по март 2003 года — Генеральным директором ФАПСИ. В марте 2003 года назначен Первым заместителем министра обороны, исполняющим обязанности Председателя государственного комитета Российской Федерации по оборонному заказу. Воинское звание — генерал армии. С июня 2004 года по февраль 2010 года возглавлял Федеральное агентство по информационным технологиям (Росинформтехнологии).

С декабря 2010 года работает первым заместителем генерального директора АО «НИИАС» (Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте).

Доктор технических наук, действительный член Академии криптографии России, Российской академии инженерных наук и Международной академии связи, дважды Лауреат Государственной премии России.

Виктор ПЯРИН

лауреат Государственной премии Российской Федерации в области науки и техники

«ОН ВИДИТ БУДУЩЕЕ»

Наше знакомство состоялось в начале 1980-х годов и поначалу носило случайный характер. Тогда В. Г. Матюхин работал над кандидатской диссертацией и по вопросам информационной безопасности консультировался у выдающегося математика-криптографа В. Е. Степанова, который руководил отделом, где я работал. Владимир Георгиевич произвёл положительное впечатление — приветливый взгляд, высокий лоб учёного, аккуратная красивая причёска, я хорошо запомнил его с первого взгляда.

Потом некоторое время мы встречались эпизодически, пока в 1993 году В. Г. Матюхин на одном из мероприятий не начал подробно расспрашивать меня о моей работе. Я поделился, что занимаюсь перспективным направлением, связанным с микропроцессорными пластиковыми картами. Рассказал о работах, которые уже велись в Зеленограде на предприятии «Ангстрем». Упомянул о предстоящем участии в крупном деловом мероприятии по этой тематике, запланированном в Лондоне на февраль 1994 года.

Микропроцессорные пластиковые карты — это компактные носители ключевой информации, удобное и недорогое средство шифрования данных, в том числе с электронной цифровой подписью. Недаром в наши дни они применяются практически повсеместно для многих целей: в разных системах доступа на объекты и к средствам вычислительной техники, в платёжных системах и т.п. В. Г. Матюхин сразу стратегически оценил эти обширные перспективы и быстро принял решение тоже поехать на лондонскую конференцию.

В этом крупнейшем форуме участвовали разработчики, производители микропроцессорных карт и оборудования, представители сервисов с их использованием. Мы с Владимиром Георгиевичем два дня обходили стенды, осма-

тривали экспонаты, задавали вопросы специалистам. Мне довелось и переводить, и комментировать ответы.

В. Г. Матюхин показал себя исключительно пытливый и скрупулезный человеком. После моих комментариев на ответы он задавал новые, всё более специализированные вопросы. Меня поразило постоянное стремление не удовлетворяться общим впечатлением, а глубоко вникать в суть и в мельчайшие подробности научно-технических разработок, решений и сопутствующих аспектов. Это качество неизменно проявлялось у него и все последующие годы, когда мы уже тесно работали вместе, начиная с ФАПСИ (Федеральное агентство правительственной связи и информации при президенте Российской Федерации), где я был его заместителем.

Меня поразило постоянное стремление не удовлетворяться общим впечатлением, а глубоко вникать в суть и в мельчайшие подробности научно-технических разработок, решений и сопутствующих аспектов



Флаг Федерального агентства правительственной связи и информации



Генерал армии В.Г. Матюхин

КООРДИНИРОВАТЬ ВЗАИМОДЕЙСТВИЕ

После форума в Лондоне мы активно продолжили работу над тематикой микропроцессорных пластиковых карт. В 1995 году в России была проведена первая международная конференция с участием крупнейших зарубежных компаний — Siemens, Motorola, SGS-Thomson, Gemplus и других. Инициатором и организатором мероприятия выступило ФАПСИ, при поддержке Банка России, федеральных министерств и ведомств, а также Ассоциации российских банков.

В общей сложности к 2009 году удалось провести почти полтора десятка международных форумов, конференций-выставок «Интеллектуальные карты России». На них устанавливались и развивались контакты государственных регуляторов, бизнеса и других представителей отрасли. Удалось преодолеть стереотипы бизнеса, будто бы от государственных регуляторов нужно ждать только подвохов и лишних ограничений.

Всем сторонам очень помогло прямое личное общение на форумах, где каждому была предоставлена возможность высказать и отстаивать своё мнение в дискуссии. Государственные регуляторы начали лучше понимать проблемы бизнеса, а бизнес — необходимость регулирования и поддержки со стороны органов государственной власти.

Сильное деловое качество В.Г. Матюхина — умение организовывать взаимодействие и координацию ключевых участников отрасли. Для этого по его инициативе в 2000 году была создана Межведомственная комиссия по интеллектуальным картам. Сопредседателями стали Л. Д. Рейман — федеральный министр связи и информации, М. Ю. Сенаторов — заместитель председателя Банка России, В. В. Симонов — руководитель Российского агентства по системам управления и сам В.Г. Матюхин, в то время глава ФАПСИ.

Развитие взаимодействия участников отрасли помогло создать первую и, к сожалению, пока единственную российскую интеллектуальную карту (РИК). Это полностью отечественный продукт: и разработка, и операционная система, и производство. В чипе были реализованы российские стандарты шифрования и электронной цифровой подписи. Чип РИК и по сей день производится на заводе «Ангстрем» в Зеленограде и используется в контрольно-кассовой технике.

ВИДЕТЬ БУДУЩЕЕ

В настоящее время В.Г. Матюхин продолжает активную работу и научно-исследовательскую деятельность в должности первого заместителя генерального директора АО «НИИАС».

Стиль рабочих совещаний, которые проводит В.Г. Матюхин, неизменный.

В них участвуют представители всех звеньев выработки и исполнения принятых решений: от руководителей различных структурных подразделений до непосредственных исполнителей. Это позволяет оперативно получать полную, достоверную, не «приглаженную» информацию, всесторонне обсуждать вопросы и принимать обоснованные, взвешенные решения. Качество очень важное для руководителя.

Ещё одна прекрасная черта В.Г. Матюхина — умение смотреть в будущее. Поэтому он всегда уделял и продолжает уделять большое внимание образованию в сфере информационной безопасности — подготовке научных кадров, повышению квалификации специалистов. Именно благодаря его усилиям Военный институт правительственной связи в Орле в 2000 году получил статус Академии ФАПСИ (сейчас — Академия ФСО). Это учебное заведение стало настоящей кадровой кузницей специалистов по различным направлениям информационной безопасности.

Все замечательные качества специалиста и руководителя, обогащённые огромным опытом работы, и сейчас проявляются этим замечательным человеком в полной мере. Пусть каждый будет способен сохранять и приумножать свой многолетний потенциал так, как это делает Владимир Георгиевич.

Борис ГИРИЧЕВ

лауреат Государственной премии Российской Федерации в области науки и техники

ПРАРОДИТЕЛЬ ИДЕЙ

С Владимиром Георгиевичем Матюхиным мы познакомились, когда он уже был руководителем Научно-исследовательского центра Главного Управления безопасности связи ФАПСИ, а я возглавлял тогда Научно-технический центр «Атлас». Знакомство было на конференциях и научно-технических советах. Мы встречались, обсуждали общие научно-технические проблемы, спорили на различные темы. И нам всегда было крайне интересно контактировать в этом плане. Потому что в процессе разработки аппаратуры всегда возникает много технических и научно-технических проблем. Владимир Георгиевич, что меня в нём привлекало и очень подкупало, всегда очень глубоко видел научно-техническую составляющую задачи. Потому что у него была хорошая теоретическая база и он прекрасно разбирался в технике. То есть это уникальное сочетание, когда человек понимает и теоретическую часть, и может рассуждать как прикладник.

В 90-е годы был сильный провал в заказах со стороны различных ведомств и оборонных предприятий: была перестройка и заказы для оборонной промышленности сильно сократились. В итоге высвободились большие производственные мощности, которые необходимо было чем-то загрузить. С нашего предприятия высококвалифицированных специалистов было трудно пристроить в гражданские области, потому что у них специализированные знания именно по военной продукции. Это математики, технологи, конструкторы. К тому же это значило, что мы можем потерять будущий потенциал государства. И в «Атласе» встала задача этих специалистов занять какой-то деятельностью.

Однажды мы с Владимиром Георгиевичем встретились за обедом, стали обсуждать проблемы и рассуждать, куда двигаться и что делать в это «застойное» время. Я ему рассказал о пробле-

ме предприятия, что нечем загружать рабочих, нечем им платить. И тогда он сказал, что у него есть некоторые идеи и разработки, которые могут и должны стать составной частью дальнейшей работы НТЦ «Атлас». Я ему объяснил, что это так не сработает, а если и сработает, то в лучшем случае лет через пять. Из моего опыта руководителя и прохождения всех ступеней разработки на предприятии я знал, что для плодотворной работы обязательно нужно вместе собрать разработчика идеи, конструкторов и технологов. Ведь что такое разработка аппаратуры? Это итерация. Ты пробуешь что-то, собрал, запустил — нет, не пошло. Тебе правит теорию разработчик идеи, а конструктор подстраивается под него. То есть это непосредственное взаимодействие. И я тогда предложил ему следующее: он своих теоретиков передаст мне как штатные единицы, мы это всё решим на уровне ведомства, поскольку ведомство у нас было общее. Выйдем с таким совместным предложением. И он согласился.

ПРАРОДИТЕЛЬ ИДЕЙ

Идея защищённой телефонии, защищённой GSM-связи витала в воздухе. Потому что с появлением новых видов

связи всегда вставал вопрос об их защите. GSM-связь — это открытая связь, это отдельное направление, которым занимался тогда весь мир. И в Россию оно пришло из Европы. Но у нас в практическую плоскость в то время защиту этого вида связи пока никто не выводил. Владимир Георгиевич как раз занимался этим вопросом. Я бы назвал его прародителем этой идеи. И именно с его подачи эта идея была доведена до промышленного применения, до реального защищённого телефона.

При той нашей встрече он сказал, что существует практическая технологическая задача сделать защищённую связь и что на моём предприятии это можно сделать. Надо отметить, что именно Владимир Георгиевич был для «Атласа» толчком к развитию закрытой GSM-связи. Его идея легла на благодатную почву. Это была такая невинная беседа, мы не понимали последствия этих шагов. Я-то точно не понимал. Может, он и понимал. Но как осторожный и истинный учёный, он это выражал очень аккуратно.

Владимир Георгиевич передал «Атласу» полномочия, передал своих разработчиков, у которых, как оказалось, уже был примерно двадцатилетний опыт работы в этой области. Я им сразу вы-



делил отдельное помещение, снабдил вычислительной техникой и специальной аппаратурой, что-то пришлось докупить, в результате мы полностью оборудовали помещение. И буквально за 2–3 года появились первые защищённые сотовые телефоны в России.

Многие сначала сомневались, что направление защищённой GSM-связи укрепит и разовьётся до такой степени. Почему? Традиционный консерватизм людей, связанных с защитой информации. Отрасль очень консервативна, потому что очень большая плата за ошибки. Любые ошибки ведут к раскрытию связи, а раскрытие связи соответственно ведёт к большим потерям. И там действительно очень много научно-технических проблем. Но настойчивость Владимира Георгиевича и его уверенность, что мы добьёмся успеха, в итоге привели к положительному результату и прорыву в этой области.

Что я ещё в нём хотел бы подчеркнуть — научный оптимизм. Он очень тщательный и вникающий человек. У него это склад характера или особенности психики. В науке это очень важный элемент. С другой стороны, он не боялся рисков. Вот этот эксперимент с переводом сотрудников — это тоже было рискованно тогда.

И это дело превратилось в отдельное направление и в «Атласе», и в других фирмах России. А сейчас это воспринимается как естественное направление науки и техники.

ЧЁТКОСТЬ И ПОНИМАНИЕ

Когда Владимир Георгиевич был гендиректором ФАПСИ, я каждую неделю ходил к нему с докладами. Это могло быть от 2 до 5 встреч в неделю — директорат, технические совещания, научно-технические совещания. По всем техническим проблемам, касающимся «Атласа», я докладывал Владимиру Георгиевичу. И по любой инициативе с моей стороны Владимир Георгиевич всегда был открыт для встреч, то есть достаточно было поднять трубку, сказать, что есть вопрос, который нужно доложить. Он назначал время и нужно было чётко к этому времени приехать. Сам Владимир Георгиевич очень пунктуален и чётко, поэтому к нему на встречи старались никогда не опаздывать.



Кроме того, он был нормальным руководителем. С одной стороны, в нём сочетались стратегическое мышление, а с другой — навыки человека, прошедшего все ступени развития техники: он сам разрабатывал, сам считал формулы, сам нажимал на кнопки, сам что-то делал, сам добивался успеха, чтобы то, что он разработал, заработало. Когда сам прошёл все ступени и начинаешь руководить — совершенно другая картина. Он понимал все внутренние трудности создания чего-то. Поэтому, когда объясняешь ему, говоришь, что это невозможно сделать — он понимал.

Ещё он мгновенно понимал фальшь, если ты не знал предмета, о котором говоришь. Вот это у него исключительное чувство, чувство дотошности и чёткости. То есть к нему нужно было идти абсолютно подготовленным. Вот когда подготовлен, разговор получался аб-

солютно на «раз-два», просто глазами махнул, понял, идём дальше. А если ты не понимал его вопрос, лучше было говорить, что не понимаешь. В лучшем случае он отправлял ещё подумать и самому разобраться, в худшем — разводил руками и удивлялся твоему незнанию. Причём это не было обидно. Потому что чувствовалось, что за этим стоит огромный потенциал.

Но при этом он был достаточно требовательный. Очень мог спросить. И его слушались и уважали. Мы-то разработчики, которые из техники выросли, уважали его вдвойне за хороший и цепкий ум, за очень высокую квалификацию.

Он много создал в жизни. Поэтому удовлетворение от его работы испытывает не только он. Он как руководитель очень грамотный, и люди его любят. И за толковость, и за человеческие качества. Толковость с большой буквы.

Андрей ГАЛДИНруководитель Научно-технического комплекса технологий
информационного общества АО «НИИАС»

ЧЕЛОВЕК С БОЛЬШОЙ БУКВЫ

За долгие годы своей плодотворной профессиональной деятельности Владимир Георгиевич Матюхин в качестве участника и руководителя был причастен ко многим проектам, которые можно смело назвать прорывными для своего времени и которые сейчас составляют основу процесса цифрового развития страны и нашего общества.

Цифровизация обретает новый смысл в сегодняшней непростой экономической и эпидемиологической ситуации, требующей новых способов организации системы государственного управления и нетрадиционных механизмов взаимодействия между государственными органами, бизнесом и рядовыми гражданами.

Одним из высокотехнологичных инструментов технологии удалённого доступа, широко используемой в последнее время, являются видеоконференции, которые проводятся как в корпоративном секторе, так и на уровне органов государственной власти, в том числе с участием Президента Российской Федерации и членов правительства. При этом нельзя не отметить, что первые защищённые системы видео-конференц-связи высших государственных органов, в том числе защищённая система видео-конференцсвязи Президента Российской Федерации в федеральных округах и Ситуационный центр Президента Российской Федерации, были созданы на рубеже XXI века под научным руководством В. Г. Матюхина.

Обеспечение безопасности информационно-телекоммуникационных систем органов государственной власти (ОГВ) Российской Федерации являлось основным направлением деятельности В. Г. Матюхина в течение многих лет. Под его руководством введены в эксплуатацию информацион-

но-телекоммуникационные системы в Аппарате Правительства Российской Федерации, Совете Федерации и Государственной Думе Федерального Собрания Российской Федерации, Конституционном, Высшем и Арбитражном судах России.

Достоин упоминания и тот факт, что в созданном в первое десятилетие XXI века под руководством В. Г. Матюхина территориально-распределённом общероссийском государственном информационном центре (ОГИЦ) были впервые реализованы на практике ме-



Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте



ханизмы предоставления государственных услуг населению и организациям в электронном виде на принципе «одного окна». В настоящее время подобные механизмы позволяют эффективно обеспечивать непрерывность и качество предоставления необходимых государственных услуг, что особенно актуально сейчас в сложившихся неблагоприятных экономических условиях, а также в условиях режима самоизоляции граждан.

Удалённый режим работы, столь актуальный в настоящее время, связан с обработкой большого количества электронных документов, содержащих не только открытую, общедоступную информацию, но и сведения ограниченного доступа, например, коммерческую тайну. В таком случае на первый план выходят вопросы защиты обрабатываемой информации от несанкционированного доступа и искажения. Концептуальные основы защиты информации в электронном документообороте (ЭДО) на базе передовых научно-технических решений в области системотехники ЭДО и средств обеспечения информационной безопасности были разработаны и реализованы при руководстве и непосредственном участии В.Г. Матюхина в межведомственной системе защищённого электронного документооборота в интересах ОГВ Российской

Федерации, в первую очередь в Администрации Президента Российской Федерации и в Аппарате Правительства Российской Федерации.

Здесь нельзя обойти вниманием такое эффективное средство криптографической защиты информации в ЭДО как электронная цифровая подпись (ЭЦП), широкое внедрение которой в межведомственное информационное взаимодействие началось после вступления в силу в 2002 году Федерального закона «Об электронной цифровой подписи», разработанного под руководством В.Г. Матюхина. ЭЦП, кроме обеспечения целостности передаваемого сообщения, позволяет однозначно определить его автора, т.е. ее применение в текущей обстановке может препятствовать распространению в массовых сетях передачи данных недостоверной информации.

Большой вклад внёс В.Г. Матюхин в развитие такого незаменимого сегодня платёжного средства как микропроцессорные платёжные карты, призванные заменить наличные деньги, использование которых связано со многими проблемами. Ещё в 1993 году он выступил с предложением создания национальной платёжной системы на единой платформе информационной безопасности и на основе отечественных программно-технических решений, которая в настоящее время успеш-

но функционирует в России на базе платёжных карт «Мир».

В настоящее время плодотворная деятельность В.Г. Матюхина связана с железнодорожным транспортом России. Его тесные контакты с транспортной отраслью начались ещё в начале 2000-х годов, во время его работы на различных руководящих постах в государственных органах власти. Начиная с декабря 2010 года, на посту первого заместителя Генерального директора АО «НИИАС» Владимир Георгиевич все свои силы и знания отдаёт совершенствованию работы железнодорожного транспорта с использованием уникальных математических моделей и инновационных информационных технологий. Созданная в последние годы под его руководством и внедрённая в эксплуатацию в ОАО «РЖД» интеллектуальная система управления железнодорожным транспортом (ИСУЖТ) является незаменимым инструментом обеспечения эффективности и бесперебойности перевозочного процесса, что особенно актуально в текущей сложной обстановке. При создании этой системы был использован весь накопленный за долгие годы опыт Владимира Георгиевича и применены технологии и подходы, ранее апробированные в других отраслях нашего государства и заложенные при его участии в ОАО «РЖД» в начале двухтысячных годов.

Приведённые результаты многогранной и эффективной деятельности В.Г. Матюхина на различных научных направлениях свидетельствуют об его уникальных способностях предвидеть и реализовывать передовые научно-технические решения, востребованные в течение долгого времени и в любой обстановке для обеспечения государственных интересов и суверенитета России.

Уместным будет отметить, что именно благодаря разработке этих систем и внедрению их в АО «НИИАС», сотрудники института получили возможность в условиях борьбы с распространением коронавируса работать удаленно, с соблюдением всех технологических процессов, как и при обычной работе. Очень красноречивый пример цифровизации экономической деятельности в России.

Александр ШАБУНИН

руководитель научно-технического комплекса АО «НИИАС», лауреат премии Правительства России в области науки и техники 2019 года

КОЛОССАЛЬНЫЙ СДВИГ В ОТРАСЛИ

Владимир Георгиевич Матюхин — мой непосредственный начальник. В АО «НИИАС», дочерней компании РЖД, мы вместе работаем над проектом единой интеллектуальной системы управления на железнодорожном транспорте (ИСУЖТ). 9 лет назад Владимир Георгиевич по заданию руководства РЖД инициировал новое научное направление, началась напряженная работа, поиск компетенций и формирование коллективов.

НОВАТОРСТВО И ВНИМАНИЕ К ДЕТАЛЯМ

Один из важнейших принципов единой интеллектуальной системы — обеспечение автоматического адаптивного управления, которое реализуется через построение множества детализированных планов, покрывающих преимущественно все аспекты перевозочного процесса и все временные горизонты. Система призвана заменить человека в диспетчерском управлении. Я считаю, что это на тот момент была большая научная смелость сказать, что все эти планы и решения, которые традиционно делает человек, можно рассчитывать. Такого рода расчеты, учитывая размерность задачи, относятся к ряду сверхсложных систем. До В.Г. Матюхина таких требований к системам не предъявлялось, системы носили чисто информационный характер, а управление строилось в ручном режиме. И в итоге, сейчас это уже стало нормой в отрасли. И тема управляющих и интеллектуальных систем, и тема автоматического расчета планов и графиков. Это колоссальный сдвиг во всей отрасли. И В.Г. Матюхин стал тем человеком, который во многом способствовал этому сдвигу.

Вообще, ИСУЖТ очень сложная система с множеством новых сложнейших алгоритмов, преимущественно уникальных для железнодорожного транспорта. И эти алгоритмы нужно придумать или найти и применить для

каждого отдельного направления деятельности. Например, есть диспетчерское управление поездами на направлении, сменное-суточное планирование поездопотоком на полигоне железных дорог, нормативный график движения поездов и другие. Владимир Георгиевич едва ли не единственный человек, с которым мы всё это обсуждаем в деталях и ищем уязвимости. Не так много людей, которые даже в силу своих профессиональных обязанностей, вникают так глубоко в эти вопросы. Разработка и анализ алгоритма достаточно скрупулёзная тема, требующая высокого уровня технического образования, интуиции и опыта, и, конечно, большого терпения. Несмотря на то, что В.Г. Матюхин человек очень высокого ранга, ему это интересно. Он воодушевляет своим интересом. Рисуем на доске, разбираем ситуации, а потом это уходит в проектную группу, которая занимается реализацией. Всё идет через обсуждение с ним, через его участие. Он достаточно досконально участвует во всём.

УВАЖЕНИЕ К ЛЮДЯМ И ИХ ИДЕЯМ

Всем бросается в глаза, что В.Г. Матюхин уважительно относится к людям, к подчинённым. Меня всегда поражало, что даже если человек излагает свои мысли очень долго, Владимир Георгиевич всегда очень терпеливо, с большим уважением к чужому мнению (даже если его личное мнение будет другим) выслушает до конца. Мне кажется, это важная профессиональная черта не упустить какую-то мысль, которая будет полезна.

Вместе с тем он очень требовательный руководитель. Решение, которое ты предлагаешь, должно быть хорошо взвешено и продумано. Это своего рода как шахматная партия: ты должен на несколько шагов вперёд всё просчитать. Я думаю, что Владимиру Георгиевичу важно, чтобы у сотрудника была своя мысль, идея, просчитанная и аргументированная. Тогда к нему при-

слушаются. Если сотрудник говорит о том, в чём не разбирается, или лукавит, то Владимир Георгиевич его просто больше не позовёт на совещание. При этом ему ничего не будет высказано, но просто его больше не позовут. Я это наблюдал.

ОТСУТСТВИЕ СНОБИЗМА И СКРОМНОСТЬ

У Владимира Георгиевича очень демократичное общение. Когда ты общаешься с ним, понимаешь, что это человек из первой когорты управления государством, но при этом в нём нет чиновничьего пафоса. Я в каждодневном общении не воспринимаю его как генерала армии. Ещё я убедился в рамках нашего института, что попасть к нему в кабинет намного проще, чем к целому ряду других руководителей. Если ты идёшь по делу — на тебя всегда найдут время.

Мне очень симпатично это сочетание в В.Г. Матюхине — отсутствие снобизма, большое самоуважение и скромность. Например, я до прошлого юбилея не знал про многие его достижения и награды. Это всё не выпячивается. Мне кажется, это очень важная черта.

Ещё он очень пунктуален, будь это совещание с высоким руководством или с рядовыми сотрудниками, Владимир Георгиевич не опоздает.

За 9 лет у меня была возможность оценить дальновидность решений В.Г. Матюхина. Наряду с большим знанием людей, разных мнений, у него глубокий аналитический ум, который позволяет предвидеть вещи, всё взвесить, вернуться к вопросу, даже когда прошло какое-то время, и предложить решение, которое иногда кажется спорным, и через 2 года кажется спорным, а через 3 или 5 лет ты понимаешь, что это было чуть ли не единственно правильным решением. Это и есть такое стратегическое мышление. Я считаю работу рядом с ним большой честью — он действительно большой мыслитель.

Артем ЗУБКОВ

генеральный директор Медиа Группы «Авангард», издатель BIS Journal

«ВЫ — ЭТО ВАШ МАСШТАБ!»

Моё знакомство и дальнейшая работа с Владимиром Георгиевичем Матюхиным связаны с организацией и проведением РКІ-Форумов. Проводятся они с 2002 года, и «отцом-основателем» — инициатором, идеологом и главным организатором является именно он. Нас познакомил Сергей Кирюшкин, за что я ему глубоко благодарен. На встрече состоялся обстоятельный, очень дельный разговор. В результате наша Медиа-группа вот уже много лет выступает оператором организации и проведения РКІ-Форумов.

Ещё до первой встречи у меня сложилось представление о В. Г. Матюхине как о человеке легендарном, фундаментальном. Мои коллеги и знакомые отзывались о нём часто восторженно, с огромным пиететом. Государственный деятель, занимавший посты руководителя ФАПСИ, Росинформтехнологии, первого заместителя Министра обороны России... Генерал армии и видный учёный — доктор наук, действительный член нескольких академий...

При личном знакомстве я понял, что всё это, безусловно, важно, но не это — главное. Высокие чины и звания — это естественное следствие, внешняя форма мощной, масштабной личности. Меня поразило сочетание его очень доброжелательного отношения к собеседнику, ощущения полного контак-



та и, в то же время, чувство непреодолимой дистанции с человеком такого масштаба.

Неудивительно, что именно этот масштаб личности заставил Владимира Георгиевича поставить свои дарования на службу Родине, её благу. Глубокое знание истории, стратегическое мышление и умение видеть проблемы в широком контексте позволяют ему предвидеть будущее и тонко чувствовать международный контекст. А организаторский талант и умение выстраивать отношения с людьми создают широкие сети профессиональных

связей и направляют их потенциал на успех общего дела.

Все эти ценнейшие качества проявились и в ходе нашей совместной работы по организации и проведению РКІ-Форумов. Сейчас это ведущая Международная научно-практическая конференция, посвящённая «пространству доверия» — тематике электронной цифровой подписи и удостоверяющих центров. Не сомневаюсь, что во всех других выполненных проектах В. Г. Матюхину удавалось достигать таких же впечатляющих, максимально возможных результатов.

Мы привели лишь малую толику отзывов людей, близко знающих Владимира Георгиевича Матюхина, многие годы и десятилетия сотрудничавших с ним. Но даже эти короткие рассказы говорят о масштабе личности юбиляра. За скобками остались, к сожалению, многие свершения, отмеченные Государственными премиями, высокими правительственными наградами. Лишь упомянута и его сегодняшняя деятельность как большого ученого и умелого, мудрого организатора

науки, на десятилетия вперед закладывающая основы развития технических средств, инновационных интеллектуальных систем, востребованных завтрашним днем.

Поздравляя Владимира Георгиевича с 75-летием, таким, по сути, личным праздником, мы желаем ему долгих лет плодотворного служения родной стране, выбранной профессии и всему обществу в целом! Крепкого здоровья и новых свершений!

КРИПТОГРАФИЧЕСКИЙ ФРОНТ

В ДОКУМЕНТАХ ВРЕМЁН ВОВ

Криптографический фронт, сам по себе тайный, отразился, тем не менее в документах военного времени. Их не так много, но они позволяют почувствовать и особенности внешне малозаметных событий на этом фронте, и оценить повседневные заботы интеллектуального противоборства.

ВЕСТИ С ПРОТИВОПОЛОЖНОЙ СТОРОНЫ

Среди доступных ныне архивных документов времён Великой Отечественной войны присутствуют вести с противоположной стороны криптографического фронта: из шифровальных и дешифровальных организаций противника.

В военные годы такая информация была особенно ценна для военачальников и специалистов, поскольку создавала необходимую обратную связь и позволяла корректировать собственные оценки и действия.

ПОКАЗАНИЯ ПЛЕННОГО ПЕРЕБЕЖЧИКА

Один из подобных документов 1943 г. приведён на илл. 1, вот его содержание.

«Начальнику штаба Южного фронта
Гвардии генерал-лейтенанту тов. Бирюзову

15.9.43 года пленный перебежчик, немец ДЮВАЛЬ Фридрих, переводчик дешифровальной службы, 11 радиоразведывательной роты 549 полка связи 6А показал:

Немецкая радиоразведка 6А, за летний период 1943 года, дала командованию армии весьма ценный материал. В основном успешно перехватывалась двух, трёх и четырёх значная шифрпереписка 5УА, 2АК и армии, действующей в районе Красного Луча.

В результате дешифрования материала они устанавливали нумерацию войсковых соединений и частей указанных армий, намерение нашего командования и т.п.

Весь отработанный материал помещался в разведсводку, которая выпускалась три раза в день.

Пленный показал, что особенно легко поддаются к дешифрованию наши двух, трёх и четырёх значные коды, у которых ключи менялись через 5–7 дней. На дешифрование такого материала требовалось до двух часов, а после того как откроют все величины кодовой таблицы, то на дешифрование требуется 5–10 минут.

О предыдущем наступлении Южного фронта им было известно из материала дешифрования и в особенности по материалам миномётных частей — «Катюш», которые ранее получали по 1/2 боекомплекта, то в период наступления получали до 7 боекомплектов.

Из личного состава, применяющих кодированную передачу, часто встречались — Пономарёв, Собакин, Зайцев.

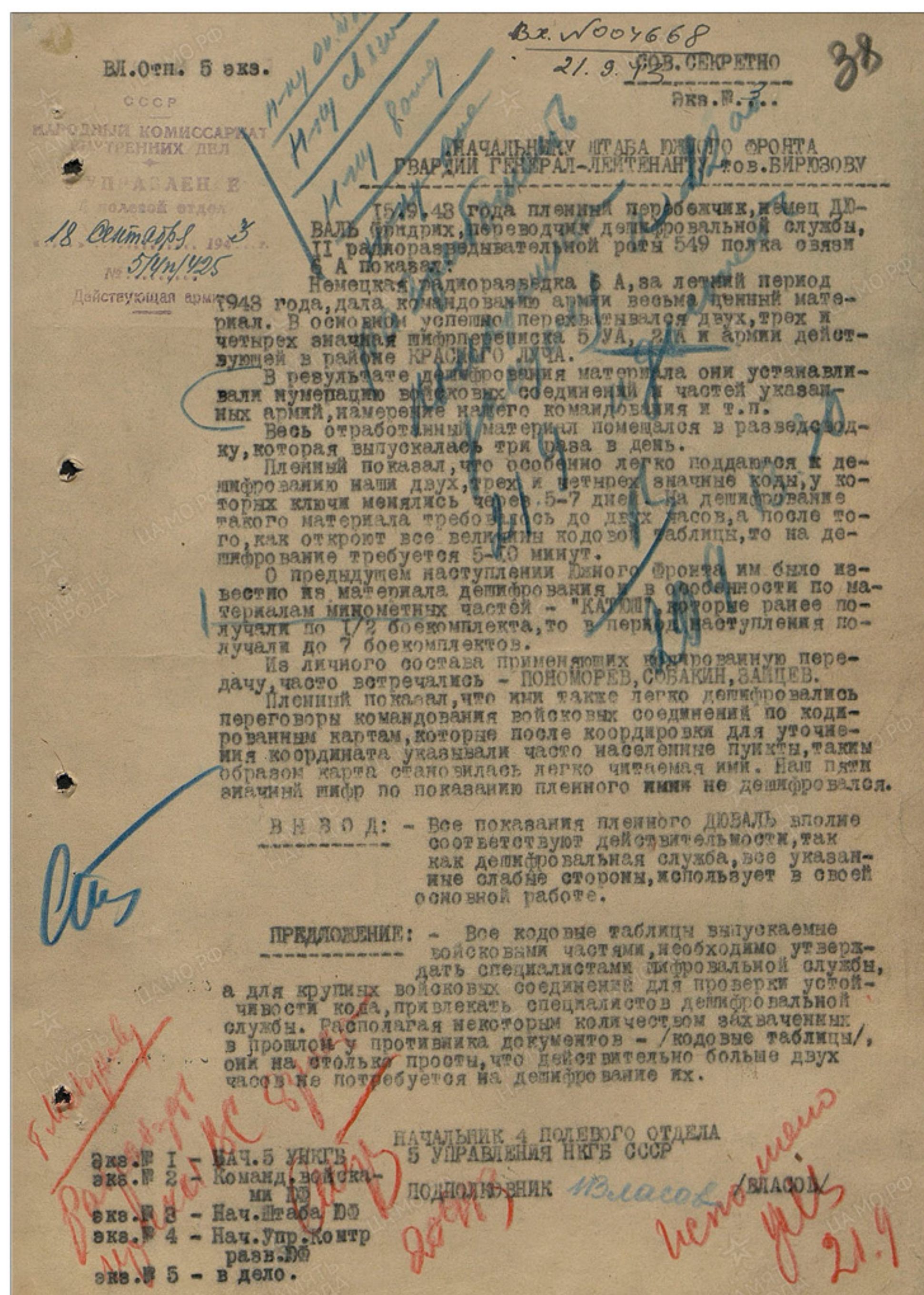


Иллюстрация 1. Сообщение о перебежчике из немецкой дешифровальной службы

Пленный показал, что ими также легко дешифровались переговоры командования войсковых соединений по кодированным картам, которые после кодировки для уточнения координат указывали часто населённые пункты, таким образом карта становилась легко читаемая ими. Наш пятизначный шифр по показаниям пленного ими не дешифровался.

Вывод: Все показания пленного Дюваль вполне соответствуют действительности, так как дешифровальная служба все указанные слабые стороны использует в своей основной работе.

Предложение: Все кодовые таблицы, выпускаемые войсковыми частями, необходимо утверждать специалистами дешифровальной службы, а для крупных войсковых соединений для проверки устойчивости кода, привлекать специалистов дешифровальной службы. Располагая некоторым количеством захваченных в прошлом у противника документов — (кодовые таблицы), они настолько просты, что действительно больше двух часов не потребуются на дешифрование их.

Начальник 4 полевого отдела 5 Упр. НКГБ СССР подполковник Власов».

НА ПЕРЕДНЕМ КРАЕ — ГИДРОМЕТЕОСЛУЖБА

Неоценим вклад советских криптографов в гигантскую работу по обеспечению безопасности проводной связи и радиосвязи для военных и гражданских нужд в масштабах всего СССР. Ведь криптографический фронт начинался за тысячи километров от линий боевого соприкосновения. Легко представить себе, например, как значимы были метеопрогнозы, особенно в суровых условиях Арктики. От метеосводок зависело и движение арктических конвоев союзников, и снабжение тружеников Крайнего Севера по всему Северному Морскому Пути, и боевая деятельность советского Северного флота. Германское командование было очень заинтересовано в получении арктических метеосводок. А поскольку собственные его возможности по сбору метеоданных в полярных морях были весьма ограничены, то от немецких подводников, случалось, требовали добывать секретные документы связи прямо на советских полярных станциях. Конечно, поляр-

6. Начальникам управлений Гидрометслужбы, начальнику Центрального института погоды и начальнику ГАМС совместно с органами НКС или узлов связи установить контроль за сохранностью г/м телеграмм, телеграфных лент и своевременным их уничтожением.

II. Порядок распространения цифровых метеорологических и аэрологических сводок

7. Все учреждения Гидрометеорологической Службы Красной Армии и других ведомств, ведущие передачу сведений о погоде, должны передавать поступающие к ним метеорологические и аэрологические сведения в виде сводок следующим порядком:

а) по радиотелефону, радиотелеграфу все метеорологические и аэрологические сводки, независимо от их объема, по всей территории Союза ССР только в зашифрованном виде, по действующему гидрометеорологическому шифру;

б) по прямому проводу (телеграфу и телефону) в адреса командования, АМС ВВС и органов Гидрометслужбы в открытом виде по всей территории СССР;

в) по коммутаторному телефону только в зашифрованном виде.

Примечание 1. В целях исключения случаев передачи по радио или коммутаторному телефону открытых метеорологических сводок в начале этих сводок должна делаться обязательная отметка «Только по прямому проводу».

2. Телеграммы с отметкой «Только по прямому проводу» обрабатываются, хранятся, учитываются и уничтожаются порядком, установленным для секретных документов.

8. В действующей армии сводки с результатами г/м наблюдений станций и (постов) наземных войск и АМС ВВС, по территории фронта разрешается передавать через коммутаторы войсковых частей и соединений открыто, при этом названии пунктов может передаваться только позывными, установленными командованием.

III. Штормовые предупреждения, оповещения и штормовая сигнальная служба

9. Гидрометеорологические станции, привлеченные к подаче штормовых оповещений, передают их по проводному телеграфу и телефону (прямому и коммутаторному) в установленные адреса, открыто по всей территории СССР, а по радио только порядком, предусмотренным в пункте 3 настоящего приказа, т. е. по специальным кодовым схемам.

10. Штормовые оповещения по территории фронта передаются отдельными метеопостами и станциями, в том числе ВВС и наземных войск — открыто. Название пункта (поста, станции) при передаче штормового предупреждения не передается, а сообщается только условный позывной данной воинской части или соединения, присвоенный командованием.

11. Штормовые предупреждения об ожидаемых опасных явлениях погоды передавать по проводному телеграфу и телефону в установленные адреса, а также по запросам командования армии, флота АМС ВВС и органов Гидрометслужбы открыто, а по радиотелеграфу и радиотелефону только в зашифрованном виде, по всей территории СССР.

3

Иллюстрация 2. Одна из страниц инструкции Гидрометслужбы

ники нередко оказывались не готовы к встрече с десантом врага среди ледяного безмолвия далеко-далеко от фронта.

РЕОРГАНИЗАЦИЯ СИСТЕМЫ ПЕРЕДАЧИ МЕТЕОДАНЫХ

Руководство Гидрометслужбы (ГМС) зимой 1941–42 гг. реорганизовало систему передачи метеоданных, обратив особое внимание на обеспечение секретности при пересылке сообщений. В марте 1942 г. вышла соответствующая инструкция, введенная в действие приказом по армии и флоту. Одна из её страниц приведена на илл. 2. В дальнейшем руководство ГМС постоянно разъясняло необходимость и порядок шифрования метеоданных в документах, рассылаемых в ГМО фронтов, добиваясь сознательного исполнения строгих требований. Об этом свидетельствует документ, направленный в

штаб Брянского фронта в январе 1943 г. Вот его содержание.

«Штаб Брянского фронта, Оперотдел
Начальнику Гидрометеотделения
...Учитывая, что за истекшее время несколько обновился личный состав ГМО, вторично направляю для руководства экземпляр инструкции, которую предлагаю изучить всему личному составу ГМО фронта и армий.

В виде разъяснения некоторых разделов этой инструкции, имеющих прямое отношение к работе ГМО, сообщаю.

Сбор метеорологических, гидрологических телеграмм о снеговом покрове и наблюдений за болотами с постов и станций наземных войск производится по кодам КН-02, КН-17, КН-18, КН-20 при наличии проводочной связи открыто, а при передаче этих сведений по радио дополнительно зашифровывается по специальным таблицам, согласованным

с Ш.О. Штаба фронта и утверждённым Начальником Штаба фронта. При этом название пункта, а также название или номер войсковой части включать в телеграмму категорически запрещается, как при передаче телеграммы по проводам, так и по радио. Вместо этих сведений указывать в начале телеграммы позывной, установленный командованием для данной войсковой части или соединения...

Сводные телеграммы из ГМО армий и ГМО фронта передаются по коду КН-2. При передаче этих телеграмм по проводам зашифровываются шифром «Горизонт» только координаты пунктов, при передаче по радио зашифровывается вся телеграмма.

Распространение краткосрочных прогнозов погоды в дивизии, полки, как правило, надо осуществлять при помощи связных, а в случае необходимости передачи этих прогнозов по проводам или радио последние надо кодировать (шифровать) действующими общевойсковыми секретными кодами или переговорными таблицами.

Гидрологические прогнозы передаются в адреса ГМО фронтов, армий в письменном виде, а в случае необходимости передачи их по проводам или радио только в зашифрованном виде, в этом случае табличная часть прогноза составляется по несекретному коду КП-56, а текстовая по несекретному коду КС-80, после чего производится перешифровка их по шифру «Горизонт».

Прогнозы суммы температур на декаду и прогноз приращения толщины льда, составленные по коду КС-80, перешифровываются по шифру «Горизонт».

Во избежание могущих быть недоразумений ещё раз разъясняю, что текстовой код КС-80 (как и всякий другой постоянный код) не является секретным, а служит лишь способом, при помощи которого секретный текст прогноза, консультации или справки переводится в цифровые группы, которые можно перешифровывать секретным шифром (в данном случае таблицами «Горизонт»). Поэтому код КС-80 без перешифровки никогда не применяется, т.к. секретности он не обеспечивает, а несекретные сведения по нему кодировать нецелесообразно, т.к. объём телеграммы при его употреблении по сравнению

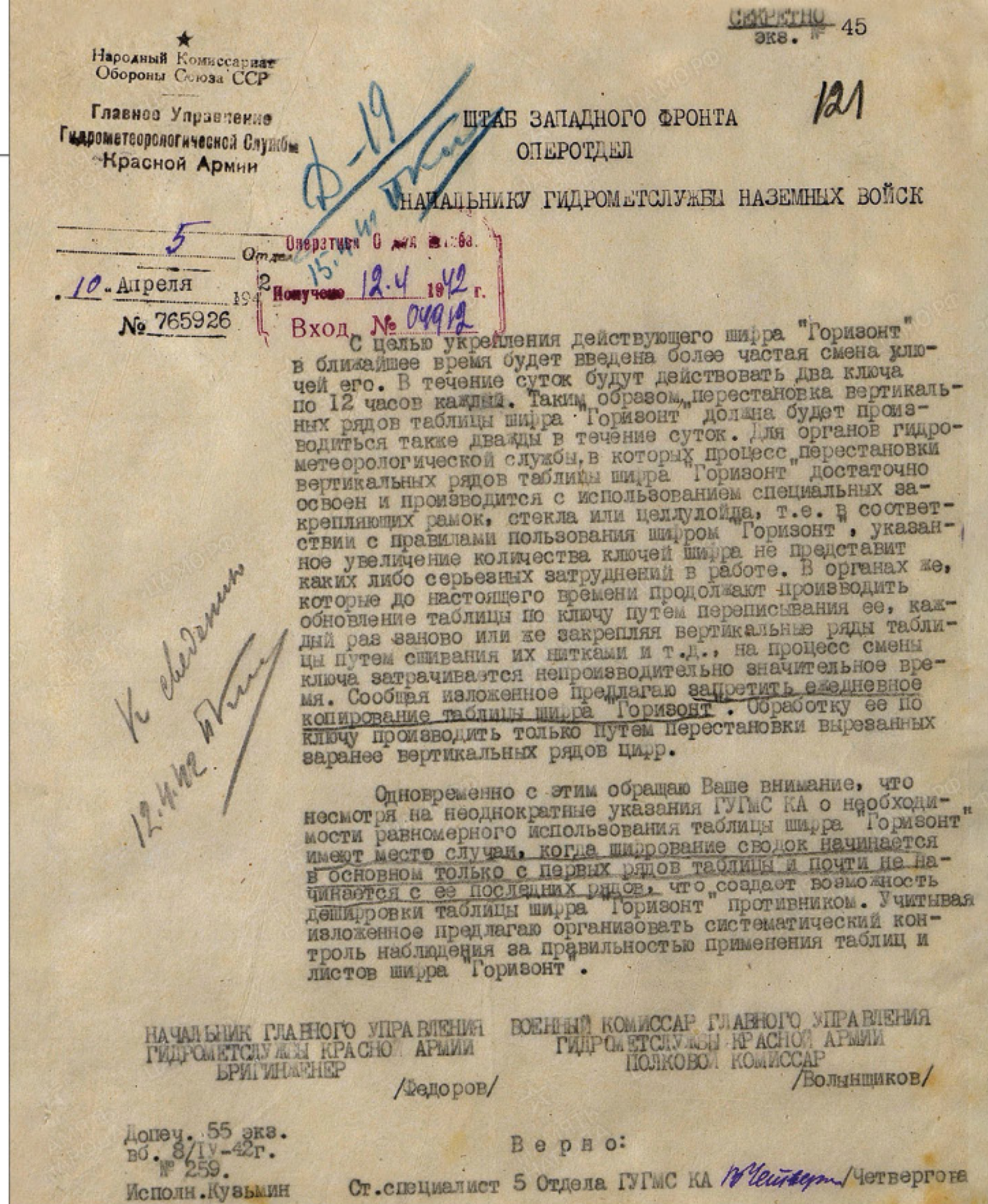


Иллюстрация 3. Директива ГУГМС Красной Армии

с открытым текстом не уменьшается, а количество искажений увеличивается».

«С ЦЕЛЮ УКРЕПЛЕНИЯ ДЕЙСТВУЮЩЕГО ШИФРА «ГОРИЗОНТ»

Документ с илл. 3, относящийся к апрелю 1942 г., свидетельствует о принятии мер по улучшению работы с шифрами по линии Гидрометслужбы.

«Штаб Западного фронта
Оперотдел
Начальнику Гидрометслужбы наземных войск

12.4.1942 г. С целью укрепления действующего шифра «Горизонт» в ближайшее время будет введена более частая смена ключей его. В течение суток будут действовать два ключа по 12 часов каждый...

Одновременно с этим обращаю Ваше внимание, что несмотря на неоднократные указания ГУГМС КА о необходимости равномерного использования таблицы шифра «Горизонт» имеют место случаи, когда шифрование сводок начинается в основном только с первых рядов

таблицы и почти не начинается с её последних рядов, что создаёт возможность дешифровки таблицы шифра «Горизонт» противником... Усилить контроль...».

Такое внимание к шифру «Горизонт» вполне объяснимо тем, что он был одним из основных метеошифров.

Начальник ГУ Гидрометслужбы Красной Армии бригадир Фёдоров, подписавший все приведённые здесь документы ГМС, это знаменитый полярник и геофизик, будущий академик Евгений Константинович Фёдоров. За работу на первой советской дрейфующей станции «Северный полюс — 1» в 1938 г. ему присвоили звание Героя Советского Союза. Начиная с 1939 г., он много лет возглавлял Гидрометслужбу СССР. Возможно, с такой стабильностью руководства этого ведомства связана и хорошая сохранность документов по засекречиванию метеосвязи военного времени.



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

«СЛУШАЮТ ИЛИ НЕТ?..»

ПУТЬ СОВЕТСКОЙ СЕКРЕТНОЙ ТЕЛЕФОНИИ ВО ВРЕМЯ ВОВ

Среди всех видов связи один привлекал к себе особенное внимание военачальников и организаторов обороны страны в годы ВОВ. Советское руководство и специалистов, конечно, весьма интересовал вопрос о возможностях противника по дешифрованию переговоров на линиях секретной телефонной связи.

ВЫДАЮЩЕЕСЯ ДОСТИЖЕНИЕ

Секретная телефония с 1943 г. заслужила одобрение и доверие высоких руководителей. И это было действительно выдающееся достижение криптографов и производителей. Оно дало возможность командующим армиями и фронтами связываться на поле боя друг с другом и со Ставкой Верховного Главнокомандования, не беспокоясь о сохранении секретности информации. Ныне мы можем с уверенностью сказать, что противнику не удалось дешифровать советскую секретную телефонию. Но в военные годы такой вопрос стоял перед криптографами постоянно. Постепенно развивались и методы дешифрования. В конце 1945 г. они позволили успешно дешифровать собственную секретную телефонию. Безусловно, это был большой

успех советской криптографии. Многие интересные подробности привёл в своей книге «В круге третьем» один из создателей советской секретной телефонии К. Ф. Калачёв.

ПРЯМОЕ ПРОСЛУШИВАНИЕ ЛИНЕЙНОЙ ПЕРЕДАЧИ

Первоначально, в 1930-е годы, и до 1943 г. в СССР использовался единственный метод оценки стойкости аппаратуры засекречивания: прямое прослушивание линейной передачи. Конечно, метод совершенствовался по мере накопления опыта разработок, промышленного изготовления аппаратуры и эксплуатации на линиях связи. Исходя из метода прямого прослушивания, подбирались и способы преобразования речевого сигнала, обеспечивающие достаточную маскировку речи. Речевой сигнал в электрическом виде имеет две основные характеристики — частотный спектр речи (300–3400 Гц в канале связи) и распределение энергии по спектру речи.

ОСНОВНЫЕ СПОСОБЫ ПРЕОБРАЗОВАНИЯ РЕЧЕВОГО СИГНАЛА В 30-Е ГОДЫ

Сначала, конечно, инверсия всего спектра речи, относительно его цен-

тра, в приборе — инверторе. При этом самые низкие частоты речи становятся самыми высокими и наоборот, и т.д. Этот способ имел широкое применение в мировой технике связи. Хотя инвертор обеспечивал маскировку в линии (вместо нормальной речи слышались визги и шумы), всё же противник мог восстановить исходную передачу, подключив к каналу связи аналогичный прибор.

Возможны также разбиение частотного спектра на ряд полос и перестановка их между собою, с применением независимой инверсии в отдельных полосах. Если преобразования меняются во времени под управлением шифратора, то задача для противника при перехвате усложняется: такая передача уже требует дешифрования.

Хотелось бы иметь и временные преобразования речевого сигнала, например, временные перестановки отдельных отрезков речи. Они ещё сильнее усложняют задачу противника. Но как сделать то, чего ещё никто не делал?

ПРЕДЛОЖЕНИЕ В.А.КОТЕЛЬНИКОВА

В.А. Котельников предложил использовать в аппаратуре засекречивания перестановку частотных полос с инверсией в сочетании с временными перестановками отрезков речи по 100 миллисекунд. При этом управление частотными и временными перестановками на передаче и приёме должно было осуществляться шифратором с выдачей 5 бит гаммы шифра примерно 10 раз в секунду.

В.А. Котельников предложил использовать в аппаратуре засекречивания перестановку частотных полос с инверсией в сочетании с временными перестановками отрезков речи по 100 миллисекунд

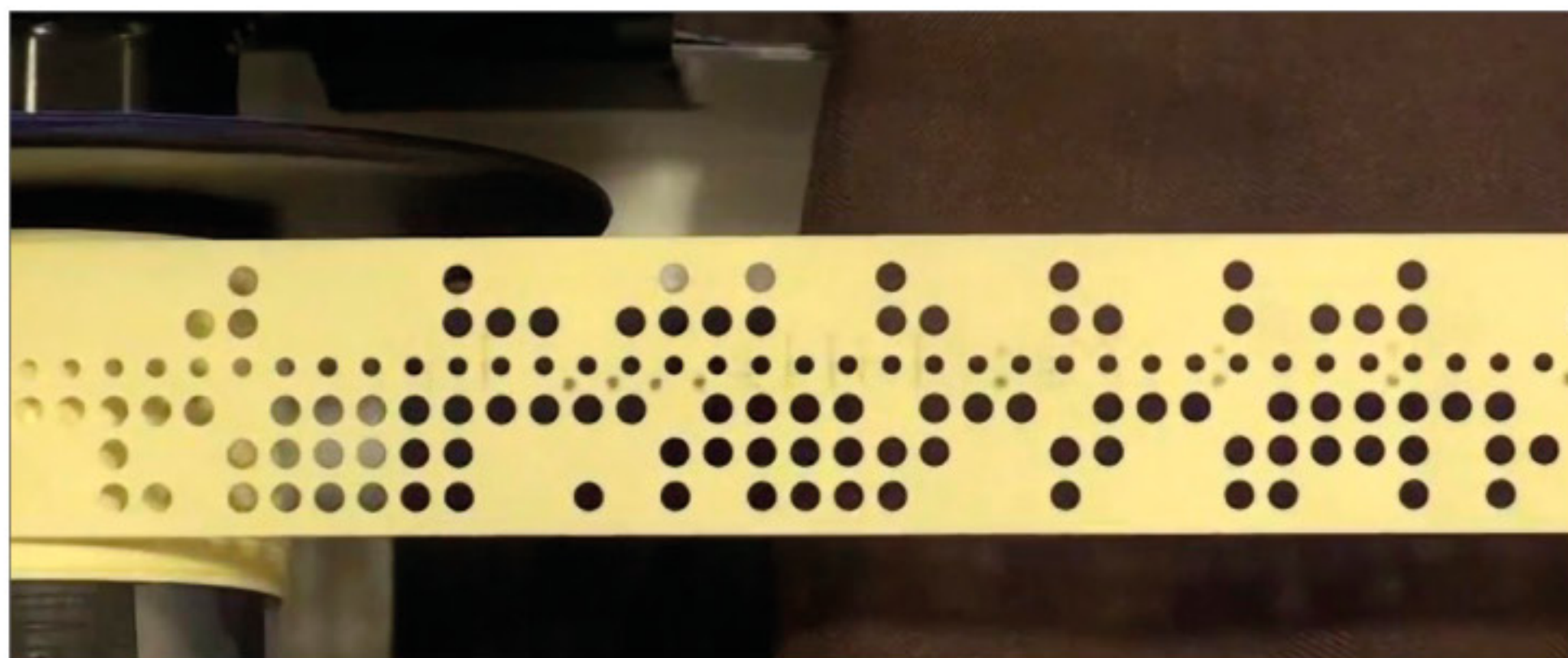


Иллюстрация 1. Пятирядная телеграфная лента

Заказчиком аппаратуры стал Отдел правительственной связи НКВД. И в 1940 г. в лаборатории Котельникова начались работы по изготовлению образцов наиболее сложного по тем временам аппарата телефонного засекречивания «Соболь-П», в котором использовались временные и частотные перестановки, а в качестве шифратора использовалась пятирядная телеграфная лента со случайно нанесёнными отверстиями. Случайность эта была весьма условной: ленту набивали «вслепую» машинистки, статистический контроль был слабый. Да и серьёзные статистические проверки в ту пору были невозможны.

ЦЕНОЙ САМООТВЕРЖЕННЫХ УСИЛИЙ...

Ценой самоотверженных усилий уже через три месяца после начала войны были изготовлены и испытаны лабораторные макеты основных узлов будущей аппаратуры «Соболь-П». Это были: узел частотных перестановок с инверсией спектра; узел временных перестановок; узел шифратора на базе транзистора и пятирядной перфорированной телеграфной ленты; макет генератора, создающего гамму управления перестановками частотных полос и временных отрезков.

Весьма ответственный узел временных перестановок состоял из двух главных частей: прибора замедления сигнала на 100 и 200 миллисекунд и схемы переключения замедленных сигналов, осуществлявшей перестановку отрезков речи по 100 миллисекунд. Много сложностей было связано с разработкой прибора замедления сигнала, пока, наконец, пришли к ре-

шению найти подходящую для магнитной записи сталь, а запись осуществлять не на плоскости диска, а на его ободе. К счастью, подходящей сталью поделился московский завод «Серп и Молот». Так решилась проблема создания узла магнитной записи, испытания которого показали приемлемый результат.

СЛОЖНЕЙШАЯ АППАРАТУРА ЗА ГОД ВЫДАНА НА БОЕВУЮ СВЯЗЬ

Лаборатория Котельникова, эвакуированная из Москвы в Уфу в ноябре 1941 г., вскоре после прибытия была разделена на две части. Большая часть во главе с В.А. Котельниковым вошла в ГСПЭИ 56. Другая часть лаборатории была переведена в НКВД.

В Уфе лаборатория Котельникова работала по своей основной теме — аппаратуре «Соболь-П». Её образцы получили боевое крещение уже в конце 1942 г. на радиолинии, восстановившей связь Москвы с Закавказьем. Закавказский фронт тогда имел исключительно важное значение. Он обеспечивал безопасность поставок грузов от союзников через Иран и Туркестан, по южному маршруту ленд-лиза. Кроме того, в портах Грузии базировался Черноморский флот, не позволявший румынским танкерам доставлять нефтепродукты на Кубань напрямую по Чёрному морю. В результате, горючее для немцев и их союзников, наступавших на Сталинград и Северный Кавказ, везли из Румынии автотранспортом.

Вызывает восхищение способность разработчиков, производителей и связистов, преодолев все трудности, за



Иллюстрация 2. Аппарат правительственной связи 1940-х годов

год создать сложнейшую аппаратуру и поставить её на боевую связь.

НАЧАЛО РАБОТ ПО ДЕШИФРОВАНИЮ ЛИНЕЙНОЙ ПЕРЕДАЧИ

Проработав немного более года в Уфе, лаборатория Котельникова в апреле 1943 г. перебазировалась обратно в Москву: её передали в ОПС НКВД. Таким образом, с весны 1943 г. в Москве, в НКВД, активно работали две лаборатории. В них ведущую роль играли сотрудники бывшей лаборатории Котельникова. Сам Владимир Александрович в 1944 г. перешёл на работу в МЭИ. В лабораториях разрабатывались несколько типов аппаратов секретной телефонии и одновременно начались серьёзные работы по дешифрованию линейной передачи. Кроме того, эти подразделения стали экспертами по оценке стойкости аппаратуры, создававшейся в других организациях страны.

Так, в конце 1942 г. при КБ завода № 209 в Ленинграде была организована лаборатория по разработке секретной телефонии. Лабораторию усилили специалистами из ОПС, бывшими сотрудниками Котельникова, в том числе А. П. Петерсоном.

АНАЛИЗИРУЕМЫЕ АППАРАТЫ

Опытное производство ГСПЭИ-56 в Уфе выпустило с 1941 г. 70 аппаратов типа инвертора. Завод № 697 в Уфе произвёл 1898 аппаратов засекречивания, в основном типа инвертора. В ряде аппаратов, в том числе опытных образцах аппарата «Соболь-П», использовался шифратор для изменения способа преобразования речи.

Завод № 209 в блокадном Ленинграде, начиная с 1942 г. выпустил 56 аппаратов засекречивания, причём в основном это были аппараты, имевшие шифрующие устройства со сложной механикой.

Из общего числа 22 разработок засекречивания телефонии 16 использовались на линиях, 6 завершились на уровне лабораторных образцов. При этом из 22 аппаратов 10 были маскирующими (с простой инверсией спектра), остальные имели шифратор. Самая сложная аппаратура была разработана в лаборатории Котельникова.

ОПЫТ ЭКСПЛУАТАЦИИ

1. Для связи Ставки Верховного Главнокомандования с фронтами по коротковолновым радиоканалам использовалась аппаратура «Соболь-П», а по проводным — «Сова», «Нева» и другие. Впервые аппаратура «Соболь-П» заработала в конце 1942 г. на КВ радиосвязи Москва-Тбилиси, заменяя нарушенную немцами на Волге проводную связь Москвы со штабом Закавказского фронта. Она действовала до окончания строительства новой линии проводной связи вдоль побережья Каспийского моря.

2. Техника засекречивания переговоров использовалась во время проведения Тегеранской, Ялтинской и Потсдамской конференций.

3. Аппараты «Соболь-П», «Нева» продолжительное время работали на связи Москвы с Хельсинки, Парижем и Веной в период проведения мирных переговоров.



Иллюстрация 3. Завод № 209

4. Тысячи инверторов и десятки аппаратов засекречивания с шифраторами работали на внутренних линиях связи страны.

СЕКРЕТНАЯ ТЕЛЕФОНИЯ В ДРУГИХ СТРАНАХ

Ныне известно, что работы по созданию техники секретной телефонии в Германии начались в 30-е годы. Первые аппараты были выпущены в 1932–33 гг. К работе были привлечены крупные фирмы АЕТ, Телефункен, Сименс. Согласно сведениям К. Ф. Калачёва, до 1945 г. они разработали 15 типов аппа-

ратуры и изготовили 2180 аппаратов. Основную массу (более 2100) составили различные типы инверторов.

Одновременно в военном ведомстве под руководством доктора Лотце велись исследования возможности дешифрования этой аппаратуры. Доктор Лотце дал отрицательное заключение о гарантии стойкости всех разработанных фирмами аппаратов. «К концу войны Германия не имела аппаратов засекречивания, которые были бы устойчивы против дешифрования».

К. Ф. Калачёв также отметил, что «В США и Англии в период войны использовалась пятиполосная аппаратура засекречивания с инвертированием спектра в отдельных полосах. Перестановка полос осуществлялась через продолжительное время, поэтому стойкость такой системы была весьма низкой».

«Что же можно сказать о переговорах, засекреченных нашей аппаратурой с наличием шифратора: дешифровались они в ходе войны или нет? На этот вопрос надо дать отрицательный ответ — нет.

Во-первых, спецслужбой таких фактов не зафиксировано. Во-вторых, как объяснили немецкие специалисты, дешифровальная группа доктора Лотце

BIS-СПРАВКА

Кратко напомним о Калачёве Константине Фёдоровиче (1915–2001 г.г.), одном из создателей советской секретной телефонии, ученике и соратнике В. А. Котельникова. С начала 1941 г. он участвовал в разработке прибора замедления сигнала; в октябре добровольцем выступил на защиту Москвы в составе дивизии народного ополчения; отозван с фронта в июне 1944 г. в Лабораторию специальной техники, бывшую лабораторию Котельникова, где занимался вопросами дешифрования аппаратуры телефонных передач; в Марфино он руководил группой, являвшейся криптографическим центром всей лаборатории; К. Ф. Калачёв занимал пост зам. директора по научной работе НИИ-2, преемника Марфинской лаборатории, с момента создания института в 1952 г. до 1970 г.

в Германии состояла из нескольких человек и имела целью давать оценки стойкости только разрабатываемой в этой стране аппаратуры. В-третьих, в первые послевоенные годы на связи Париж-Москва передачи с аппаратурой «Соболь-П» забивались помехой, а не перехватывались». Таково компетентное мнение К. Ф. Калачёва.

НОВЫЕ МЕТОДЫ ДЕШИФРОВАНИЯ

В СССР целенаправленные работы по дешифрованию телефонной засекреченной передачи начались с 1943 г. в 6 управлении НКГБ, в группе А. П. Петерсона из 5 человек. Одновременно эта группа вела разработки техники засекречивания.

Новые методы появились в связи с осмыслением всего опыта работ по разработке, производству и применению аппаратуры, а также в связи с появлением новых измерительных приборов.

Постепенно, под влиянием консультаций с Котельниковым, в группе Петерсона утвердилась мысль о необходимости изучения распределения энергии сигнала по частотам во всё время передачи. Идея была простой: следует попытаться восстановить энергетическую функцию исходного сигнала по энергетическим следам в отдельных полосах спектра за короткие временные промежутки передачи. Заметим, что с целью экономии полоса частот стандартного канала связи ограничивается примерно до частоты 3300–3400 Гц. При этом обеспечивается достаточно хорошая разборчивость речи и узнаваемость голоса.

Осуществить идею было очень сложно из-за отсутствия подходящих измерительных приборов, их тоже надо было создавать.

НАЧАЛО «СОКРУШЕНИЯ»

«Первые результаты появились в середине 1944 года. Используя многошлейфный осциллограф, группа А. П. Петерсона начала «сокрушать» аппараты засекречивания один за другим».

Лишь в 1946 г. в США, в журнале «The Acoustical Society», была опубликована статья с описанием анализатора спектра речи, Саунд Спектрографа. Это и был необходимый прибор. Ана-

лизатор давал двумерное изображение энергетики спектра речи: по горизонтали — время, по вертикали — частота, а энергия в отдельных полосах спектра определялась степенью почернения фотобумаги, что характеризовало уровень сигнала при его записи.

При этом вся площадь спектрограммы разбивалась на маленькие прямоугольники размером $F \times t$, где F — ширина полос разбиения спектра речи, а t — минимальная длительность отрезка передачи при разбиении ее по времени. Подобные приборы и стали основой для создания новых методов дешифрования по фиксации распределения энергии сигнала. Тем самым, в криптографии решительно утвердились физические методы анализа аппаратуры.

ДЕШИФРОВАНИЕ МОЗАИЧНЫХ СИСТЕМ

Поясним сначала, что такое мозаичная система шифрования. «Узел шифратора, осуществляющий частотные преобразования, переставляет прямоугольники $F \times t$ по частоте, в некоторых случаях инвертируя спектр частот, а узел временных перестановок переставляет их по времени. Так, из «плавной» спектрограммы речи появляется «мозаичная» картинка».

До 1943–1944 г.г. казалось невозможным по линейной передаче восстановить нормальную речь с исходным положением её отрезков, ведь спектрографа или сходных приборов ещё не было. Единственным методом оценки стойкости был метод прослушивания линейной засекреченной передачи, при этом использовались двузачные числа, отдельные слова и фразы. И аппараты засекречивания с шифратором обеспечивали необходимую стойкость против такого дешифрования.

А вот многошлейфный осциллограф или, ещё ярче, спектрограф при значениях F в сотни герц и величинах t в 60–100 миллисекунд при глубине временных перестановок в 200 миллисекунд позволили восстановить исходную картину спектрограммы, т.е. дешифровать передачу.

ПО СТУПЕНЯМ УСПЕХА

Начиная с середины 1944 г. до конца 1945 г. группа А. П. Петерсона вы-



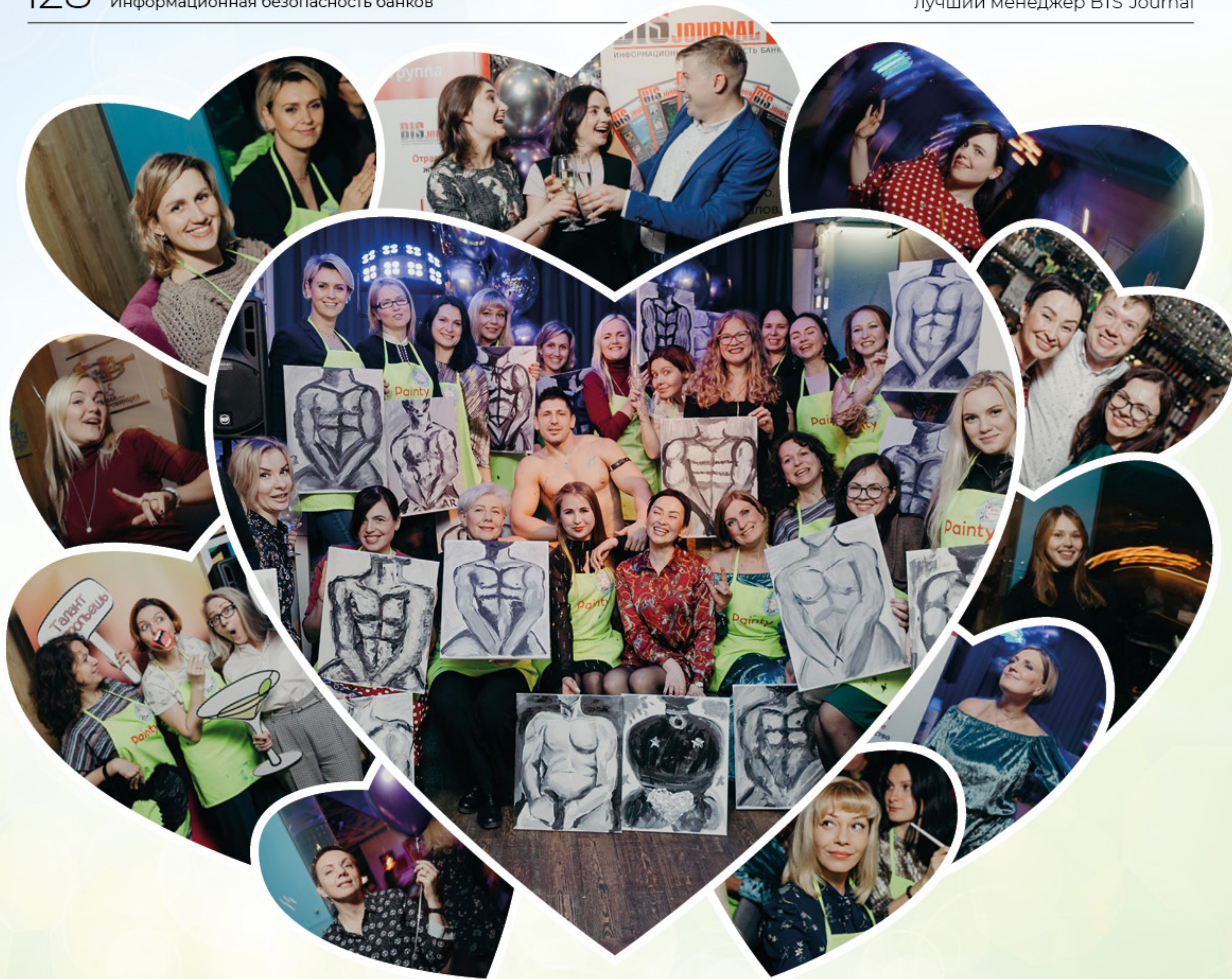
Иллюстрация 4. В. А. Котельников, дважды лауреат Сталинской премии, 1946 г.

дала отрицательные заключения на все аппараты засекречивания телефонии, используя в своём анализе многошлейфный осциллограф, прообраз американского Саунд Спектрографа.

Итоговым документом исследований явился отчёт, утверждённый 28.12.1945 г. Его главные положения:

1. Все аппараты мозаичного типа дешифруемы.
2. Нельзя увеличить стойкость за счёт уменьшения F и t , так как резко ухудшается качество восстановленной речи.
3. Создавать стойкую аппаратуру можно двумя путями — усложнением разрабатываемой мозаичной аппаратуры, а также использованием вокодера в качестве речепреобразующего устройства.

Значение этих событий трудно переоценить. Следствием их в скором времени стали организация известной ныне Марфинской лаборатории, широкий разворот работ по созданию стойкой к дешифрованию секретной телефонии и высокоскоростных шифраторов, а затем и постепенный выход советской криптографии на передовые позиции в мире.



РАЗОЖГЛИ В СЕРДЦЕ ОГОНЁК

За последние два года BIS Journal создал традицию чисто женских встреч для маркетологов в сфере ИБ. Одна из самых ярких состоялась 11 марта — она стала последней фееричной вспышкой перед тем, как мир замер, и всё в нашей жизни пошло не по плану.

Это был вечер, полный сюрпризов. Эмоции зашкаливали, им не было конца: от недоумения при виде строя мольбертов с кистями и красками, загадочных улыбок организаторов и трепета от хлопков открывающегося шампанского до неожиданного и крайне эффектного появления натурщика, рельефный торс которого нашим гостям и предстояло запечатлеть на своих холстах. Боевые жрицы маркетинга не растерялись и изящными движениями рук справились с поставленной задачей. Думаем, любоваться на собственные шедевры и вспоминать моменты напряжённого творчества они будут ещё долго!

Ну, а по окончании творческой части, по традиции, все понеслись в вихре танцев! BIS-Огонёк — это когда все на одной волне, это праздник, на котором встречаются старые друзья и заводятся новые знакомства, это непередаваемые ощущения и впечатления!

От всей души говорим СПАСИБО прекрасным девушкам, которые приходят к нам на огонёк, дарят улыбки и заряжают своей энергией. Не сомневаемся, что равновесие в мире скоро восстановится, и мы встретимся вновь!

Что будет? Новый сюрприз...



НАША ИГРА

— *home edition* —

Новые впечатления, интересные вопросы и призы —
в ИБ-викторине «Наша игра» Home edition!
Проведите вечер в компании коллег, соревнуйтесь
и общайтесь в онлайн-игре для специалистов
информационной безопасности

ib-bank.ru/igra/home



АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Образование
и карьера

ib-bank.ru