



29 Игорь ЛЯПУНОВ
ПАО «Ростелеком»
5 лет стартапу!

34 Анатолий АКСАКОВ
Государственная дума РФ
ЕФРДН. Третий лишний

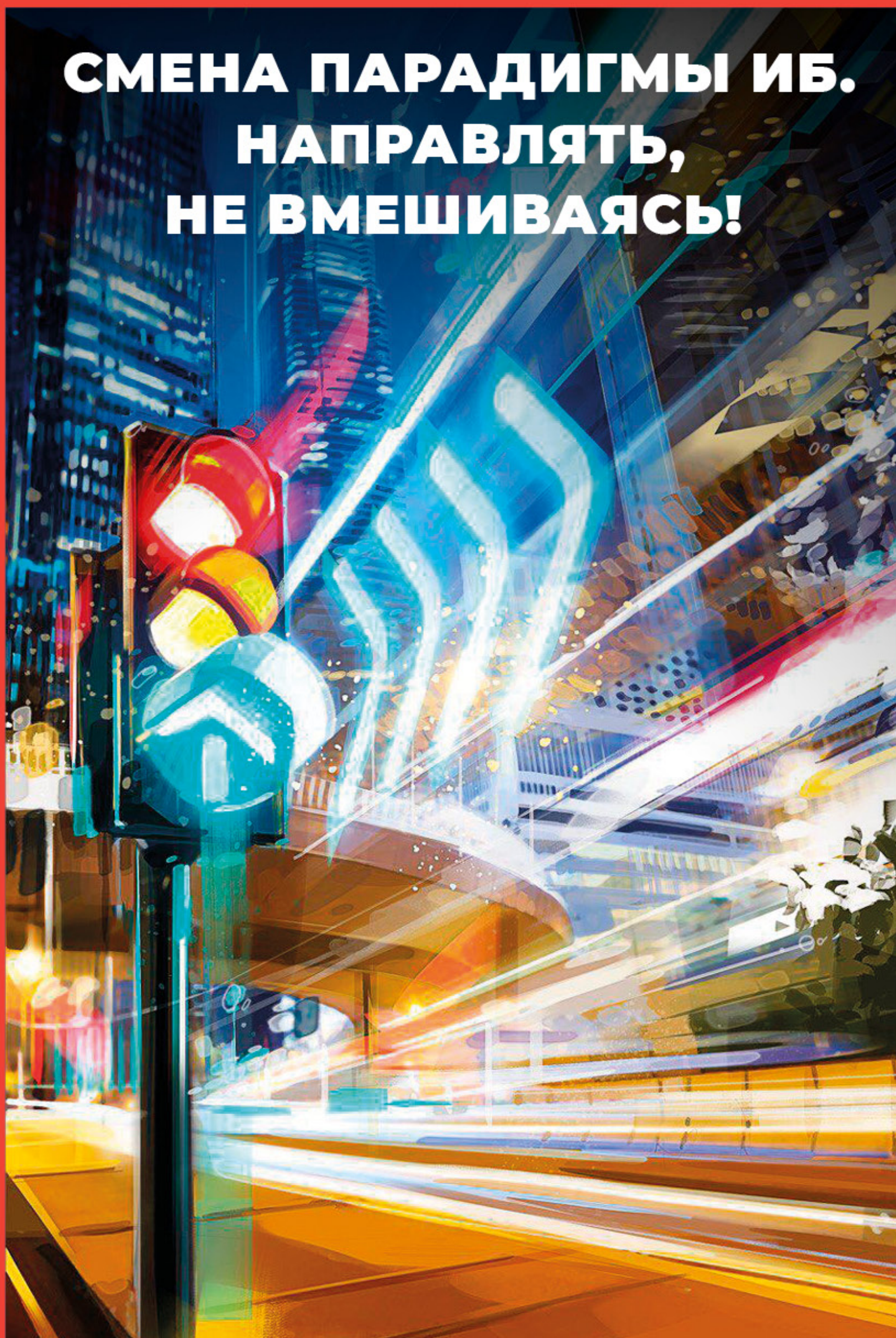


42 Сергей ПАЗИЗИН
Банк ВТБ (ПАО)
Про экспертное сообщество

60 Александр БОДРИК
Бизнес-инкубатор Cyberlands B.V.
Нашествие маленьких контейнеров

104 Дмитрий ЛАРИН
историк криптографии
Криптографы СССР
против самураев

СМЕНА ПАРАДИГМЫ ИБ. НАПРАВЛЯТЬ, НЕ ВМЕШИВАЯСЬ!



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



Рустэм ХАЙРЕТДИНОВ
приглашённый редактор
юбилейного номера BIS Journal

Вы держите в руках или разглядываете на экране уникальный номер. Когда я читал вёрстку, мне вспомнились перестроечные дискуссии в стиле «открытых писем» — известный эксперт высказывает спорную и даже в чём-то провокационную точку зрения, порождая дискуссию, которая захватывает не только первоначальную тему, но и после нескольких итераций расширяется до крамольного «а не сменить ли всю систему?» Давно так предельно откровенно экспертное сообщество публично не обсуждало животрепещущую тему государственного регулирования информационной безопасности.

Сегодня с ускоренной цифровизацией выбор «эффективное или сертифицированное», «делать как положено или как работает» и т.п. вышел за пределы тесного экспертного сообщества и стал системным — от него зависит работоспособность ключевых государственных и бизнес-систем. Начав говорить о том, как государству стоит регулировать информационную безопасность, большинство экспертов не останавливаются на этом и развивают тему до смены парадигмы информационной безопасности в стране и мире.

А эксперты все как на подбор — это и, не побоюсь этого слова, патриархи отечественной информационной безопасности, стоявшие у колыбели российского регулирования ИБ, и практики информационной безопасности, ежедневно защищающие огромные информационные системы отраслевого и государственного значения, и производители и поставщики решений в области безопасности, составляющие значимый кусок профильного рынка. Каждый эксперт видит проблему под собственным углом, но на то он и эксперт, чтобы понять чужую точку зрения и аргументированно ей возразить.

Какой быть информационной безопасности в цифровую эру? Чем мы ответим на ещё не до конца понятые угрозы нового мира? Чем нам может помочь или помешать государственное регулирование? Как совместить противодействие наднациональной международной киберпреступности и национальные интересы? Международные практики или свой путь?

Пожалуй, впервые эти вопросы вылились из кулуаров профильных конференций и стали достоянием общественности. Спасибо всем экспертам за взвешенность суждений и открытость. А журналу — за инициативу и этот поистине прекрасный номер, который с интересом читается от корки до корки.

Наслаждайтесь.

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
Левинов Д. О. — председатель Совета НП «Партнёрство 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, waralbum.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 (Роскомнадзором).
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 21.07.2020. 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





ТОЧНО В ДЕСЯТКУ

10 ЛЕТ НАЗАД ВЫШЕЛ В СВЕТ ПЕРВЫЙ НОМЕР BIS JOURNAL

Десять лет назад стартовало издание BIS Journal — свидетель и участник становления и расцвета отрасли информационной безопасности финансовой сферы. Теперь мы отмечаем юбилей; но какой, большой или малый? Для седых пирамид десятилетие — миг, а «для звезды, что сорвалась и падает», — практически вечность.

ИНФОРМАТОР-ОРГАНИЗАТОР
Десять лет назад отрасль информационной безопасности финансовой сферы только завершала своё становление. Её целостность собиралась встречно: сверху донизу и снизу доверху, всё многообразие секторов и сегментов. «Вершками» выступали государственные регуляторы с их нормативно-правовой базой, контролем и надзором.

Дальше шли финансовые организации, в первых рядах которых гвардия — банки. Ещё дальше разработчики и поставщики товаров и услуг — оборудования, ПО, подготовки и переподготовки кадров. И наконец, корневая система — огромная аудитория пользователей электронных финансовых услуг — организаций и граждан.

Окончание на стр. 4

Артём СЫЧЁВ

Первый заместитель директора Департамента информационной безопасности Банка России, доктор технических наук



«ИЗДАНИЕ УНИКАЛЬНОЕ, ЕДИНСТВЕННОЕ В СВОЁМ РОДЕ»

— Какую роль, на ваш взгляд, сыграл BIS Journal в становлении отрасли ИБ?

— BIS Journal — отраслевое издание, первое и, пожалуй, уникальное, единственное в своём роде на рынке СМИ. Сфера ИБ в принципе новая в России, а ИБ финсектора создавалась буквально на наших глазах. В этих условиях редакции было необходимо держать планку, точно фиксируя темп и направление развития отрасли и обеспечивая детализацию и глубину проработки освещаемых вопросов. Это означало необходимость с одной стороны оперативно отслеживать происходящие изменения, с другой — подталкивать участников рынка быстрее и правильнее на них реагировать и инициировать свои собственные в ответ. В итоге журнал стал «настойной книгой» и учебником для многих наших коллег в финансовых организациях, ИБ-компаниях, госструктурах. Но самое важное то, что подшивки журнала читают студенты профильных вузов. Это залог преемственности и при этом творческого переосмысления накопленной базы знаний — которые в конечном итоге и обеспечивают развитие отрасли.

— Вспомните интересные эпизоды, ситуации, связанные лично для вас с BIS Journal?

— Уральский форум, который мы ежегодно проводим при поддержке Медиа Группы «Авангард». Каждый год это не эпизод, а событие, значимое для всей отрасли.

— Как изменялся за эти десять лет ландшафт российской ИБ? И как изменился BIS Journal?

— ИБ — сфера очень консервативная, как, наверное, любая, в общем-то, безопасность. С одной стороны, это помогает минимизировать риски наиболее незатратным способом, с другой — несколько ограничивает возможности развития зависящих от нее направлений. Поэтому сейчас мы как регулятор выводим деятельность ИБ-подразделений финансовых организаций из области периметровой защиты, делая её более проактивной путем оценки рисков с точки зрения обеспечения надежности и непрерывности оказания услуг. BIS Journal нам в этом смысле оказывает неоценимую поддержку, публикуя подробные разъясняющие материалы и подробно освещая профильные мероприятия. Очень радует, что некоторое время назад редакция начала обращать более пристальное внимание на зарубежную практику, публикуя новости о резонансных событиях в сфере ИБ. Хотелось бы видеть на страницах ещё больше таких материалов, в том числе, касающихся практики регулирования и стандартизации.

Андрей КУРИЛО

президент компании «Реальная безопасность», кандидат технических наук



«СТАЛ ЛУЧШИМ ЖУРНАЛОМ ОТРАСЛИ»

— Какую роль, на ваш взгляд, сыграл BIS Journal в становлении отрасли ИБ?

— Несомненно, обогатил, став, пожалуй, лучшим журналом отрасли. Причём он очень быстро перерос и отраслевые рамки.

— Вспомните интересные эпизоды, ситуации, связанные лично для вас с BIS Journal?

— Для меня журнал неразрывно связан с Уральским форумом.

— Как изменялся за эти десять лет ландшафт российской ИБ? И как изменился BIS Journal?

— Журнал развивался адекватно развитию и модификации отрасли.

— Какой вы видите отрасль ИБ через десять лет? И каким, на ваш взгляд, станет BIS Journal?

— Хотелось бы видеть отрасль более структурированной.

— Что, на ваш взгляд, нужно сделать сегодня, чтобы журнал стал ещё лучше, ещё интереснее для своих читателей?

— Думаю, расширять тематику публикаций: право, блокчейн, цифровые валюты, управление безопасностью, импортозамещение — как постоянные рубрики.

Окончание. Начало на стр. 2

Важную роль играли гуманитарные коммуникации — общение и дискуссии, обсуждение насущных проблем и совместная выработка решений. Организация и проведения деловых и прочих мероприятий, отраслевые периодические издания и специальная литература.

Учитывая межотраслевой характер информационной безопасности, такие коммуникации были крайне важны. Чтобы помочь выработать общий язык и найти взаимопонимание специалистам довольно разных специальностей: по финансам, общей и цифровой безопасности, каналам связи, противодействию преступности и ещё много чему.

Вот на этом-то, казалось бы, второстепенном, «надстроечном», но крайне важном уровне и родился журнал «BIS Journal — Информационная безопасность банков». Как постоянный канал внутриотраслевого общения, прекрасно дополняющий мероприятия, проходящие «в реале».

Журнал был призван сыграть роль, в духе формулировки классика, не только коллективного информатора, но и коллективного организатора. Неудивительно, что издателем стала Медиа Группа «Авангард», многолетний оператор главного делового события отрасли — Уральского форума. Смелая инициатива превратилась в начинание, на смену становлению пришло устойчивое развитие.

ПЕРВАЯ ЛАСТОЧКА

За прошедшие десять лет переменилось многое: мир и наша Родина, средства информационных атак и защиты, отрасль и её участники, в том числе и мы сами. Наш журнал всегда старался находиться на переднем крае острой и актуальной проблематики.

Дистанционное обслуживание, актуализировавшееся во время карантина от коронавируса, автоматизированные антифрод-системы, импортозамещение, национальная платёжная система, защита персональных и биометрических данных, противодействие киберпреступности и «социальной инженерии»...

«Все промелькнули перед нами, все побывали тут».

Рождались и гибли миры, могущественные и влиятельные силы исчерпывались, оставаясь в прошлом, появлялись новые герои и действующие лица. Иных уж нет, а те далече...

Тем временем компания «Авангард» постепенно переросла в формат медиа группы, стала холдингом гуманитарных коммуникаций. Наше специализированное издание стало бесспорным медиа-лидером отрасли, а по ряду параметров вообще уникальным. BIS Journal оказался первой ласточкой — медиа-первенцем, пробой сил, экспериментальной площадкой и... космодромом для новых стартов.

Базовый сайт ib-bank.ru разросся в ведущий отраслевой многопрофильный информационный портал. К деловым мероприятиям (ib-bank.ru/events), кроме журнала (ib-bank.ru/bisjournal), добавился раздел BIS Job (bisjob.ib-bank.ru), посвящённый сквозному обучению, образованию и карьере. Ресурс прирастал отраслевыми интернет-телевидением BIS TV (ib-bank.ru/bistv), издательством (books.ib-bank.ru), «энциклопедией» терминов (ib-bank.ru/glossary) и каталогом решений (catalog.ib-bank.ru).

ЛЮДИ — ГЛАВНОЕ БОГАТСТВО

Нельзя не отдать должного сотрудникам Медиа Группы «Авангард» и лично А. Н. Зубкову, её бессменному лидеру. Слагаемые успеха одновременно и банальны, и почти неповторимы. Это фантастическая энергия, чутьё на перспективное новое, дерзание и выдержка, неистощимая энергия и умение вовремя проводить «работу над ошибками». А также способности вкладывать в дело всего себя, всю душу и сердце, устанавливать теснейшие взаимосвязи с единомышленниками и «товарищами по оружию»...

Однако редакции и издателю журнала мало что удалось бы без дорогих коллег, которые приняли участие в развитии журнала, разделяя все трудности и радости побед. Без участников редакционной коллегии, общественного совета и экспертов журнал оставался бы узким междусобойчиком.

Прочтите список в выходных данных — это лучшие специалисты, энергичные, активные, инициативные, отзывчивые

люди, которые не за страх, а за совесть радеют за успех нашего общего дела. Не только пишут статьи, но и привлекают других авторов. Хотелось бы рассказать о каждом; по крайней мере, ту информацию, которая является открытой... Увы, места в небольшой статье не хватит, понадобится специальный выпуск журнала.

Но необходимо упомянуть тех, кого уже нет с нами. Алексея Сергеевича Кузьмина — крупного руководителя, большого учёного, дальновидного стратега, требовательного и доброжелательного человека. Фарита Музипова — «самого вежливого человека в отрасли», как его называли все; инициативного и исполнительного, согревавшего любой коллектив своей улыбкой и теплом души.

Слова благодарности и тем, кем и для кого живёт журнал — всем авторам и аудитории. Тем, кто вынашивал и рождал важные мысли. Тем, кто читал статьи, выражал восторги и высказывал критические замечания. И, конечно же, рекламодателям, представляющим свой взгляд на проблемы и их решения. Без их поддержки журналу развиваться было бы нелегко.

Каждый из коллег по журналу, независимо от званий, регалий, места работы и должности — наш соратник. Главное, что все вместе мы — соучастники выработки и реализации редакционной политики. Поровну и трудности, и заслуженная слава. Сердечное вам спасибо и самые теплые пожелания в эти юбилейные дни!

Оглядываясь на прошедшее десятилетие, сравнивая исходные позиции и нынешние, оцениваешь динамику развития. Выигрывать темп важно не только в шахматах, но и в жизни, и тем более в информационной безопасности финансов.

Мы будем уверенно двигаться от ретроспективы к футурологии, смело смотреть в будущее, стараясь правильно предугадывать и... творить по мере сил. Наш журнал вслед за Медиа Группой «Авангард» неуклонно старается следовать лозунгу: всегда впереди!

Александр ВЕЛИГУРА

председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», кандидат физико-математических наук



«ЖУРНАЛ СТАЛ „КОРНЕМ“ ПОРТАЛА И BIS TV»

— Какую роль, на ваш взгляд, сыграл BIS Journal в становлении отрасли ИБ?

— Важную. Журнал «держал» аудиторию между мероприятиями и давал возможность высказаться тем, кто по разным причинам не выступал на конференциях. Многим из тех, кто выступал, журнал давал возможность изложить свою точку зрения более развернуто, а читателю — лучше её воспринять. Многие темы вообще не отражались на конференциях.

— Как изменялся за эти десять лет ландшафт российской ИБ? И как изменился BIS Journal?

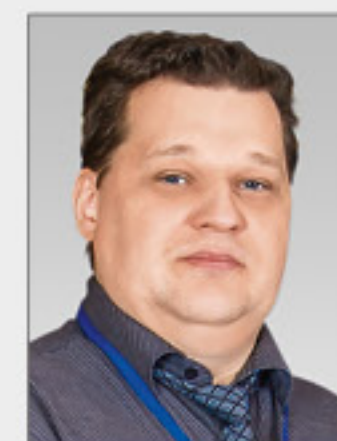
— Ландшафт менялся вместе с жизнью — новые технологии, новые угрозы. Журнал стал, на мой взгляд, «корнем» портала, появилась электронная версия, BIS TV. Это правильно.

— Что, на ваш взгляд, нужно сделать сегодня, чтобы журнал стал ещё лучше, ещё интереснее для своих читателей?

— Сейчас, на мой взгляд, он уникален (среди журналов по ИБ-тематике) тем, что он, как это раньше называлось, «научно-популярный». Это нужно сохранить. Что можно бы добавить — регулярные обзоры международного положения в нашей области — какие документы выходят, какие предложения делаются, какие события происходят.

Александр ВИНОГРАДОВ

специалист Службы информационной безопасности КБ Максима



«ЕГО ДАЖЕ КУРЬЕРЫ ЧИТАЮТ!»

— Какую роль, на ваш взгляд, сыграл BIS Journal в становлении отрасли ИБ?

— Думаю, одну из важных. Многие ИБ-шники ждут новые выпуски с нетерпением. Бывает, получишь свежий номер, откроешь, и видишь в нём статьи своих друзей. Радует за них. Не каждый журнал может похвастать, что в него пишут люди одного круга — знакомые, друзья, те, с кем можно поговорить на конференциях, вживую обсудить их публикации.

— Вспомните интересные эпизоды, ситуации, связанные лично для вас с BIS Journal?

— Помню, работая в Златкомбанке, прохожу мимо ресепшна и вдруг вижу, сидит наш курьер и с живейшим интересом читает BIS Journal. Других журналов рядом лежит много и разных. Но он читает именно этот. Спросил, почему? Ответ поразил: «Он очень хороший, остальные — красивые картинки и реклама. А тут все интересно. Жалко, редко выходит. Но первый читаю его я». И тогда я понял, что команда, создающая этот журнал — настоящие профи.

— Какие статьи или акции журнала вам запомнились?

— Наверное, те, которые писал сам или в соавторстве с коллегами. Могу сказать еще, что за все десять лет не было

ни одного номера, который я не прочел бы от корки до корки. И все сохранил на память.

— Как изменялся за эти десять лет ландшафт российской ИБ? И как изменился BIS Journal?

— Журнал все время развивается и продолжает удивлять. Появляются новые авторы, рубрики. Продолжением журнала можно назвать BIS TV, портал ib-bank.ru и многое другое.

— Какой вы видите отрасль ИБ через десять лет? И каким, на ваш взгляд, станет BIS Journal?

— Я не прорицатель, так далеко заглядывать не могу. Помнится, предложил организовать рубрику «Лайфхак». Она всем понравилась и тут же появилась в журнале. Придут новые идеи — воплотим в жизнь.

— Что, на ваш взгляд, нужно сделать сегодня, чтобы журнал стал ещё лучше, ещё интереснее для своих читателей?

— В кулуарах его называют «Красный журнал», и только немногие не понимают, что это BIS Journal. Если провести независимый опрос, какой журнал по ИБ поставить на первую строчку в ТОП-5, не сомневаюсь, что победа с большим перевесом будет за BIS Journal. Это заслуженно.

Михаил ОДУВАЛОВруководитель службы Управления
по обеспечению ИБ Банка ВТБ (ПАО)

«УЧАСТВОВАЛ В АКЦИИ ЖУРНАЛА В РОЛИ ТАЙНОГО ПОКУПАТЕЛЯ»

— Какую роль, на ваш взгляд, сыграл BIS Journal в становлении отрасли ИБ?

— Расширил и углубил понимание тематики и проблем, стоящих перед отраслью, познакомил с имеющимися на рынке решениями.

— Вспомните интересные эпизоды, ситуации, связанные лично для вас с BIS Journal?

— Акция «Тайный покупатель» в августе 2018 года, в которой я принял участие. Пришел «сдать биометрию» в офис банка ВТБ, и меня узнали по голосу. Узнала заместитель управляющего офиса, с которой я раньше говорил по телефону.

— Какие статьи или акции журнала вам запомнились?

— Было много интересного. Особенно хорошо запомнился исторический раздел.

— Как изменялся за эти десять лет ландшафт российской ИБ? И как изменился BIS Journal?

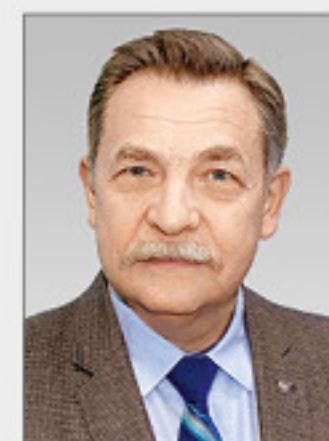
— Стал более выпуклым и ярким. И ландшафт и журнал. В хорошем смысле.

— Какой вы видите отрасль ИБ через десять лет? И каким, на ваш взгляд, станет BIS Journal?

— Это к Роману Вильфанду. Прогнозы — его конёк.

— Что, на ваш взгляд, нужно сделать сегодня, чтобы журнал стал ещё лучше, ещё интереснее для своих читателей?

— Продолжать работать! Творить, зажигать (в рамках разумного, конечно).

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

«MUST HAVE ДЛЯ КАЖДОГО БЕЗОПАСНИКА»

— Какую роль, на ваш взгляд, сыграл BIS Journal в становлении отрасли ИБ?

— Представьте себе переохлажденную воду! Принимает форму сосуда, в который налита, и своей формы не имеет, а только объем и аморфность. И вот в нее бросили маленькую песчинку, и она сразу начала кристаллизироваться в прочный красивый кристалл, который к тому же можно огранить и придать правильную форму.

Вода — это ИБ, BIS Journal — та самая песчинка, а редколлегия — гранильщики.

— Вспомните интересные эпизоды, ситуации, связанные лично для вас с BIS Journal?

— Журнал — Уральский форум — территория, где коллеги становятся друзьями. Это первая ассоциация. А вторая... была одна из первых статей, написанных мной и Сергеем Потаниным, когда мы неожиданно для себя получили огромное для нас количество самых разных откликов и мнений, и тогда возникло ощущение community, братства ИБ, что ли, и за это я благодарен журналу.

— Какие статьи или акции журнала вам запомнились?

— Статей было много, не буду выделять отдельные, но вот рубрика про историю криптографии, подкреплённая книгой, — очень сильное впечатление!

— Как изменялся за эти десять лет ландшафт российской ИБ? И как изменился BIS Journal?

— Ландшафт, наконец, появился, и стало немного понятнее, что такое ИБ. А журнал просто вырос из коротких штанишек во фрак и джинсы.

— Какой вы видите отрасль ИБ через десять лет? И каким, на ваш взгляд, станет BIS Journal?

— Про отрасль не знаю, гадать не буду, очень все быстро и непредсказуемо вертится, а журнал должен стать must have для каждого безопасника.

— Что, на ваш взгляд, нужно сделать сегодня, чтобы журнал стал ещё лучше, ещё интереснее для своих читателей?

— Держать темп, который набрали за последние пару лет, держать руку на пульсе отрасли.

ОТ РЕДАКЦИИ

- 2 10 лет BIS Journal**
Павел Былевский (BIS Journal)
Точно в десятку

НОВОСТИ

- 10 В мире, в России, криминал, технологии**

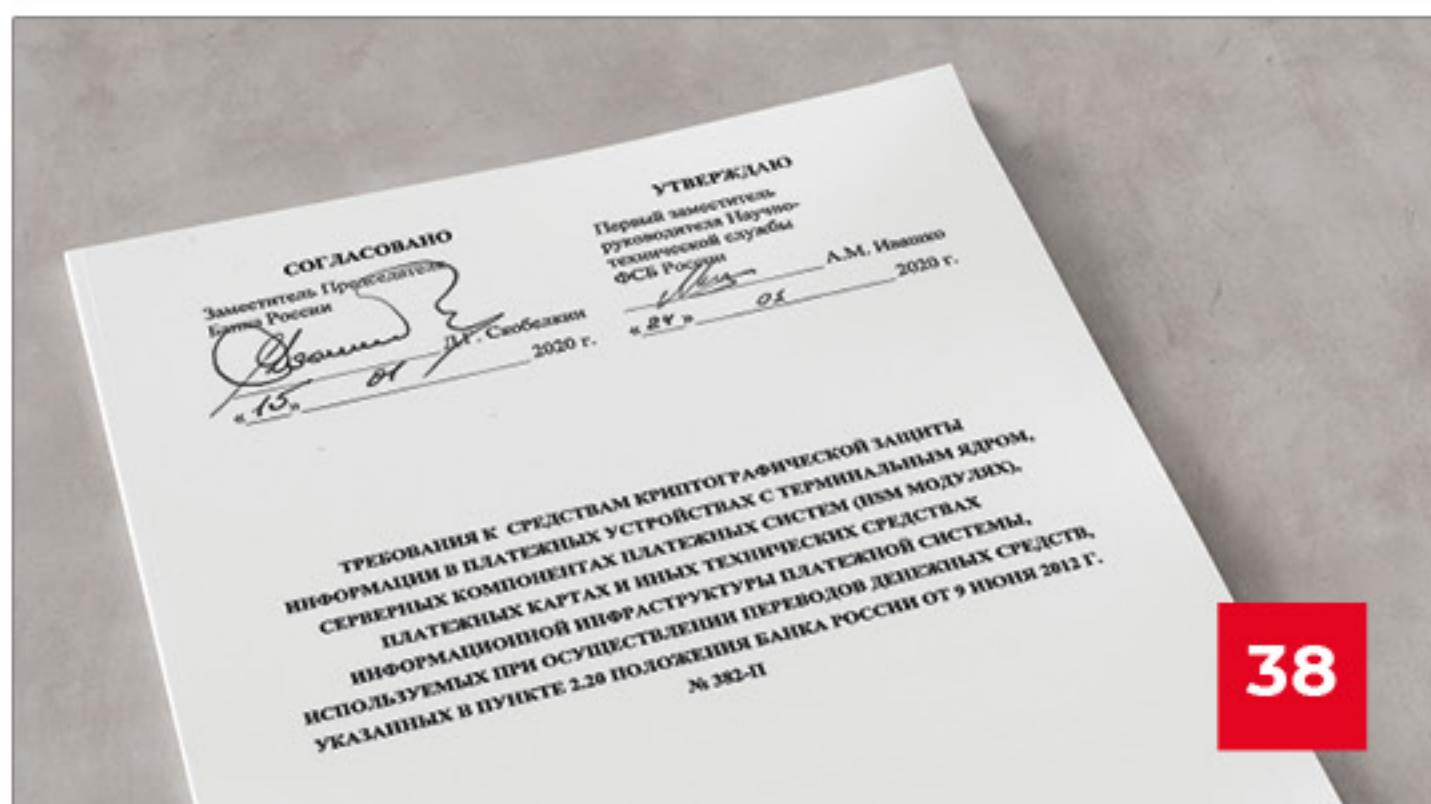
ТЕМА НОМЕРА

- 14 Смена парадигмы ИБ**
Андрей Курило (Реальная безопасность)
Как нам реорганизовать ИБ
- 21 Александр Баранов (НИУ ВШЭ)**
«Лучше решить одну очень важную задачу, чем не решить две...»
- 22 Рустэм Хайретдинов (InfoWatch)**
«Регулирование ужасно отстаёт от требований дня»
- 23 Марк Новоначный (BIS Journal)**
«Сегодня ведомства — единственная надежда»
- 25 Алексей Сабанов (Аладдин Р.Д.)**
Про опыт регулирования «снизу»
- 26 Олег Чутов (Информзащита)**
«Нельзя пугать, не требуя»
- 28 Владимир Иванов (Актив)**
«Застой идей, гонки за хайпом, размытые зоны ответственности»
- 29 Игорь Ляпунов (Ростелеком)**
«Через 2–3 года рынок ИБ кардинально изменится»



РЕГУЛЯТОРЫ

- 34 Законотворчество**
Анатолий Аксаков (Государственная дума РФ)
«Единое окно» для государства и граждан. Третий лишний
- 36 Нормативы**
Михаил Бухтин (Банк России)
Инциденты обойдутся банкам намного дороже
- 38 СКЗИ**
Анастасия Толстолуцкая, Андрей Елистратов, Валерий Никитенков (ТК 26)
В штатном режиме





50



52

БАНКИ

- 42 Лидеры мнений**
Сергей Пазизин (Банк ВТБ (ПАО))
Про детали и главное
- 48 Деликатная ситуация**
Тимур Аитов (ТПП РФ)
Записали в злоумышленники
- 50 Вредные советы**
Екатерина Рачкова (Калашникова)
(Банк ВТБ (ПАО))
И заведите клона...
- 52 Удалёнка**
Василий Окулесский (BIS Journal)
«Удалёнка» как кейс
- 54 Удалёнка**
Сергей Вихорев (ИТ-Экспертиза)
**«Меняйте ваши мнения, сохраняйте
ваши принципы; меняйте листья,
сохраняйте корни»**
- 55 Удалёнка**
Тимур Аитов (ТПП РФ)
Новый импульс или дезорганизация?
- 56 Открытый банкинг**
Татьяна Жаркова (Ассоциация ФинТех)
Игра в открытую. Выигрывают все!

УГРОЗЫ И РЕШЕНИЯ

- 60 Новые вызовы**
Александр Бодрик (Cyberlands B.V.)
Нашествие маленьких контейнеров
- 63 Уязвимости**
Вей Тай (Tenable),
Илья Осадчий (Тайгер Оптикс),
Никита Цыганков (ДиалогНаука)
Рейтинг особого назначения
- 66 Удалённый доступ**
Павел Луцик (КриптоПро)
Простые решения
- 68 Импортзамещение**
Корней Ревт (BIS Journal)
**Сделано в России, сертифицировано
ФСТЭК**



56

ИНФРАСТРУКТУРА

- 72 Событие**
Иван Меденников, Сергей Смирнов
(ГК ЦРТ)
Опять победа!
- 76 Социальные сети**
Валерия Мещерякова (студентка
факультета журналистики МГУ
им. М. В. Ломоносова)
Исследуем вирусы... агрессии

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 80 Обзор**
Дарья Савенкова (Сбербанк)
Телефонный развод
- 84 Осведомлённость**
Ольга Лимонова (Антифишинг)
Клиенты знают мало. Почему?
- 88 Инсайд**
Ольга Лимонова, Андрей Жаркевич
(Антифишинг)
«С кем мы имеем дело?»
- 93 Госструктуры**
Анна Катанкина (BIS Journal)
«Выбрось это старье!»



ОБРАЗОВАНИЕ И КАРЬЕРА

- 96 Обзор**
Марина Бродская (BIS Journal)
Триггер сработал
- 101 Взгляд**
Валерий Куликов (BIS Journal)
«...пока не потеряно всё»

СУБЪЕКТЫ

- 104 История**
Дмитрий Ларин (историк криптографии)
Криптографы СССР против самураев
- 108 История**
Борис Столпаков (историк криптографии)
«Он был образцовый начальник...»
- 114 Проекты**
Валерия Чапчаева
(Медиа Группа «Авангард»)
«Наша игра» на удалёнке

ШПИОНАЖ ПО КАБЕЛЮ

Комитет по оценке иностранного участия в секторе телекоммуникационных услуг Team Telecom рекомендовал Федеральной комиссии по связи отказать в прокладке подводной кабельной системы Pacific Light Cable Network (PLCN) по дну Тихого океана — из Лос-Анжелеса в Гонконг. Исходя из соображений национальной безопасности.

Team Telecom (состоящий из Минюста, Минобороны и Министерства внутренней безопасности США) опасается, что кабель позволит разведслужбам КНР получить доступ к американским данным.



ТРОЯНСКОГО КОНЯ — В КАЖДЫЙ ДОМ

Власти Германии предложили законопроект, предоставляющий спецслужбам страны право шпионить за гражданами с помощью троянов. Провайдеры будут обязаны устанавливать в своих ЦОДах правительственное оборудование, перенаправляющее информацию сначала правоохранителям, и только после в место назначения.

Блог Netpolitik сообщил, что пользователи не будут знать, что их личная переписка и даже обновления ПО передаются через прокси. Для заявленных целей предположительно будет использоваться софт FinFly ISP от компании FinFisher. В FinFisher говорят, что он способен легко внедрять трояны на целевые устройства уровня провайдеров. В документах, обнаруженных WikiLeaks, встречалась информация, что FinFly ISP обладает возможностями для проведения MitM-атак.

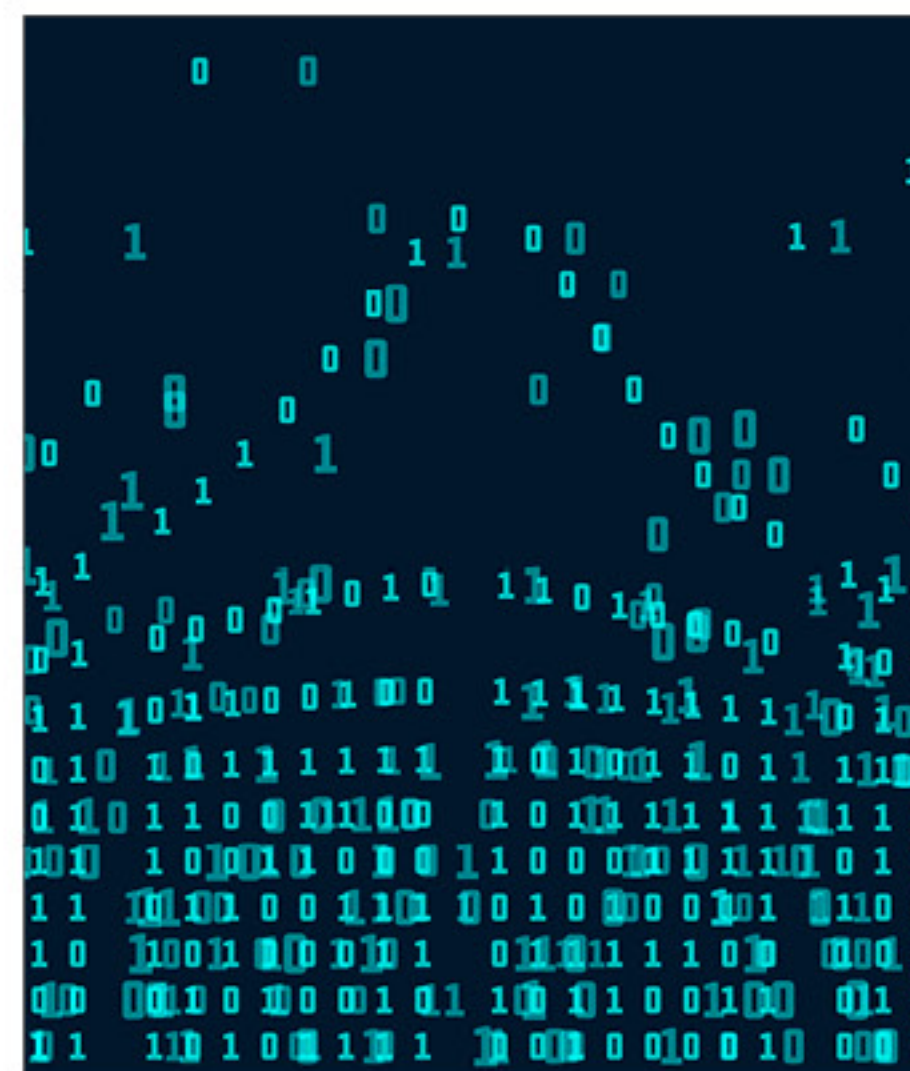
КОНЕЦ СКВОЗНОМУ ШИФРОВАНИЮ?

Конгресс США рассмотрит законопроект «О правомерном доступе к зашифрованным данным» (LAEDA), который может стать угрозой шифрованию как инструменту безопасности. Об этом сообщило «Общество интернета» (ISOC), занимающееся развитием и обеспечением доступности интернета.

По словам некоторых сенаторов США, документ должен защитить американские интересы в области нацбезопасности и положить конец технологиям шифрования, используемым террористами. LAEDA призван обязать сервис-провайдеров и производителей электроники содействовать правоохранителям в доступе к зашифрованным устройствам или данным при наличии судебного ордера.

Под письмом ISOC, адресованным авторам законопроекта, уже подписались порядка ста общественных организаций, техкомпаний, торговых

ассоциаций, а также ИБ-экспертов. В ISOC заявляют: LAEDA — конец сквозному шифрованию. Ведь для того, чтобы иметь возможность исполнять требование закона, компаниям придется либо встраивать в свои продукты бэкдоры, либо отказаться от этой механики.



ЦРУ СТАЛО КИБЕР-ОПАСНЫМ

В 2018 году Дональд Трамп подписал секретное распоряжение, предоставляющее расширенные полномочия ЦРУ для осуществления кибератак.

Бывшие сотрудники администрации президента утверждают, что это распоряжение позволило ЦРУ проводить собственные кибероперации, не дожидаясь одобрения Белого дома: «Указ Трампа был очень агрессивным и дал ведомству особые полномочия совершать наступательные действия в отношении ряда стран-противников».

Новые полномочия не были предназначены для взлома и хищения разведанных — они позволяли ведомству проводить наступательные операции с целью вызвать сбои в работе систем. Также были снижены требования к доказательствам, которые ограничивали способность ЦРУ проводить тайные кибероперации против медийных и благотворительных организаций, религиозных учреждений или предприятий, якобы работавших от имени разведслужб стран-противников.





ЕБС СТАНЕТ ГИС

Единую биометрическую систему (ЕБС) планируют наделить статусом государственной информационной системы (ГИС). Такой статус сейчас имеют Госуслуги и ЕСИА. На обсуждении вариант государственно-частного партнёрства. В этом случае права собственности на систему передаются государству, а оператор («Ростелеком») остаётся прежним.

На базе ЕБС будут оказываться государственные, муниципальные и коммерческие высокорисковые услуги, осуществляться доступ к персональным данным и совершаться юридически значимые действия. Кроме того, она может стать доверенной для

получения облачной квалифицированной электронной подписи, удалённого судопроизводства, дистанционного образования, услуг связи, нотариальных, финансовых и многих других сервисов.

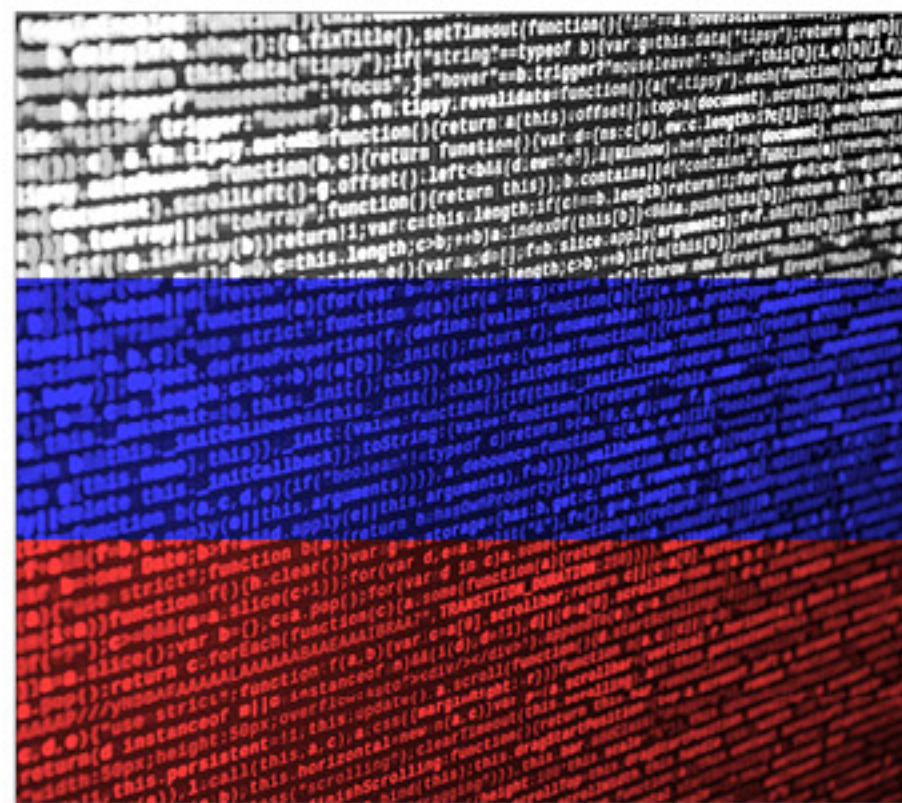
В «Ростелекоме» рассчитывают, что при новом статусе ЕБС скорость наполнения и количество регистраций заметно увеличатся. В свою очередь банки считают, что перевод системы в статус ГИС расширит возможности по наполнению базы за счёт использования государственных услуг и популяризирует биометрию среди граждан. В итоге биометрия получит широкое развитие.

БАНКИ ПРОТИВ СПЕШНОГО ИМПОРТОЗАМЕЩЕНИЯ

Ассоциация банков России направила письмо Михаилу Мишустину с просьбой отложить перевод на отечественное ПО объектов критической информационной инфраструктуры на четыре года. Замещение иностранного оборудования отечественным осложнено в связи с отсутствием у производителей последнего современных технологий производства радиоэлектроники и его элементно-компонентной базы, сказано в письме Ассоциации.

Банки утверждают: многие программы заменить просто нельзя — не будет ни мобильного, ни интернет-банкинга. По оценке АБР, для замещения всего «харда» и «софта» кредитным организациям разово придётся потратить более 700 млрд рублей. А средние сроки замещения с учётом непрерывности деятельности банков составят не менее трёх лет.

Кроме того, «авторское» ПО есть у многих крупных банков, но при этом его нет в реестре разрешённого для использования. Вероятно, что в условиях повсеместного снижения доходов финансирование замещения ПО и оборудования будет перенесено на потребителей услуг, что может выразиться в росте стоимости банковских продуктов и услуг.



НОВЫЙ КЛАССИФИКАТОР ПО

Минкомсвязи разработало новый классификатор российского софта, который будет использоваться в Едином реестре. Вносимые в структуру классификатора изменения оптимизированы для доработки реестров российского и евразийского ПО.

Кроме того, новая структура требуется для точного определения соответствия программного продукта, сведения о котором планируются для включения в реестры, классу ПО, а также для удобного поиска государственными и муниципальными заказчиками планируемых для закупки программных продуктов.

Проект нового классификатора включает 13 новых разделов, число новых классов в которых варьируется от трёх до 13. В числе новых классов есть средства разработки ПО на основе квантовых технологий, интегрированные платформы для создания приложений, системы управления содержимым (CMS), сайты и порталные решения.

РОССИЯ ВЗЯЛА «СЕРЕБРО»

США и Россия стали лидерами по числу утечек в 2019 году, говорится в исследовании InfoWatch.

В прошлом году в стране произошло 395 случаев утечки информации из компаний и госорганов. Это более 172 млн записей персональных данных и платёжной информации. По сравнению с 2018 годом число инцидентов выросло на 46%.

По этому параметру Россия седьмой год подряд занимает второе место после США. Чаще всего утекают персональные данные и платёжная информация россиян — 87,3% всех утечек. Половина этой цифры — всего один инцидент: ошибка в настройках сервера оператора фискальных данных «Дримкас». В 72,1% случаев виновными в утечке оказались рядовые сотрудники компаний, в 4,6% случаев — руководство, в 18,4% — киберпреступники.

«900» НЕ БЕЗОПАСЕН

Мошенники научились использовать сервисы Сбербанка по открытию счетов, чтобы отправлять SMS с официального номера банка — 900.

Они прибегают к помощи сервиса по дистанционному резервированию расчётного счета для ИП: зная телефонный номер, можно сделать так, что клиент Сбербанка в любой момент получит SMS с номера 900.

Мошенник связывается с клиентом Сбербанка, представляется безопасником, и пытается выудить данные карты. В случае отказа мошенник убеждает жертву, что «на самом деле» является сотрудником банка — предлагает направить клиенту SMS с номера 900 для открытия резервного счёта. Клиент действительно получает сообщение и код для подтверждения номера. Преступник же специально акцентирует внимание на том, что данный код ему не нужно сообщать, и таким образом ещё больше вводит жертву в заблуждение.

ПРИГОВОР КРИПТОВАЛЮТЕ В ПЕТЕРБУРГЕ

Петроградский районный суд Санкт-Петербурга исключил из обвинения «завладение криптовалютой». Речь о деле П. Пирона и Е. Пригожина, которые под угрозой пыток заставили жертву перечислить им 5 млн рублей, 99,7 биткоинов и другую криптовалюту на общую сумму 55 млн рублей.

В пресс-службе судов С.-Петербурга прокомментировали решение так: «Криптовалюта не является предметом преступления против собственности. В связи с отсутствием правового статуса признать её объектом гражданского права не представляется возможным. Данный вид виртуальных денег не подпадает ни под одну из категорий, не является признанным средством платежа на территории России, и отнесен законодателем к суррогатам денежных средств».

УКРАЛИ 232 МЛРД РУБЛЕЙ

232 млрд рублей украдено со счетов россиян в прошлом году. Об этом говорится в анализе состояния преступности в ежегодном докладе генпрокурора Совету Федерации.

В документе отмечено, что в РФ «продолжает увеличиваться удельный



вес преступлений в финансово-кредитной системе: если в 2018 году он составил 27,8%, то в 2019 году — 28,8%». «Растёт размер выявленного ущерба по таким преступлениям: в 2019 году — 232,1 млрд рублей (в 2018 году — 171,4 млрд рублей). Это, прежде всего, обусловлено ростом мошенничеств с использованием электронных средств платежа», — также сказано в докладе.

За последние пять лет в три раза выросли кражи, совершенные с использованием информационно-коммуникационных технологий — с 32,6 тыс. до 98,78 тыс. (их доля в общем числе таких преступлений увеличилась до 33,6%). Самыми частыми среди преступлений с применением информационных технологий остаются мошенничества — за пять лет их количество выросло с 90,6 тыс. до 119,9 тыс. за год (на 32,2%), однако, их удельный вес среди киберпреступлений снизился до 40,7%.

ОБЕЗВРЕЖЕНА ПРЕСТУПНАЯ ГРУППА

Правоохранители и эксперты Group-IB задержали в Москве организаторов преступной группы, перевыпускавшей SIM-карты и похитившей у клиентов банков десятки миллионов рублей.

Преступники взламывали учётные записи Instagram и мессенджеров, а также имейлы известных блогеров, бизнесменов и звёзд шоу-бизнеса, после чего требовали выкуп для восстановления доступа. Также нередко были случаи компрометации онлайн-банкинга и похищения денег с банковских счетов.

Мошенники планомерно «пробивали» людей в соцсетях. Получив данные жертвы и информацию о состоянии её банковского счёта, они задействовали сообщницу, которая изготавливала поддельную доверенность от имени клиента на возможность проведения операций с его SIM-картой. С этой доверенностью

она перевыпускала карту в салоне сотовой связи. У жертвы пропадала сотовая связь, а мошенница отправляла в банк пострадавшего запросы на получение одноразовых кодов доступа в привязанный к номеру телефона мобильный интернет-банкинг. Деньги со счетов жертв переводились на третьих лиц и обналичивались в других городах. Разовые суммы составляли 50–100 тыс. рублей.



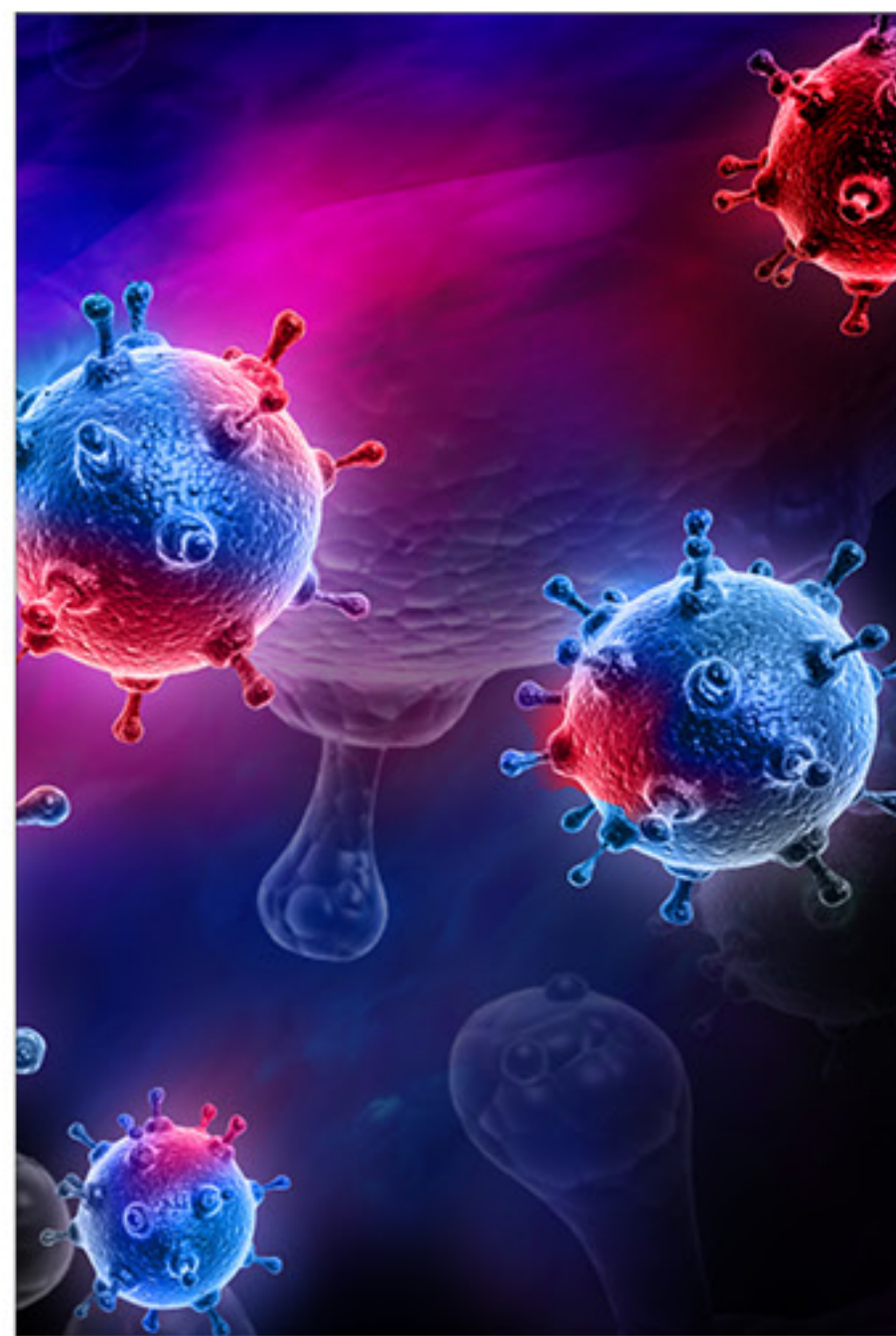
COVID ПОМЕСТИЛИ ПОД КОЛПАК

Минкомсвязь разработала регламент отслеживания контактов носителей коронавируса SARS-CoV-2 на основе геолокации и данных операторов связи. В Кремле отметили, что отслеживание такого рода не нарушает права граждан.

За основу будут браться данные Минздрава о номере телефона больного COVID-19. После этого специальные алгоритмы составят список тех людей, кто контактировал с ним посредством мобильной связи. Список же будет уточняться «с учётом данных о времени совместного нахождения абонентов и особенностей перемещения в течение наблюдаемого периода».

«В результате формируются списки номеров абонентов, которые были подвержены риску заражения COVID-19 в ходе непосредственного общения с заболевшим. Полученные данные централизуются на информационных ресурсах Минкомсвязи и

направляются в оперативные штабы субъектов РФ, Росгвардию, МВД и Минздрав», — говорится в документе ведомства.



ПЛАТЁЖ «ЛИЦОМ»

Бесконтактные платежи с использованием технологии распознавания лиц точно возможны при не очень больших суммах, — заявил зампред Совбеза РФ и председатель попечительского совета фонда «Сколково» Дмитрий Медведев.

Основатель компании «ВижнЛабс», которая занимается созданием ПО в области распознавания лиц и объектов, рассказал зампреду о новом решении, которое позволяет проводить транзакции бесконтактным способом — через идентификацию лица.

Разработчик также заверил, что сегодня вероятность ошибки составляет примерно один случай на 10 млн попыток, и добавил, что этот вопрос проработан с рядом инвесторов, в числе которых Сбербанк.

«Наверное, в тех случаях, когда платежи не являются очень объёмными по сумме, допустим, какие-то стандартные платежи, это точно возможно, — на бензоколонке или в метро... Я не разговаривал на эту тему со Сбербанком, но, видимо, здесь модель понятная», — заключил Медведев.

ОБУЧЕНИЕ В БОЮ

В Иллинойском университете предложили новый метод обучения глубоких нейронных сетей, снижающий число ошибок и повышающий надёжность в критических ситуациях. Он основан на сопоставлении нейронных сетей, ответственных за реконструкцию изображений, и сетей, генерирующих примеры состязательных атак, по типу GAN алгоритмов.

Через повторяющиеся циклы состязательная сеть попытается обмануть сеть, отвечающую за реконструкцию изображений — чтобы та генерировала элементы, не являющиеся частью оригинальных данных. Сеть реконструкции же будет модифицироваться с тем, чтобы не дать себя обмануть, таким образом повышая свою надёжность.

Хотя на этапе теста обученная сеть оказалась эффективной, она всё ещё требует доработки.

ЗАЩИТА ОТ МИНТРАНСА

По сообщению газеты «Известия», Минтранс планирует разработать единую систему мониторинга, фиксирующую онлайн возможные кибератаки и сбои в информационной инфраструктуре транспортного оборудования.

На создание системы до 2024 года может быть потрачено около 732 млн рублей. Тендер на разработку будет проведён этим летом.

В ведомстве рассказали: для транспортной сферы характерны потоки большого количества данных, которые необходимо быстро обрабатывать. Единая среда мониторинга защищённости (ЕСМЗ) будет собирать, обрабатывать и хранить информацию об управлении транспортной инфраструктуры. Она будет обнаруживать не только внешние попытки взлома, но также и возможные сбои в работе оборудования.

КАК НАМ РЕОРГАНИЗОВАТЬ ИБ

ОТРАСЛЬ НУЖДАЕТСЯ В ПОДХОДЕ
«НАПРАВЛЯТЬ, НЕ ВМЕШИВАЯСЬ»



СИСТЕМА УЮТНАЯ, НО РАБОТАЕТ ПЛОХО

К настоящему времени в России сложилась законодательно оформленная, нормативно обеспеченная, представленная системой подготовки кадров, печатными изданиями и рядом публичных мероприятий отрасль информационной безопасности.

Отрасль живёт своей жизнью, идут обсуждения наиболее важных вопросов, проходят вебинары, ведутся странички в соцсетях, работают целые блоги уважаемых экспертов, и многие высказывают мнение, что всё нормально, любое вмешательство в сложившуюся, как сейчас говорят, «экосистему» приведёт только к ухудшению ситуации.

Результаты, с одной стороны, вроде неплохие, а с другой — мы постоянно слышим и об утечках баз данных, и о компьютерных инцидентах, реализованных атаках, хищениях. Эксперты заявляют, что при целевой атаке даже низкого уровня сложности 93 % систем будут взломаны в первые полчаса, а число похищенных записей персональных данных исчисляется миллионами^{1,2}.

Ещё раз скажу о сохранности баз данных. В 90-е годы я просто собирал на свалках дискеты с базами данных ведомств СССР. Они были никому не нужны. Сейчас вроде дела обстоят иначе, но с завидной регулярностью мы узнаём о появлении на рынке новых и актуальных баз данных совершенно различного назначения. Не боюсь повториться, но украдено почти всё, кто бы что ни говорил и как бы ни оправдывался.

Таким образом, напрашивается неутешительный вывод: система работает плохо. При этом регулярно на протяжении многих лет раздаются голоса о необходимости усиления управления ею, очевидно, с целью повышения эффективности работы.

Можно ли найти разумное объяснение, сформулировать причины недовольства и предложить хотя бы варианты решения?

Вопрос непростой и, похоже, системный.

С УЧЁТОМ ОСОБЕННОСТЕЙ

Хочу обратить внимание на то, что информационная безопасность (в смысле задачи обеспечения безопасности информационных систем

и информационных ресурсов) наряду с информатизацией относится к категории обеспечивающих видов деятельности. В отличие от бизнес-направлений.

Работы по обеспечению информационной безопасности, как бы этого ни хотелось, не создают прибыль субъектам экономической деятельности, они только обеспечивают возможность её получения, снижая риски бизнеса, имиджевые издержки, финансовый ущерб, а также решают задачу защиты информации граждан и о гражданах, то есть защищают их права. В этом их цель. Поэтому, как ни крути, объективно выстраивается следующая иерархия видов интересующей нас деятельности: бизнес — информатизация — безопасность.

В этой иерархии и кроется много проблем ИБ, и, прежде всего, проблема недостаточной численности работников и формирования бюджета служб безопасности: из прибыли, по остаточному принципу, в размере от 5 до 20 % от расходов на информатизацию. А информатизация — ох, какая недешёвая, уступает только расходам на капитальное строительство, и, как известно, денег всегда не хватает.

Поэтому на финансирование деятельности в области ИБ, на её возможности и позиции существенным образом влияют обязательные требования, устанавливаемые регулятором, типа «должен быть МСЭ такого-то класса» или «по классификатору Вы относитесь к объектам КИИ». На это руководство субъектов защиты вынуждено реагировать, а требования выполнять.

С учётом таких особенностей и сложилась отрасль ИБ.

СЕКТОРЫ ОТРАСЛИ

Состав секторов отрасли весьма неоднороден. К ним относятся:

1. Государственные и отраслевые регуляторы (ФСТЭК, ФСБ, Минкомсвязь, Роскомнадзор, ЦБ РФ, а теперь и Сбербанк как центр компетенции проекта «Информационная безопасность» федеральной программы «Цифровая экономика», опосредованно Минэк и Минюст, существенно влияющие на содержание принимаемых НПА). Как раз почти «семьяnek».

В соответствии со ст. 16 ч. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» государственное регулирование отношений в сфере защиты информации осуществляется путём установления требований о защите информации, а также ответственности



Андрей КУРИЛО

кандидат технических наук, доцент, лауреат Премии Правительства РФ в области информатизации

¹ <https://www.securitylab.ru/news/508630.php> «Всего полчаса понадобится хакеру для проникновения в локальную сеть компании».

² Аналитический отчёт Infowath «Исследование структуры утечек персональных данных: мир и Россия, 2019 год», 28 мая 2020 года.

за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

В соответствии с федеральным законодательством мы имеем семь субъектов госрегулирования (регуляторов), в соответствии с законом и в пределах своей компетенции устанавливающих требования по безопасности, и ответственность за нарушение закона, которая в настоящее время зафиксирована в четырёх статьях КОАП РФ в части:

- ♦ нарушения лицензионных требований или деятельности без лицензий;
- ♦ использования не сертифицированных систем защиты;
- ♦ нарушения установленных требований по безопасности;
- ♦ разглашения информации ограниченного доступа;
- ♦ нарушения правил обработки и использования персональных данных.

В УК РФ есть ещё статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», однако она составлена таким образом, что фактически не несёт никакой угрозы владельцам объектов КИИ за невыполнение требований ФЗ № 187-ФЗ и не оправдывает возлагавшихся на неё надежд в части принуждения владельцев систем к выполнению этого закона.

Таким образом, в сложившейся на сегодня конструкции органы регулирования выстроены горизонтально, без вертикальной иерархии, что в принципе отвечает задачам регулирования, но не отвечает задачам управления.

Отмечу, что в финансовой сфере по факту возникает два регулятора, один из которых является регулятором отрасли, а второй — центром компетенции по информационной безопасности с определёнными финансовыми возможностями. При этом рамки проекта «Информационная безопасность» далеко не ограничены финансовой сферой, что создаёт, как сейчас говорят, «когнитивный диссонанс».

2. Службы информационной безопасности, так или иначе представленные в субъектах

экономической деятельности и органах федерального, регионального и муниципального управления. В зависимости от размеров субъектов эти службы могут представлять собой либо нормативно и законодательно обеспеченные иерархически выстроенные структуры с собственными органами управления, либо просто обособленные подразделения. Некоторые обладают собственным бюджетом.

3. Вендоры.

4. Системные интеграторы (внедрение продуктов и услуг и построение систем информационной безопасности).

5. Консалтинговые структуры.

6. Аутсорсеры.

7. Аудиторы.

8. Учебные заведения.

9. Медиафирмы, работающие в области ИБ.

РЫНОК ПРОДУКТОВ И УСЛУГ

Службы информационной безопасности, вендоры, системные интеграторы и некоторые другие создают рынок продуктов и услуг информационной безопасности, ёмкость которого напрямую зависит от:

- ♦ наличия механизмов принуждения к выполнению требований закона и регуляторов, которых, как мы убедились, недостаточно, чтобы серьёзно влиять на ход работ по обеспечению информационной безопасности на местах;
- ♦ потребностей и возможностей субъектов экономической деятельности в решении задач ИБ и их соответствия требованиям законодательства;
- ♦ открывающихся новых направлений деятельности государства (цифровизация) и бизнеса (например, биометрическая идентификация);
- ♦ поддержки государства.

Размер рынка, по экспертным оценкам, составил в 2019 году 67 млрд руб., из них 70% средств пришлось на поставки оборудования и ПО. Рынок явно небольшой, поэтому вендорам, за исключением единиц компаний, фактически заходящих на новые сегменты рынка, невыгодно заниматься новыми разработками. Они не окупаются, особенно разработка ПО, так как она стоит недорого, но при этом требует серьёзных финансовых вложений. Это не стимулирует. Исходя из складывающихся реалий, наиболее приближённые и раскрученные фирмы гонятся за крупными заказами, типа биометрической аутентификации в метро, разработки систем цифровых пропусков и т.д. Но это единичные, хотя и крупные заказы, они не развивают рынок, а скорее наоборот.

Органы регулирования выстроены горизонтально, без вертикальной иерархии, что в принципе отвечает задачам регулирования, но не отвечает задачам управления

Анализ статистических отчётов Росстата показывает, что пик информатизации (финансирования работ) пришёлся на период 2000–2010 гг. Сейчас наступила стадия насыщения субъектов средствами информатизации и информационной безопасности. Фактически наблюдается только перманентная замена оборудования и ПО после истечения срока амортизации и реализация некоторых дополнительных новых сервисов. Больших проектов очень мало.

В результате рынок сжимается.

КАК УПРАВЛЯТЬ, НЕ ЗНАЯ ЧЕМ?

К большому сожалению, в связи со сложившейся практикой управления только через установление требований о защите информации и слабого принуждения к их выполнению статистический учёт рынка продуктов и услуг в области ИБ в стране вообще не ведётся; в мониторинг, проводимый Роскомстатом, экономические показатели рынка ИБ не включены; в официальной статистической информации, публикуемой этим уважаемым органом, упоминаний об отрасли ИБ нет.

Это означает, что государство, устами разных людей говорящее по всем медиаканалам о проблеме информационной безопасности, киберпреступности, хищениях с банковских карт, биометрической аутентификации, импортозамещении, цифровом концлагере и т.д. как официальное направление работ отрасль ИБ не видит, оставляя её в статусе некой инициативной деятельности.

Как же можно управлять, не зная чем? И как отзовутся управляющие действия на практике?

Может быть, поэтому, может быть, нет, но преференции и льготы для рынка продуктов и услуг информационной безопасности практически никогда государством не устанавливались.

В этих условиях рынок продолжает регулироваться соответствующим общим законодательством, изъяны которого видны уже невооружённым глазом, что снова наглядно показали события, связанные с преодолением последствий пандемии.

ПРО ЛИЦЕНЗИРОВАНИЕ

Есть ещё вопрос о механизме лицензирования деятельности в сфере защиты информации. Он задумывался как способ отсека от этого вида деятельности недобросовестных субъектов. Насколько эффективно решена эта задача? На примере Минкомсвязи, в части лицензирования деятельности УЦ, видим, что не решена. На примере ФСТЭК и ФСБ видим, что лицензии получили все, кто хотел: и большие фирмы,

Рынок продолжает регулироваться соответствующим общим законодательством, изъяны которого видны уже невооружённым глазом

и маленькие, и российские «дочки» мировых трансконтинентальных корпораций. Влияет ли этот механизм на качество работ, да ещё и при огромной текучке кадров, — похоже, что нет. Вопрос требует проработки, но простое решение в современном духе типа «Ужесточить требования!» может просто-напросто разрушить рынок.

Что же мы видим в результате?

Происходит заход на рынок поставок крупных непрофильных организаций, имеющих лицензии на осуществление деятельности в области защиты информации (например, предприятия гидроэнергетики). Конкурсы выигрываются легко, и средства с сегмента поставок, по некоторым оценкам до 70 % от всего объёма, уходят к ним. Результат — схлопывание рынка для СИ.

ПРОБЛЕМЫ РЫНКА

Средства, которые вроде как выделяются государством, имеют своего адресного получателя — соответствующие центры компетенции с узким кругом фирм вокруг них. Это ведёт к монополизации и уничтожает конкуренцию.

Далее. Практически стало правилом, когда при заключении договоров исключается этап авансирования работ, а расчёт осуществляется по факту завершения работы. К чему это привело? У подрядчика, как правило, не хватает оборотных средств. Если сроки затягиваются, а это бывает часто, дефицит средств загоняет фирмы в очень сложное положение, возникают проблемы с кредиторами и налоговой.

Содержать дорогих квалифицированных специалистов сложно. Следствие — массовое сокращение и перетекание специалистов в благополучные фирмы, что просто убивает конкуренцию, создаёт монополизм и крайне негативно сказывается на качестве выполняемых работ и поддержке уже поставленных заказчику продуктов. Фирмы начинают «сжиматься», причём процесс этот носит массовый характер.

Добавим сюда и низкую ответственность заказчиков, так как в этой ситуации над ними «не каплет». Добавим массовое неисполнение планов финансирования, позднее заключение договоров. В результате рынок сжимается, особенно по результатам 2019 года, средства не попадают

Позволю себе высказать крамольную мысль. Регулирование такого маленького рынка рыночными механизмами неэффективно. Или: чем меньше рынок, тем более он нуждается в госрегулировании

к СИ, это ещё больше ухудшает их положение. Возникают проблемы с налоговой инспекцией и кредитованием под уже ведущиеся работы.

Вообще, позволю себе высказать крамольную мысль. Регулирование такого маленького рынка рыночными механизмами неэффективно. Или: чем меньше рынок, тем более он нуждается в госрегулировании.

ПРО СРЕДСТВА ЗАЩИТЫ

Что касается средств защиты, то на рынке есть достаточное количество отечественных средств, хотя можно выделить две проблемы:

- ♦ недостаточная производительность для обработки больших потоков данных;
- ♦ запаздывание реализации новых функций, что отчасти связано с запаздыванием включения соответствующих требований в нормативные документы регуляторов.

В результате отрасль не развивается, а наоборот, сжимается. Если мы этого хотим, то всё нормально. Но хотим мы ЭТОГО или всё-таки заинтересованы в развитии и движении вперёд? На этот вопрос нужно ясно ответить самим себе.

Что-то мне представляется, что десяток оставшихся крупных корпораций и фирм не решат задачу.

ПРО ПУБЛИЧНЫЕ ОПОРЫ

В отрасли практически свернулся механизм публичной опоры на общественников: заинтересованных экспертов и специалистов. Формальный процесс публикации проектов НПА на сайте разработчика или Минюста — плохой эрзац общественных слушаний или экспертных обсуждений. Популярные сейчас онлайн-конференции, проводимые фирмами, — это всё-таки в первую очередь реклама продуктов.

ПРО СЛУЖБЫ ИБ

Теперь о собственно службах (подразделениях) информационной безопасности.

Эта практически единственная структура, на которой лежит вся ответственность за обеспечение ИБ в организации, а опосредованно — и в стране в целом. Причём ответственность

прямая, самая жёсткая, перед высшим руководством (собственником). По сравнению с этим все остальные меры ответственности вторичны.

В целом эти структуры достаточно автономны в своих действиях и нуждаются в основном в научно-технической и вендорской поддержке для того, чтобы не утратить достигнутый уровень безопасности и своевременно реагировать на новые вызовы. Их трудности: зарегулированность, большой объём задач и требований, наличие несвойственных задач, непростые внутренние взаимоотношения с другими подразделениями, недостаток новых, удобных с точки зрения использования в бизнес-проектах сертифицированных средств и решений по безопасности. Недостаточное финансирование, конечно.

Результатом деятельности службы ИБ является достижение и постоянное поддержание состояния защищённости контролируемого объекта и его информационной инфраструктуры. Состояние защищённости означает, что настройки оборудования и средств (систем) безопасности и регламенты деятельности персонала, а также клиентов выполнены в соответствии с эксплуатационной документацией, соответствующими регламентами и требованиями регуляторов и эффективно контролируются. Это также означает, что выполнение на объекте всех перечисленных требований, правил и регламентов позволяет считать объект защищённым, а уровень его информационной безопасности можно измерить и оценить³. Однако отмечу, что подавляющее число нашумевших случаев нарушений ИБ возникли не в результате воздействия новых, неизведанных угроз, а в результате эксплуатации злоумышленником ошибок и слабостей, выявленных им либо в настройках средств защиты и вычислительного или телекоммуникационного оборудования, либо в результате отсутствия регламентов деятельности персонала, либо грубых нарушений принципов безопасной эксплуатации систем, в первую очередь системными администраторами и разработчиками.

Отмечу также, что уровень информационной безопасности любого объекта можно измерить только косвенно, например, через оценку соответствия выполнения требований по безопасности. Подобный подход реализован

³ Следует оговориться, что защита будет обеспечена только от тех атак и угроз, которые были учтены политикой безопасности при проектировании системы защиты. Перед новыми угрозами объект, как правило, незащищён.



на основании стандартов ISO Банком России в ГОСТ Р 57580.2–2018 «Методика оценки соответствия».

ЛУЧШИЙ ПОКАЗАТЕЛЬ

Тем не менее лучший показатель работы службы ИБ — отсутствие нарушений и инцидентов, что позволяет в этом случае полностью использовать ИБ как фактор снижения рисков бизнеса.

Показателями качества работы в этом случае служат:

1. Высокий уровень доступности сервисов;
2. Результат оценки соответствия требованиям по информационной безопасности;
3. Отсутствие (наличие) инцидентов информационной безопасности в организации.

Собственно, этими самыми общими показателями можно измерять уровень ИБ в стране в целом. Предпосылки и опыт для создания нормальной и эффективной системы мониторинга уровня ИБ в стране есть. Так, ЦБ РФ к настоящему времени отладил и запустил достаточно эффективную систему сбора отчетности, пройдя этап роста в течение почти 10 лет. Запускается система сбора информации и реагирования по линии НКЦКИ ФСБ. Но это пока, к сожалению, частные решения. А чем мы пытаемся измерять уровень ИБ в стране? Средним

А чем мы пытаемся измерять уровень ИБ в стране? Средним временем простоя государственной информационной системы в результате компьютерной атаки?

временем простоя государственной информационной системы в результате компьютерной атаки, как это делается в упомянутом федеральном проекте?

ДЕСЯТЬ ПРОБЛЕМ ОТРАСЛИ

Вот в целом и обозначились проблемы отрасли. Это:

1. Отсутствие опережающих исследований, позволяющих определить и своевременно сформулировать и откорректировать главные цели, задачи и приоритеты развития отрасли ИБ на отдалённую (3, 5, 10 лет) перспективу с учётом тенденций развития кибероружия, компьютерной преступности, развития нашего общества. Также необходимо определить приоритеты работы государственных регуляторов.

2. Отсутствие сформулированных на национальном уровне целей, задач и показателей

Вопрос создания Министерства (кибер) безопасности, по аналогии с США, отпадает, так как оно в наших условиях, находясь в составе Правительства, не сможет эффективно взаимодействовать с силовым блоком и ЦБ РФ

их достижения в области информационной безопасности.

3. Отсутствие какой-либо статистической информации, позволяющей внятно описать состояние отрасли информационной безопасности и её сегментов.

4. Отсутствие налаженной системы сбора и достоверной публичной отчётности об уровне информационной безопасности и инцидентах в целом по стране, по основным отраслям экономической деятельности и субъектам Федерации.

5. Зарегулированность.

6. Отставание появления на рынке сертифицированных средств и систем защиты, удобных для встраивания в бизнес-процессы и приложения.

7. Отсутствие публичных механизмов взаимодействия сообщества безопасности и госрегуляторов. Неэффективность действующих механизмов.

8. Отсутствие регулирования определённых экономических функций:

- ♦ стимуляция экономического роста и развития отрасли путём целенаправленного воздействия на экономическую деятельность субъектов рынка через систему таких экономических регуляторов, как государственный бюджет, налоги, различные льготы при налогообложении доходов, кредиты, цены, заработная плата и т.д.;

- ♦ защита конкуренции и контроль соблюдения антимонопольного законодательства, обеспечение более благоприятных для бизнеса, особенно субъектов МСП, правил и условий конкурсных торгов.

9. Проблема импортозамещения.

10. Низкое качество подготовки кадров для отрасли.

Все перечисленные проблемы могут быть решены только централизованно, так как затрагивают всех без исключения субъектов отрасли. Очевидно также, что предусмотренные законом методы управления в этом контексте являются недостаточными и реализованы быть не могут.

Кстати, ведущие экономисты и аналитики обращают внимание на тот факт, что рыночный механизм, в соответствии с которым были

выстроены принципы управления экономикой (включая ИБ, в соответствии с ФЗ № 149-ФЗ), самостоятельно уже не может противостоять таким негативным явлениям макроэкономического уровня, как затяжной спад производства, высокий уровень долгосрочной инфляции, поляризация населения и субъектов экономической деятельности по уровню доходов, монополизация, схлопывание рынка и др. Эти негативные явления могут быть компенсированы только через специальный государственный механизм.

Это в полной мере относится и к тематике информационной безопасности.

ЧТО ДЕЛАТЬ?

А теперь реалии.

Вопрос носит системный характер, поэтому простых и лёгких решений нет.

Вмешиваться в работу госрегуляторов и навешивать на них дополнительные несвойственные функции нецелесообразно, они выполняют свои задачи в рамках полномочий, установленных законом.

Ряд регуляторов входит в структуру правительства, ряд находится под управлением Президента РФ. Таким образом, вопрос создания Министерства (кибер)безопасности, по аналогии с США, отпадает, так как оно в наших условиях, находясь в составе Правительства, не сможет эффективно взаимодействовать с силовым блоком и ЦБ РФ. Да и набор задач не тянет на статус министерства. Речь должна идти скорее о централизованном управлении и координации деятельности уже имеющихся структур.

Совет безопасности РФ? Это сильный совещательный орган, а его аппарат выполняет большую, часто не наблюдаемую общественностью работу, но в основном он готовит решения Председателя (Президента РФ) по важнейшим вопросам безопасности Российской Федерации и плохо подходит для задачи управления разнообразными субъектами отрасли ИБ.

Что остаётся? Федеральная программа? Уже есть, вместе с центром компетенции её дорабатывали без участия госрегуляторов, при очень низкой явке заинтересованных экспертов, кстати. Посмотрим, конечно, но есть опасения, что она не даст требуемых результатов. Но что положительного в этой программе, так это то, что она обеспечена финансированием.

Идея хорошая, однако представляется, что центр компетенции при Президенте РФ, располагающий финансовыми (достаточно небольшими) и внятыми административными

ресурсами в виде компактного агентства, бюро или комитета с привлечением известных на рынке опытных специалистов не только в области ИБ, но и экономики и права, был бы хорошим решением, способным сформулировать стратегические цели, провести необходимые исследования и поисковые работы, поставить задачи многим ведомствам, включая Минэк, и добиться результата, которого мы хотим, не вмешиваясь непосредственно в оперативную деятельность субъектов отрасли.

Были в истории нашего народа прецеденты?

Конечно. Вспомним:

- ◆ Специальный комитет при СМ СССР (атомный проект);
- ◆ Совет по радиолокации при ГКО;
- ◆ Научный совет по комплексной проблеме «Кибернетика» при президиуме АН СССР;
- ◆ Государственный комитет по вычислительной технике и информатике;
- ◆ Государственная техническая комиссия СССР, наконец. И многое другое.

Было нужно — делали. Надеюсь, и сейчас сделаем, если действительно нужно.

BIS-КОММЕНТАРИЙ

«ЛУЧШЕ РЕШИТЬ ОДНУ ОЧЕНЬ ВАЖНУЮ ЗАДАЧУ, ЧЕМ НЕ РЕШИТЬ ДВЕ...»

Основные тезисы статьи уважаемого Андрея Петровича поддерживаю и хочу сделать некоторые добавления в части предложений конструктивного характера. Направлений импортозамещения в IT-сфере действительно много, и все они выглядят достаточно актуально. Тем не менее следует сформировать главную, первоочередную задачу. Поэтому вношу предложения, которые кратко попытаюсь обосновать.

На мой взгляд, основной проблемой информационной безопасности IT-сферы сейчас стала возможность разрушения стабильной работы Интернета в России, вплоть до полного отключения российского сегмента. В современных условиях остановка сети Интернет в той или иной стране и теперь в России приведёт к экономическому, политическому и психологическому коллапсу, т.е. к полной дестабилизации общественно-экономической системы России. Я даже не буду полностью обосновывать этот тезис и сошлюсь только на отключение сотовой связи в случае остановки телекоммуникационной основы Интернета.

Разрушение Ethernet-основы телекома в одной России многим представляется невозможной задачей. Однако это не так. В любом коммуникационном или каналобразующем устройстве современного телекома на первом уровне (физическом) модели ISO стоит микросхема, преобразующая физический сигнал в логический с очень большой скоростью и реализующая код с исправлением ошибки Рида — Соломона. Эти микросхемы называют ASIC. Если в программе ASIC присутствует ошибка или закладка, позволяющая

перевести её в нерабочее состояние, то этот канал отключается. Шифрование на уровнях выше первого не спасает, а на первом уровне его применяют редко, поскольку требуется много шифраторов с большой скоростью работы.

Выход — в налаживании производства указанных ASIC или сертификации их на НДВ. Это позволит вынести защиту Интернета на более высокие уровни модели ISO, что уже с определённым успехом делается сейчас.

Конечно, за физическим уровнем следует необходимость разработки и производства отечественной, сертифицированной по ИБ телекоммуникационной платформы. Особенность такого подхода в том, что он позволит создавать локальные и устойчивые к отключению извне районы с их дальнейшим разрастанием и стыковкой, т.е. решать задачи поэтапно. Развёртывание производства отечественных микросхем, конечно, требует денег, но денег гораздо меньших, чем запланировано на развитие «журавлей в небе» в виде квантового компьютера. Если, не дай бог, встанет Интернет, квантовый компьютер не будет нужен никому. Об организационно-законодательных проблемах импортозамещения, в том числе в области телекоммуникационной платформы, в статье А. П. Курило правильно сказано довольно много.

Мне представляется, лучше решить одну очень важную задачу, чем не решить две просто важных.



Александр БАРАНОВ
заведующий
кафедрой ИБ НИУ
ВШЭ, академик
Академии
криптографии РФ



Рустэм ХАЙРЕТДИНОВ
вице-президент
группы компаний
InfoWatch,
генеральный
директор ООО «Атак
Киллер» (Attack Killer)

«РЕГУЛИРОВАНИЕ УЖАСНО ОТСТАЁТ ОТ ТРЕБОВАНИЙ ДНЯ»

НАДО СМОТРЕТЬ НА ИБ ПО-ДРУГОМУ

Информационная безопасность, как и многие другие отрасли, сегодня находится в процессе трансформации. На неё воздействуют несколько векторов:

- ◆ цифровизация, выставляющая новые требования не только к собственно защите, но и к эффективности, адаптивности, управляемости и прозрачности функций безопасности;
- ◆ обострение международной обстановки, выливающееся в антиглобализацию и приравнивание кибероружия к обычному оружию;
- ◆ отставание регулирования от реальных угроз ввиду инерционности законотворческой машины и несоответствия интернационального характера угроз национальным попыткам их нивелировать.

Взаимодействие этих трендов порождает порой противоречивые требования к системам безопасности. Так, национальные интересы требуют проверки систем защиты информации на предмет соответствия государственным требованиям, что, в свою очередь, требует фиксации кода приложения. При нынешней производительности сертификационных лабораторий сертификация может растянуться на год и больше, что означает, что функциональность сертифицированных систем отстаёт от функций несертифицированных решений более чем на год, то есть их использование уменьшает защищённость цифровых систем.

Отсюда же проистекает раздельное проектирование цифровых систем и средств их защиты — сначала проектируется и разрабатывается цифровой бизнес-процесс, и только потом вызывают безопасников исследовать его защищённость и защитить. Такой подход ведёт к проблемам на стыке ИТ и ИБ и вызывает негативный пользовательский опыт.

Примеров противоречивых требований ещё много, но их наличие объективно — бизнес стремится пользоваться открывающимися возможностями цифровизации, игнорируя риски, государство защищает свой суверенитет и права граждан, законы всегда отстают от технологического прогресса. Состояние ИБ в государстве динамично и зависит от того, какой тренд берёт верх. Поэтому, какой бы ни была

государственная модель безопасности, она будет вынужденно меняться, подстраиваясь под быстро меняющийся ландшафт возможностей и угроз. Важно при этом поддерживать обратную связь и обеспечивать диалог экспертного сообщества, то есть практиков, ежедневно отражающих атаки, и чиновников, отвечающих за регулирование.

Бизнес, с одной стороны, умеет работать в любом ландшафте, если правила не меняются или меняются предсказуемо. С другой стороны, мы всегда видим, что можно улучшить. Что же?

◆ На наш взгляд, регулирование сегодня ужасно отстаёт от требований дня. Расследование киберпреступлений натывается на то, что они не считаются «настоящими преступлениями», преступники скрываются от наказания, совершая преступления из других юрисдикций, вспомните хотя бы многократные «минирования» российских организаций.

◆ Сертификация в существующем виде также изжила себя и не отвечает требованиям времени, в котором изменения в информационные системы вносятся практически ежедневно. Не секрет, что это вынуждает компании иметь два разных ИБ-решения: одно для аттестации, другое — для работы с актуальными угрозами. Это приводит, с одной стороны, к профанации самой идеи сертификации, с другой — к дополнительным расходам эксплуататоров информационных систем.

◆ Уже несвоевременно рассматривать ИБ как отдельную часть цифровой экономики (она даже выделена в отдельный раздел Национальной программы). На самом деле ИБ — это функция любого направления ЦЭ. Разве можно построить без ИБ такие направления, как государственное управление или информационную инфраструктуру, телемедицину или цифровые системы транспортной отрасли? Для бесшовного внедрения безопасности в цифру надо перестать рассматривать ИБ как отдельную индустрию с отдельными продуктами, надо смотреть на цифровые системы в целом и на ИБ как на их функцию, а не продукт.

«СЕГОДНЯ ВЕДОМСТВА — ЕДИНСТВЕННАЯ НАДЕЖДА»

Марк
НОВОДАЧНЫЙ
читатель
BIS Journal

КОММЕНТАРИИ К КОММЕНТАРИЮ КАРЛА СУММАНЕНА¹

ПРО ЕДИНЫЙ ИНСТИТУТ

Цитата. «...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».

Комментарий. Наличие «единого института, ответственного за ...» не является «первичной проблемой». Наличие в стране министерства, ответственного за развитие здравоохранения, министерства, ответственного за образование, министерства, ответственного за культуру, не привело к успехам в соответствующих сферах.

ПРО КАДРОВУЮ ПОЛИТИКУ

Цитаты. «Сегодня развитие системы ИБ в России происходит на основе «ведомственной» модели управления, ... 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».

«...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».

«...в отсутствие системного процесса проектирования системы ИБ его место занимает какой-нибудь суррогатный. В нашей стране роль такого суррогатного процесса играет

законодательный. ...Проблема в том, что при таком подходе конечные содержательные решения в сложной предметной области уполномочены принимать не профессионалы, 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».

Комментарий. Неожиданно, что автор противопоставляет «профессионалов» и «специалистов широкого профиля». Поневолле сразу вспоминается Козьма Прутков с его сравнением специалиста «узкого профиля» с таким болезненным явлением, как флюс. А если от литературы перейти к логике, то она в размышлениях автора напоминает попытку сравнения круглого с мягким, хотя проблема, к сожалению, далеко не в этом.

В настоящий момент развитие элементов системы ИБ в рамках «ведомственной модели» можно почтить за благо, когда механизмы управления из единого центра, очевидно, не работают.

«Ведомственная модель» позволила хотя бы создать центры компетенции, опыт которых может быть передан в тот идеальный «единый центр», который (опять же в идеале) не будет

Наличие в стране министерства, ответственного за развитие здравоохранения, министерства, ответственного за образование, министерства, ответственного за культуру, не привело к успехам в соответствующих сферах

¹ «Главная проблема — отсутствие в стране единого института, ответственного за развитие системы ИБ в целом», Карл Сумманен, BIS Journal № 2/2020.

Проблемы с целеполаганием и стратегией у нас возникают в связи с фактическим бездействием 172-ФЗ о стратегическом планировании

укомплектовываться по модной ныне модели «отрицательного» кадрового отбора. Такой отбор ведётся (не в идеале, а в реале) не по уровню профессионализма (широкого или узкого профиля), а по принципам личной преданности и/или семейственности/клановости, замешанных на желании управлять сиюминутными денежными потоками в интересах своих кланов/семей, а не решать стратегические задачи в национальных интересах. Негативные примеры можно найти в самых разных областях от авиации до микро- и радиоэлектроники.

И ИБ, как подраздел в первую очередь ИКТ, не представляет собой исключения. Вопреки здравому инженерному смыслу, но с пользой для групп влияния растащено по разным ведомствам управление развитием аппаратных и программных технологий и оборудования, вопросы стандартизации и сертификации.

При этом формальное объединение этих «центров» под единой крышей не приведёт к успеху без изменения кадровой политики.

ПРО ЦИФРОВИЗАЦИЮ И ЭКОНОМИКУ

Цитата. «Особенность ситуации сегодня в том, что экономика России, так же 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».

Комментарий. Возможно, автор искренне заблуждается, утверждая, что суть переходного состояния экономики в цифровизации. Но уже приведена масса аргументов в пользу того, что корень дестабилизации современной экономики — в её финансово-спекулятивной природе. И «цифровизация» — это последнее прибежище апологетов такой природы экономики — от «высокочастотных» ИТ-инструментов финансовых спекуляций до разнообразных «услужливых» посреднических бизнесов, выгоды которых для их владельцев в снижении транзакционных издержек предоставления безответственных услуг, не требующих зачастую использования

собственной материальной инфраструктуры и основанной на потогонной эксплуатации неквалифицированных человеко-роботов.

Да, такими бизнесами востребованы современные ИТ-технологии, но их гарантированная безопасность не является ключевым требованием. Вполне достаточно принципов риск-менеджмента. Тем более что терять владельцам такого бизнеса нечего: «банкрот отдаёт своим кредиторам пиджак, предварительно переложив бумажник в карман брюк».

ПРО ЦЕЛЕПОЛАГАНИЕ И СТРАТЕГИЮ

Цитата. «...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 задачи создания системы ИБ единого хозяина».

Комментарий. Автор, по-моему, не прав, утверждая, что «с целеполаганием и стратегией у нас и возникают проблемы в силу отсутствия задачи создания системы ИБ единого хозяина».

Проблемы с целеполаганием и стратегией у нас возникают в связи с фактическим бездействием 172-ФЗ о стратегическом планировании. Причин — очень много. Среди важнейших — отсутствие методологии включения в национальную систему планирования основного звена нынешней экономики России — предприятий и отсутствие инструментов системной увязки 62 тысяч муниципальных планов развития.

Квалификация нынешних чиновников такова, что они не обладают знаниями и опытом в области стратегического планирования, сосредотачиваясь на решении задач антикризисного управления на основе краткосрочных планов. При этом в основе планирования оперативного уровня — решение задачи макроэкономической финансовой стабильности (пресловутый «вашингтонский консенсус»), которая никак не увязана с решением задач развития реального сектора экономики. Однако суэта вокруг управления показателем инфляции позволяет изображать деятельность и красиво отчитываться, не приводя при этом к реальному решению задач.

И по этой причине действующие разрозненно ведомства пока остаются единственной надеждой тех, кто искренне заинтересован в решении текущих задач обеспечения ИБ.

ПРО ОПЫТ РЕГУЛИРОВАНИЯ «СНИЗУ»

ПОЧЕМУ НЕ РАБОТАЮТ ОСНОВОПОЛАГАЮЩИЕ ПРИНЦИПЫ?

Вопросы, поднятые в статье А. П. Курило, назрели давно и, безусловно, нуждаются в обсуждении и поиске возможных решений на разных уровнях. Многие указанные Андреем Петровичем проблемы созвучны тем, у кого душа болит не только за свой карман и интересы организации (место работы), но и за страну в целом.

Централизация управления защитой информации в стране — мечта многих специалистов ИБ, но, к сожалению, мечта почти несбыточная. Если создавать такой орган, надо слишком многое менять. Всем уполномоченным органам, которые перечислены в статье А. П. Курило, законодательно переданы вполне определённые задачи по принципу «всем сёстрам по серьгам». Чтобы объединить эти заполненные «поляны», надо создавать орган, которому будут подчиняться все. Возможно ли это? Наверное, да, но для этого должна быть воля руководителя самого высокого ранга и достаточно много времени на подготовку такого преобразования.

Куда проще попробовать решить часть озвученных в статье проблем на гораздо более низком уровне. Коротко расскажу историю. В марте 2015 года было создано некоммерческое партнёрство СОИБ (содействие организациям, работающим в сфере ИБ), которое планировалось перевести в СРО (саморегулируемая организация). Я возглавлял НП СОИБ до недавнего времени. Идея регулирования рынка на низшем уровне была простая. В первую очередь это защита интересов служб информационной безопасности: помощь в подготовке независимых требований к конкурсам, сито для допуска к конкурсу только компаний, которые смогут выполнить работы на высоком профессиональном уровне и с необходимым уровнем качества, консалтинг, подбор аутсорсеров и т. д.

Во вторую очередь планировалось помогать регуляторам в подготовке проектов актуальных методических и нормативных актов, снабжать

их свежей аналитикой по новым технологиям, состоянию зарубежной нормативной базы, тенденциям, анализу отечественного рынка и т. д.

В третью очередь были планы защищать рынок СИ, который за прошедшие семь лет претерпел серьёзные (если не сказать фатальные) изменения. Честные конкурсы — мечта сильных интеграторов...

Ну а в последнюю очередь защита интересов отечественных вендоров, которым тоже весьма непросто. Даже имея хороший продукт, вендор может по пальцам пересчитать компании, имеющие качественно обученных специалистов по своим продуктам в интеграторских компаниях и у заказчиков. На конкурсы подчас выходят компании, готовые «упасть» ниже пола, чтобы укрепить свой имидж или заработать три копейки...

Но идея не была поддержана регуляторами и умерла. Некоторые ассоциации, родившиеся на волне идеи саморегулирования, продолжают существовать, но главная мысль о регулировании «снизу» так и не осуществилась.

* * *

Эту историю я рассказал намеренно, чтобы показать, что проблемы, перечисленные в статье, имеют весьма большой шанс остаться внутри прочитавших её людей и быть забытыми, если не поднимать их для обсуждения среди специалистов разного уровня.

Централизация управления защитой информации в стране — мечта многих специалистов ИБ, но, к сожалению, мечта почти несбыточная. Если создавать такой орган, надо слишком многое менять



Алексей САБАНОВ

заместитель
генерального
директора
ЗАО «Аладдин Р. Д.»,
кандидат технических
наук, доцент МГТУ
им. Н.Э. Баумана,
эксперт ИСО, ТК 362,
ТК 122, ТК 26



Олег ЧУТОВ
вице-президент
компании
«Информзащита»

«НЕЛЬЗЯ ПУГАТЬ, НЕ ТРЕБУЯ»

БЕЗ ОБЪЕКТИВНЫХ ПОКАЗАТЕЛЕЙ
И КРИТЕРИЕВ ОЦЕНКИ МЫ НЕ ВИДИМ
РЕАЛЬНОЙ КАРТИНЫ В СФЕРЕ ИБ

Как отмечено в статье Курило А. П., проблемы сферы информационной безопасности носят системный характер, и, как мне кажется, осветить все их аспекты в одной статье представляется весьма проблематичным.

Вместе с тем Андреем Петровичем чётко выделены основополагающие. Это прежде всего объективная оценка экономических, технологических и организационных аспектов рассматриваемой тематики.

В первой редакции «Доктрины информационной безопасности» превалировал технократический подход к оценке и обеспечению информационной безопасности (далее — ИБ). Причём ИБ рассматривалась как сфера деятельности вне экономических реалий. В новой «Доктрине», принятой в 2016 году, сделан серьёзный шаг по трансформации ИБ из сферы деятельности в индустрию информационной безопасности (производство, сбыт товаров и услуг, потребительская аудитория, экономика).

Включение в общероссийские классификаторы видов экономической деятельности и продукции по видам экономической деятельности кодов¹, имеющих прямое отношение к информационной безопасности, расширяет возможности экономической оценки рынка информационной безопасности, оценки экономических последствий регулирующих воздействий, касающихся ИБ, возможно, и международной сопоставимости.

¹ Приказ Росстата от 17.02.2016 № 40-ст.

Указанное, а также масса других отраслевых статистических материалов могли бы быть использованы для развития экономических механизмов регулирования и защиты внутреннего рынка информационной безопасности, но, как правильно отмечено в статье Курило А. П., в отличие от ИТ-компаний, к ИБ-компаниям возможности тарифных и налоговых инструментов для создания преференций отечественным компаниям до настоящего времени не применялись.

Пока в числе основных инструментов регулирования деятельности субъектов сферы информационной безопасности используется лицензирование. Согласен с Андреем Петровичем, лицензии получают все, кто хочет и удовлетворяет установленным требованиям. Лицензирование носит заявительный характер. А участвует ли лицензиат в работах по обеспечению информационной безопасности? Проводится ли оценка профессионализма лицензиатов по наличию постоянного опыта выполнения работ по ИБ? Достаточны ли полномочия регуляторов в проведении таких оценок?

По данным портала ГАС «Управление», лицензиатов ФСТЭК на деятельность по технической защите информации в конце 2019 года было 2592 компании, число проверок (ограничено государством) в 2019-м — 39. Сколько лет потребуется регулятору, чтобы проверить все компании, и все ли они проживут этот срок?

Вопрос лицензирования — важный вопрос для защиты национальных интересов и интересов потребителей в информационной сфере, однако, помимо лицензиатов, важен вклад самих потребителей, для которых нет требований к наличию соответствующих должностей и профессионально подготовленных кадров в области ИБ.

Для профессиональных игроков рынка не стали новостью выводы ФГБУ «ВНИИ труда» по результатам опроса о потребности в кадрах в области ИБ, что по количеству работников, занятых ИБ, лидируют непрофильные должности, так как вопросы обеспечения

По количеству работников, занятых ИБ, лидируют непрофильные должности, так как вопросы обеспечения ИБ часто возлагаются на бухгалтеров, юристов, педагогов, специалистов безопасности (охраны) и т.д.

ИБ часто возлагаются на бухгалтеров, юристов, педагогов, специалистов безопасности (охраны) и т.д.

Текущий недостаток кадров, испытываемый профессиональным сообществом, и изложенный выше «скрытый» дефицит требуют существенного увеличения кадрового обеспечения отрасли. Это обсуждается уже не один год и Правительством России, и ИБ-общественностью, однако, даже если предположить, что в следующем году число принимаемых на ИБ-специальности будет доведено до необходимой потребности (оценочно по 20 тыс. человек ежегодно, в 2018 г. принято 8,5 тыс. человек), результат мы получим не раньше, чем через пять лет.

В этой связи следует принимать во внимание необходимость гибких комплексно увязанных решений во всех сферах, влияющих на отечественный рынок. И прежде всего в экономической.

«Цифровая повестка» и связанные с этим ожидания создают иллюзию исключительного экономического роста в ИТ-отрасли. Однако по данным, ежегодно публикуемым Минэкономразвития, годовые объёмы ИТ-рынка в период 2012–2018 гг. в сопоставимых от уровня предыдущего года ценах только уменьшались и не превысили 800 млрд руб. Доля ИБ-рынка в объёмах ИТ-рынка составляла около 10–15 %. В то же время, по данным портала Госзакупок, в 2018 году объём заключённых на портале контрактов достиг 25 трлн руб. (только 44 и 223 федеральные законы).

И здесь сложно не согласиться с Андреем Петровичем, что ИТ- и ИБ-рынки — небольшие по объёмам, оставаясь расходной частью в бюджетах потребителей, главным образом призваны способствовать росту других отраслевых сегментов экономики за счёт повышения их эффективности и защищённости.

По поводу регуляторной деятельности в ИБ-сфере. Думаю, что, с одной стороны, обсуждение «высокой зарегулированности рынка» и, с другой, призыв к интенсификации научно обоснованных подходов к обеспечению ИБ должны быть соотнесены с текущими политическими, общественными и технологическими реалиями. Нельзя одновременно пугать общество «ИТ-бедами», а от регуляторов требовать понижения требований.

Мне представляется, что в последние годы со стороны регуляторов осуществляется планомерное и взвешенное развитие форм и методов противодействия противоправным действиям. Да, не всё решено, есть недостатки, но отрицать явный наметившийся прогресс сложно.



В частности, отмечу, что регуляторные изменения в сфере ИБ (требования к защите ГИС и персональных данных, КИИ, банковских систем), принятые в последние годы, не только поддержали ИБ-рынок, но даже способствовали росту его объёмов.

За последнее десятилетие существенно выросла доля закупаемых отечественных средств защиты и покрывающих большую часть требований регуляторов, хотя продолжает сохраняться зависимость от импортных: аппаратной базы с высокой производительностью и программных средств, реализующих перспективный функционал.

И последнее, в чём я абсолютно солидарен с Андреем Петровичем, так это необходимость принятия семейства объективных показателей и критериев оценки в сфере ИБ, что обеспечило бы условия для обсуждения и принятия решений путём аргументации, а не голословных утверждений.

«ЗАСТОЙ ИДЕЙ, ГОНКИ ЗА ХАЙПОМ, РАЗМЫТЫЕ ЗОНЫ ОТВЕТСТВЕННОСТИ»

НЕ БУДУ ПИСАТЬ МНОГО, ПОСТАРАЮСЬ ИЗЛОЖИТЬ ТРИ МЫСЛИ, КОТОРЫЕ ЯВЛЯЮТСЯ, С МОЕЙ ТОЧКИ ЗРЕНИЯ, ВАЖНЫМИ ДЛЯ ПОНИМАНИЯ ТОГО, ЧТО ПРЕДСТАВЛЯЕТ СОБОЙ РЫНОК ИБ В ЦЕЛОМ, НЕ ТОЛЬКО В РОССИИ



Владимир ИВАНОВ
директор по развитию
компании «Актив»

ЗАСТОЙ НА УРОВНЕ ИДЕЙ

Вопрос не только в организации процесса управления в ИБ, но и в развитии самих технологий ИБ. На протяжении уже достаточно длительного времени можно наблюдать если не застой на уровне идей, то ожидание появления каких-то принципиально новых подходов. А ожидания раз за разом не оправдываются. Это не плохо и не хорошо, ибо ИБ — сфера довольно консервативная. Ожидать прорывов в ИБ без прорывов в ИТ в смысле фундаментальной архитектуры нет оснований.

ГОНКИ ЗА ХАЙПОМ

На рынке ИБ время от времени поднимается тот или иной «хайп», и практически все в него бросаются. Это вопрос вложения денег, инвестиций. Заказчик ищет, куда потратить бюджет при отсутствии чего-то действительно нового. Поставщики бросаются инвестировать в разработки продуктов и сервисов, которые сейчас «на волне», пытаясь отхватить кусок пирога бюджетов заказчиков. Что имеем в результате? Конкуренцию? Ну, так себе конкуренция. На рынок выбрасывается набор полусырых продуктов, поскольку сфокусироваться на чём-то не позволяет скачущая конъюнктура. Получается, что в современном мире быстрое распространение информации

даже мешает развитию. Оказывается, что пиар важнее и приоритетнее глубины и сути. Гонки за хайпом порождают освоение бюджетов в худшем смысле. Тут же бешеная борьба за ресурсы, в первую очередь — за интеллектуальные, за людей.

РАЗМЫТЫЕ ЗОНЫ ОТВЕТСТВЕННОСТИ

Сейчас сложность ИТ-систем растёт ещё быстрее, чем раньше. Раньше по большей части мы имели некоторые функционально законченные, самодостаточные информационные системы, пускай даже «облачные». Они принадлежали одному владельцу, и на них худо-бедно работала парадигма защиты периметра. Как работала — хорошо или плохо — это отдельный вопрос. Теперь же настало время объединения систем. Каждая из них выполняет какую-либо функцию, и у неё есть свой владелец. Между этими системами существуют взаимосвязи, интерфейсы, которые, в свою очередь, привносят новые слабые места, требующие защиты.

В то же самое время каждая такая система является поставщиком услуги или данных для других систем, принадлежащих другим владельцам. И на сегодняшний день нет понимания и подходов к обеспечению и управлению безопасностью таких объединённых систем в целом. У каждого из владельцев своё видение, для разных подсистем устанавливаются разные требования по безопасности, они могут находиться под разным регулированием. Это влечёт несогласованность действий по защите таких объединённых систем, поскольку зоны ответственности размываются, а как результат — их потенциальная уязвимость существенно увеличивается.

Получается, что в современном мире быстрое распространение информации даже мешает развитию. Оказывается, что пиар важнее и приоритетнее глубины и сути.

«ЧЕРЕЗ 2–3 ГОДА РЫНОК ИБ КАРДИНАЛЬНО ИЗМЕНИТСЯ»

ИГОРЬ ЛЯПУНОВ — ОБ ОПЫТЕ РАЗВИТИЯ НОВЫХ СЕГМЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ВЫЗОВАХ И БУДУЩЕМ ОТРАСЛИ

Компания «Ростелеком-Солар» (ранее — Solar Security) за пять лет прошла путь от стартапа до лидера на российском рынке информационной безопасности. История её развития — это не только частный пример успешного высокотехнологичного бизнеса, но и в определенной мере отражение эволюции отрасли информационной безопасности с её меняющимися доминантами, драйверами и подходами. В юбилейном интервью BIS Journal поговорили с Игорем Ляпуновым о том, как изменился за эти пять лет рынок ИБ.

ГЛАВА В ИСТОРИИ

— Как бы вы закончили фразу «Без нашей компании в этом мире не было бы ...»?

— Все новое — это результат стечения обстоятельств и факторов. Не хочу переоценивать роли любой компании, в том числе и нашей, в истории, но, полагаю, можно сказать, что «Ростелеком-Солар» стал катализатором формирования таких важных направлений, как мониторинг инцидентов и аутсорсинг информационной безопасности.

— Поясните, пожалуйста.

— Сегодня парадигма информационной безопасности заметно изменилась. До недавнего времени все делали акцент на средствах защиты. Строили вокруг своей информационной системы «забор», все выше и выше. Появлялся новый способ атаки — тут же разрабатывался или покупался новый продукт для защиты. С течением времени появилось понимание, что каждое следующее средство ИБ усложняет систему и скорее снижает общий уровень безопасности, потому что при таком подходе на эксплуатацию требуется все больше и больше человеческих и финансовых ресурсов.

Сейчас превалирует другой подход. Его суть в том, чтобы заниматься мониторингом инцидентов, а не строить ещё более высокий «забор». Образно говоря, держать внутри периметра

служебную собаку, специально обученных охранников, настроить видеонаблюдение... то есть постоянно следить за тем, кто и где пытается проникнуть на территорию.

Сегодня ключевым моментом становится то, как быстро будет обнаружен инцидент. Главная задача безопасника — обнаружить проникновение и отреагировать на него быстрее, чем злоумышленник нанесет ущерб.

Сегодня система информационной безопасности: а) выявляет инциденты и атаки, б) создает барьеры на пути злоумышленника от периметра до цели — места, где будет нанесен ущерб. И мы являемся пионерами, драйверами и апологетами именно такой — новой — безопасности через мониторинг.

— Спасибо. Были ли препятствия на пути становления этого подхода? Считаете ли вы себя лидером этого направления сегодня?

— Когда мы пять лет назад начали строить компанию Solar Security и выводили на рынок новую бизнес-модель и новые технологии, многие говорили: парни, вы безумны, у вас ничего не получится! Для нас же такие слова были лишь одним из признаков того, что мы делаем что-то новое, необычное, даже революционное, и действительно концепция кибербезопасности в сервисной модели серьезно повлияла на рынок. А когда мы вошли в состав компании «Ростелеком», наш потенциал мгновенно многократно увеличился. Это было не только благом, но, безусловно, и испытанием. Но мы выдержали этот стремительный рост, не свернули с взятого курса, и теперь, находясь совсем в другой весовой категории, действительно влияем на отрасль и изменяем рынок ИБ во всем его масштабе.

РАЗРУШЕНИЕ БАРЬЕРА

— Как, с вашей точки зрения, изменился за эти пять лет ландшафт рынка ИБ?

— Я вижу два ключевых процесса, меняющих рынок. Первый — за эти пять лет бизнес начал осознавать зависимость от информационных



Игорь ЛЯПУНОВ
вице-президент
«Ростелекома»
по информационной
безопасности,
генеральный
директор компании
«Ростелеком-Солар»



технологий и потребность в обеспечении реальной безопасности, а не «бумажной». Это, конечно, процесс поступательный, небыстрый, но тенденция обозначилась отчетливо. Конечно, по-прежнему есть явление, когда одни специалисты продают другим «соответствующие нормативам» решения, но появился запрос от бизнеса, и это мгновенно активизировало рынок.

Второе — вся наша экономика стремится к оптимизации, а оптимизацией, особенно сегодня, бизнес занимается через повышение эффективности непрофильных видов деятельности, в частности, информационной безопасности. Мы движемся в шеринг-экономику, экономику разделений. И «Ростелеком-Солар» первым привнес на рынок ИБ сервисную модель, аутсорсинг информационной безопасности. Когда

заказчик сталкивается с задачей обезопасить свой бизнес и начинает разбираться в теме, он понимает, что сделать это без большой специализированной команды крайне трудно. Его служба ИБ говорит: нужно потратить десять/двадцать/сто миллионов, и тогда вероятность атаки будет чуть ниже, но гарантий дать нельзя. А бизнесу нужны гарантии. В этом отношении аутсорсинговая компания с более широкими возможностями, отлаженными процессами и внутренней экспертизой имеет безусловные преимущества.

Под эти изменения подстраиваются все крупные игроки. Я считаю, что это наше большое достижение, именно мы разрушили барьер неготовности рынка к аутсорсингу. Теперь это большая, быстро развивающаяся ниша.



«ЧЕРЕЗ ДВА-ТРИ ГОДА МЫ НЕ УЗНАЕМ РЫНОК»

— Попробуйте обозначить место вашей компании в истории ИБ на данном этапе.

— До 2018 года рынок информационной безопасности развивали регуляторы и небольшие частные компании, все инвестиции были незначительными. В 2018 году на него пришли крупнейшие российские корпорации — игроки с принципиально большим капиталом. Сначала «Ростелеком», за ним «Сбербанк» и «Ростех». И это изменило всё — и размер рынка ИБ, и его потенциал, и баланс сил на нем. Ростелеком купил компанию Solar Security. На тот момент это была крупнейшая M&A-сделка на этом рынке. Сегодня инвестиции «Ростелекома» в информационную безопасность на порядок превышают

совокупные финансовые объемы этого рынка в 2015–2017 годах.

Понятно, что в таком контексте наша компания тоже масштабировалась. Мы растем как органически, так и неорганически. Помимо базовой деятельности — развития технологий, формирования потребностей у заказчика, реализации крупных проектов — мы проводим слияния и поглощения. «Ростелеком» вошел в крупнейший российский венчурный фонд — Фонд развития интернет-инициатив. Вместе с ним мы будем заниматься инвестированием в стартапы, разрабатывающие технологии кибербезопасности. И конечно, мы много вкладываемся в людей, в развитие компетенций — даже не у своих собственных сотрудников, а в целом на рынке. У нас большие вузовские программы, профильная практико-ориентированная подготовка специалистов. Мы ведем треки со школьниками, например, совместные программы с образовательным центром «Сириус».

И, конечно, такого движения, драйва на рынке ИБ два года назад не было. Я уверен, что ещё через два-три года мы его вообще не узнаем.

ПЕРЕХОД К ОТВЕТСТВЕННОСТИ ЗА ИНЦИДЕНТЫ И УЩЕРБ

— Как вы оцениваете сложившуюся в России систему регуляtorики ИБ?

— Регуляторика в последние годы активно развивается — на примере методических рекомендаций ФСБ России по созданию центров ГосСОПКА мы видим, что требования к наличию систем защиты информации сменяются требованиями по созданию процессов информационной безопасности. Это значимый шаг в уходе от парадигмы «бумажной безопасности», которая процветала за счет формального подхода многих организаций к обеспечению соответствия требованиям регуляторов. Однако в этом отношении рынку ещё есть к чему стремиться.

Следующим логичным шагом мог бы быть переход от штрафов за несоответствие нормативным требованиям к ответственности за инциденты и ущерб, который возникает вследствие этих инцидентов. Например, утечки персональных данных. Они происходят едва ли не ежедневно, но разве кого-то за это серьёзно наказали?

Да, сейчас в нормативной базе появились слова об ответственности за инциденты в КИИ, но эту историю необходимо целенаправленно развивать. Когда бизнес начнет понимать, что в случае значительного ущерба в КИИ возникает

его ответственность, он, конечно, станет внимательнее относиться к реальной безопасности, а не просто делать красивые отчеты. И средства для этого он станет выбирать сам, так как его главным ориентиром станет реальная эффективность системы, а не соответствие требованиям. И этой трансформации подхода не надо бояться: во всем мире рекомендательные стандарты вкупе с ответственностью за ущерб работают гораздо эффективнее, чем обязательные нормативные требования.

ВЗРАЩЕНИЕ КАДРОВ ЖИЗНЕННО НЕОБХОДИМО

— Безусловно, компания за пять лет изменилась, выросла. Какие направления «выстрелили» неожиданно для вас?

— Когда мы начинали, не ожидали, что так серьезно вырастет направление по возвращению кадров, по работе с вузами. Но для нас оно оказалось жизненно необходимым. Объем бизнеса удваивается ежегодно, соответственно растет потребность в квалифицированных специалистах. На рынке просто нет такого объема кадров, поэтому мы стали работать с вузами. Постепенно это превратилось в очень созидательное направление, поддерживающее и нас, и другие компании отрасли. Конечно, наши вузовские программы — это подготовка кадров не только для нас, но и для наших заказчиков, и партнеров, и даже конкурентов. По сути, мы работаем на информационную безопасность страны в целом.

— Предполагается ли в ближайшее время выделение из компании самостоятельных направлений?

— Уже сегодня направление информационной безопасности в «Ростелекоме» не монолит, а группа компаний. В целом у нас три больших бизнес-направления. Первое — это сервис-провайдер, предоставляющий сервисы центра мониторинга и реагирования на кибератаки, киберполигона и т.д. Второе — вендор-разработчик средств защиты и технологий безопасности. И третье — это системная интеграция и реализация крупных комплексных проектов в области ИБ. Мы постепенно их дистанцируем друг от друга — понятно, без потери единого управления и взаимодействия.

МАШИНА ВРЕМЕНИ

— Как, на ваш взгляд, повлиял Covid-19 на ситуацию в сфере ИБ?

— Тут надо говорить скорее про IT. На мой взгляд, самоизоляция оказалась волшебной палочкой, машиной времени, которая в один



миг перенесла цифровизацию лет на пять вперед. Технологии проникли буквально в каждый дом — с их помощью люди начали удаленно общаться с родными и друзьями, проводить школьные занятия, покупать еду и различные товары для дома. В это же время стало понятно, что цифровые компании являются нашим безальтернативным будущим. Мы все наблюдали, как за первые две-три недели самоизоляции крупнейшие консервативные компании, в первую очередь из ритейла и HoReCa, которые, казалось, никогда не уйдут с рынка, всё потеряли. И за эти же две-три недели их место заняли цифровые компании, которые в обычной ситуации доказывали бы эффективность своих бизнес-моделей долгие годы. Информационная безопасность — необходимая составляющая процесса цифровизации, она становится драйвером и этой отрасли.



Хотя сам по себе режим самоизоляции принес много проблем. Компании в авральном режиме переходили на удаленную работу, большинству было не до кибербезопасности. Периметра как такового не осталось, компании сейчас очень уязвимы. И перед безопасниками встал серьезный вызов — адаптироваться к новым условиям, обеспечить защиту от угроз в этом дивном новом мире.

О БУДУЩЕМ

— Какой вы видите компанию через пять лет? Каким представляете ландшафт ИБ вокруг нее?

— Надеюсь, что рынок станет более зрелым и будет, по аналогии с западными, иметь четкую градацию: стартапы, небольшие компании на инвестиционных циклах, институциональные игроки... На мой взгляд, мы движемся

к модели, при которой крупные компании с серьезным капиталом и инвестиционными рычагами — такие, как «Ростелеком», Сбербанк, Ростех, Яндекс, Mail.ru и другие, — будут стремиться к созданию мультисервисных платформ, агрегирующих технологии небольших сторонних вендоров, технологических стартапов. Те будут развиваться за счет этих инвестиций или развития собственной ниши.

Это движение — уже наблюдаемый тренд и признак того, что рынок информационной безопасности, когда-то анемичный и инертный, начинает превращаться в нормальную цифровую индустрию. И мы видим нашу роль в том, чтобы поддерживать, усиливать это развитие — за счет инвестиций в отрасль, развития технологий и взращивания кадрового резерва.

— Спасибо. Удачи!

Вопросы задавал
Игорь Некрасов



Анатолий АКСАКОВ
председатель Комитета
Государственной думы РФ
по финансовому рынку

«ЕДИНОЕ ОКНО» ДЛЯ ГОСУДАРСТВА И ГРАЖДАН. ТРЕТИЙ ЛИШНИЙ

ПРЕИМУЩЕСТВА ЕФРДН ФИНАНСОВЫЕ ОРГАНИЗАЦИИ ОЩУТЯТ, ХОТЯ И ОПОСРЕДОВАННО

Единый федеральный информационный регистр сведений о гражданах России — удобное и безопасное «единое окно» электронного документооборота. Данные, содержащиеся в нём, федеральное законодательство сделало доступными только для государственных нужд и физическим лицам, которым они принадлежат. Хотя и не напрямую, но пользу оптимизация этого сектора электронного документооборота принесёт и финансовым организациям, как и бизнесу в целом.

УНИВЕРСАЛЬНОЕ «ОКНО»

Федеральный закон от 8 июня 2020 года № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» служит правовой основой создания единого централизованного информационного ресурса, содержащего базовые сведения о населении России. Цели ЕФРДН — максимальное снижение объёма бумажного межведомственного документооборота, внедрение в полной мере принципа «одного окна» для всех видов взаимодействия граждан и юридических лиц с государством.

Ресурс предназначен, во-первых, для предоставления возможности получения полных и достоверных сведений о физическом лице, необходимых для оказания государственных услуг. Во-вторых, для унификации информационных ресурсов других государственных органов со сведениями, содержащимися в нём. В-третьих, для ведения централизованного статистического учёта посредством информационного взаимодействия с иными ресурсами.

Сведения, содержащиеся в ЕФРДН, могут предоставляться по запросу органов законодательной и исполнительной власти, МФЦ, внебюджетных фондов, избирательных комиссий, а также нотариусов. Коммерциализация единого федерального информационного регистра не предполагается. Бизнес,

в том числе и финансовые организации, не будут иметь доступа к находящимся в нём сведениям.

С ПОДАЧИ НАЛОГОВИКОВ

Разрабатывался законопроект Федеральной налоговой службой России, использовавшей полномочия субъекта права законодательной инициативы, которым наделено Правительство РФ. Во время первого проекта закон представлял М. В. Мишустин, в то время руководитель ФНС России, который сейчас возглавляет Правительство РФ.

23 июля 2019 года проект Федерального закона № 759897-7 с первоначальным названием «О едином федеральном информационном ресурсе, содержащем сведения о населении Российской Федерации» был внесён в Госдуму Правительством РФ. Ответственным комитетом по работе над законопроектом был назначен Комитет Государственной думы по информационной политике, информационным технологиям и связи.

В ходе обсуждения законопроекта в Госдуме РФ и в обществе был сделан ряд критических замечаний, в том числе резонансных. Всего ко второму чтению законопроекта поступило 48 поправок, из них 18 принято, 30 — отклонено. 21 мая 2020 года законопроект был принят в окончательном третьем чтении и направлен в Совет Федерации ФС РФ.

ОБСУЖДЕНИЕ И КРИТИКА

Оппозиционные фракции проголосовали против его принятия. Представители КПРФ, ЛДПР и «Справедливой России» высказали опасения относительно защиты персональных данных, ссылаясь на зарубежный опыт. Думская оппозиция высказывала предположение, что создание единого регистра чревато утечками персональных данных граждан России.

Кроме того, по мнению оппозиции, документ противоречит действующему федеральному законодательству.

В частности, он будто бы не соответствует ст. 24 Конституции России, согласно которой «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

Также критики утверждали, что законопроект не соответствует ст. 5 Федерального закона «О персональных данных» от 27 июля 2006 год № 152-ФЗ. То есть аннулирует запрет на «объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой». Якобы этот запрет технически обеспечивает конституционное право на неприкосновенность частной жизни.

ЗАКОНОДАТЕЛЬНАЯ ДОРАБОТКА

Прозвучавшая критика и состоявшиеся прения помогли доработке законопроекта. В частности, в названии предмета законопроекта слово «ресурс» было заменено на «регистр». Появилась закрытая часть — сведения о лицах, находящихся под государственной защитой.

Также возникла возможность с использованием регистра совершать нотариальные действия. Кроме того, в федеральный регистр будут включаться сведения не только о гражданах России, но и об иностранцах, а также о лицах без гражданства, проживающих либо работающих в нашей стране.

Первоначально граждане не могли получать из регистра сведения о себе. Замечания на этот счёт учли, и при доработке законопроекта они или их законные представители были наделены правом запрашивать и получать эти данные. Сведения о детях могут выдаваться их родителям, опекунам и законным представителям. Также был отрегулирован порядок внесения изменений в регистр в случае выявления гражданином ошибок в своих данных. Воспользоваться этими новыми возможностями граждане смогут с 2026 года.

ОТВЕТСТВЕННОСТЬ ЗА БЕЗОПАСНОСТЬ

Правовые нормы обеспечения безопасности данных, содержащихся в ЕФРДН, определены требованиями федерального законодательства, включая законы об информации, информационных технологиях и защите информации, персональных данных, о государственной и иной охраняемой законом тайне. Ответственность за эту деятельность распределяется следующим образом.

ФНС России является уполномоченным органом и оператором ЕФРДН и обязана обеспечить безопасность содержащихся в нём сведений о гражданах. Во-первых, самой информации о населении — от несанкционированного доступа, случайного или несанкционированного изменения, уничтожения или утраты. Во-вторых, межведомственного информационного взаимодействия при формировании и ведении этого федерального регистра.

Данные будут находиться в центре обработки данных, безопасность которого гарантируется уполномоченными органами, в первую очередь ФСБ России. Внутри этой базы будет

Дополнительного сбора сведений о гражданах не потребуется. Все сведения, которые наполнят ЕФРДН, — те, которыми государство уже располагает, только прежде рассредоточенные по разным ведомствам

ещё один внутренний периметр, связанный с деятельностью силовых структур. Необходимо отметить, что ФНС России за всю историю ни разу не допускала утечек сведений, что свидетельствует о достаточно высоком уровне защищённости.

Своя зона ответственности есть и у органов государственной власти Российской Федерации и субъектов Федерации, местного самоуправления, государственных внебюджетных фондов, МФЦ, избирательных комиссий, а также нотариусов. При обработке в своих информационных системах сведений о населении, полученных из федерального регистра, они обеспечивают их защиту.

ПРЕИМУЩЕСТВА НОВОВВЕДЕНИЯ

Дополнительного сбора сведений о гражданах не потребуется. Все сведения, которые наполнят ЕФРДН, — те, которыми государство уже располагает, только прежде рассредоточенные по разным ведомствам. Есть принципиальная новизна в сравнении с другими государственными базами персональных данных (МВД России, ФНС России и др.). ЕФРДН — первая федеральная информационная система, аккумулирующая основные сведения о гражданах России и всех лицах, прибывающих на территорию страны.

Создание Единого федерального регистра населения позволит оперативно оказывать гражданам адресную материальную и социальную поддержку, значительно сократить время оказания государственных услуг без требования избыточных бумаг, заявлений. Государство повысит качество прогнозов для долгосрочного развития страны, регионов, сможет получать актуальную статистику.

Ещё одно из преимуществ системы — это то, что она не только хранит в структурированном виде данные о гражданах, но и анализирует содержимое различных ведомственных баз данных для поиска и устранения неточностей, которые в них возникают. Сейчас такие ошибки исправляются по факту обращения граждан, а система единого информационного ресурса постепенно будет делать это в частично автоматическом режиме.

* * *

Созданные и принятые нормы деятельности ЕФРДН открывают всем гражданам возможность доступа к данным о себе, которые содержатся в регистре. Каждый, кто внесён в него, сможет проверить корректность своих персональных данных, посмотреть перечень формируемых в отношении него запросов, что исключит возможность ущемления его прав в случае возможных инцидентов, технических и иных.



Михаил БУХТИН
начальник управления
моделирования рисков
Департамента банковского
развития Банка России

ИНЦИДЕНТЫ ОБОЙДУТСЯ БАНКАМ НАМНОГО ДОРОЖЕ

БАНК РОССИИ НАЧАЛ НОРМАТИВНО
КВАЛИФИЦИРОВАТЬ РИСКИ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ КАК ОПЕРАЦИОННЫЕ

8 июня Министерство юстиции РФ зарегистрировало Положение Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе». В соответствии с этим документом, как и в международной практике, риск информационной безопасности является подвидом операционного риска, а управление им включено в систему управления операционным риском.

БОЛЕЕ СЕРЬЁЗНЫЙ УРОВЕНЬ

Банк России устанавливает нормативные требования к системе управления операционным риском, включая риски информационной безопасности и информационных систем. Формулируются требования к классификации событий реализации таких рисков, к ведению соответствующей базы событий, а также показателей контроля полноты учёта прямых потерь.

Это более серьёзный уровень требований в сравнении с Положением 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».

Включение управления риска информационной безопасности и риска информационных систем в систему управления операционным риском в целях обеспечения информационной безопасности компьютерных систем и сервисов

кредитных организаций направлено на повышение значимости этого направления деятельности, ответственности за её результаты.

Во-первых, нормы обеспечения информационной безопасности, которые прежде носили рекомендательный характер, становятся обязательными. Во-вторых, конечная ответственность за эти вопросы переходит с подразделений информационной безопасности на руководство кредитных организаций.

ИНФОРМАЦИОННЫЕ РИСКИ ДОРОЖАЮТ

Данная новация отвечает зарубежной и международной практике, подходу стандартизированной оценки Базеля III, согласно которой расчёт размера операционного риска включается в нормативы достаточности капитала. Уровень риска информационной безопасности, наряду с другими рисками, теперь напрямую влияет на размеры достаточности капитала.

Чем хуже обеспечение информационной безопасности и управление этим риском, тем чаще в банке будут реализовываться потери от реализации этих рисков, что в итоге приводит к повышению резервного капитала, выделяемого на покрытие операционных рисков через так называемый коэффициент внутренних потерь, участвующий в формуле его расчёта, и наоборот.

Информационная безопасность превращается в один из главных показателей оценки банковской деятельности. Устанавливается прямая связь между обеспечением информационной безопасности и финансовыми аспектами деятельности кредитных организаций. Это в равной мере относится как к банкам, так и к небанковским кредитным организациям.

**НЕ ОКАЗАТЬСЯ
В «ШТРАФНИКАХ»**

Для кредитных организаций это означает необходимость более серьёзного подхода к обеспечению информационной безопасности. Классификация рисков в этой сфере предполагает выделение из общего количества инцидентов, реализовавшихся в виде нарушений работы компьютерных систем, утечек информации, персональных данных, таких событий, которые приводят к прямым потерям и убыткам кредитной организации, например, в виде кражи денежных средств.

Чтобы достигнуть соответствия Положению № 716-П, кредитным организациям придётся провести ряд мероприятий. Решение об этом должно принимать руководство кредитной организации, в чью компетенцию входит ответственность за управление операционным риском и информационной безопасностью. Комплекс мероприятий, в основном организационных и связанных с изменением документации, предстоит разработать и выполнять сотрудникам подразделений информационной безопасности.

Для крупных банков выполнение требований № 716-П не должно составить больших трудностей. Учитывая масштабы и широкое распределение бизнес-процессов, информационная безопасность там, как правило, обеспечивается на достаточном уровне, и затраты на создание системы информационной безопасности уже реализованы. Небольшим банкам и небанковским кредитным организациям, возможно, придётся приложить более значительные усилия.

**ЧТО И КОГДА ПРЕДСТОИТ
СДЕЛАТЬ**

Финансовых затрат как таковых на достижение соответствия № 716-П кредитным организациям не потребуется. Востребованы организационные и технологические изменения, например, по обеспечению информационного взаимодействия между подразделениями информационной безопасности и управления операционными рисками, организации между ними документооборота, включение этих вопросов в планы и программы проверок службы внутреннего аудита.

Недостаточное выявление нарушений обеспечения информационной безопасности отныне повлияет на расчёт размера операционного риска, что может обернуться необходимостью повышения нормативов достаточности капитала.



Также за несоблюдение отдельных требований, выявленных в ходе последующего надзора после 1 января 2022 года, могут быть приняты меры в соответствии со статьёй 74 Федерального закона № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в том числе наложены штрафы.

* * *

Можно отметить следующие сроки введения новых требований в силу. 1 октября 2020 года формально начинает действовать Положение Банка России № 716-П. На достижение соответствия его требованиям кредитным организациям отводится весь 2021 год. Лишь после этого срока, в 2022 году, может быть начато проведение контрольно-надзорных мероприятий.



Анастасия ТОЛСТОЛУЦКАЯ
эксперт ТК 26



Андрей ЕЛИСТРАТОВ
эксперт ТК 26



Валерий НИКИТЕНКОВ
эксперт ТК 26

В ШТАТНОМ РЕЖИМЕ

АНАЛИЗ ПОЛОЖЕНИЙ ТРЕБОВАНИЙ К СКЗИ В ПЛАТЁЖНЫХ СИСТЕМАХ, ОПУБЛИКОВАННЫХ НА САЙТЕ БАНКА РОССИИ

Регулирование в области информационной безопасности в банковском секторе за последние годы не раз подвергалось изменениям. Требования к информационной безопасности, закреплённые в положениях Банка России не раз обсуждались в научном сообществе. Актуальность данной статьи обусловлена выходом в январе 2020 года «Требований к средствам криптографической защиты информации в платёжных устройствах с терминальным ядром, аппаратных модулях безопасности информационной инфраструктуры платёжных систем (HSM-модулях), платёжных картах и иных технических средствах информационной инфраструктуры платёжной системы, используемых при осуществлении переводов денежных средств, указанных в пункте 2.20 Положения Банка России от 9 июня 2012 года № 382-П» (далее — Требования).

Данные требования опубликованы на сайте Банка России (https://www.cbr.ru/Content/Document/File/104752/FT_32.pdf) и размещены в правовых справочных системах КонсультантПлюс и ГАРАНТ.

Документ определяет требования по информационной безопасности к техническим средствам и программному обеспечению, реализующим криптографические механизмы:

- ♦ в платёжных устройствах с терминальным ядром (терминалы и банкоматы),
- ♦ аппаратных модулях безопасности информационной инфраструктуры платёжных систем (HSM-модулях),
- ♦ платёжных картах,
- ♦ иных технических средствах информационной инфраструктуры платёжной системы.

Эти требования разработаны и утверждены в рамках мероприятий федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»: 05.02.002.017.004 — «Разработка

и опубликование требований к СКЗИ, указанных в пункте 2.20 положения Банка России от 9 июня 2012 г. № 382-П».

Требования относятся к реализации пункта 2.20 Положения № 382-П, внесённого Указанием Банка России от 7 мая 2018 г. № 4793-У.

ПОЭТАПНЫЙ ПЕРЕХОД

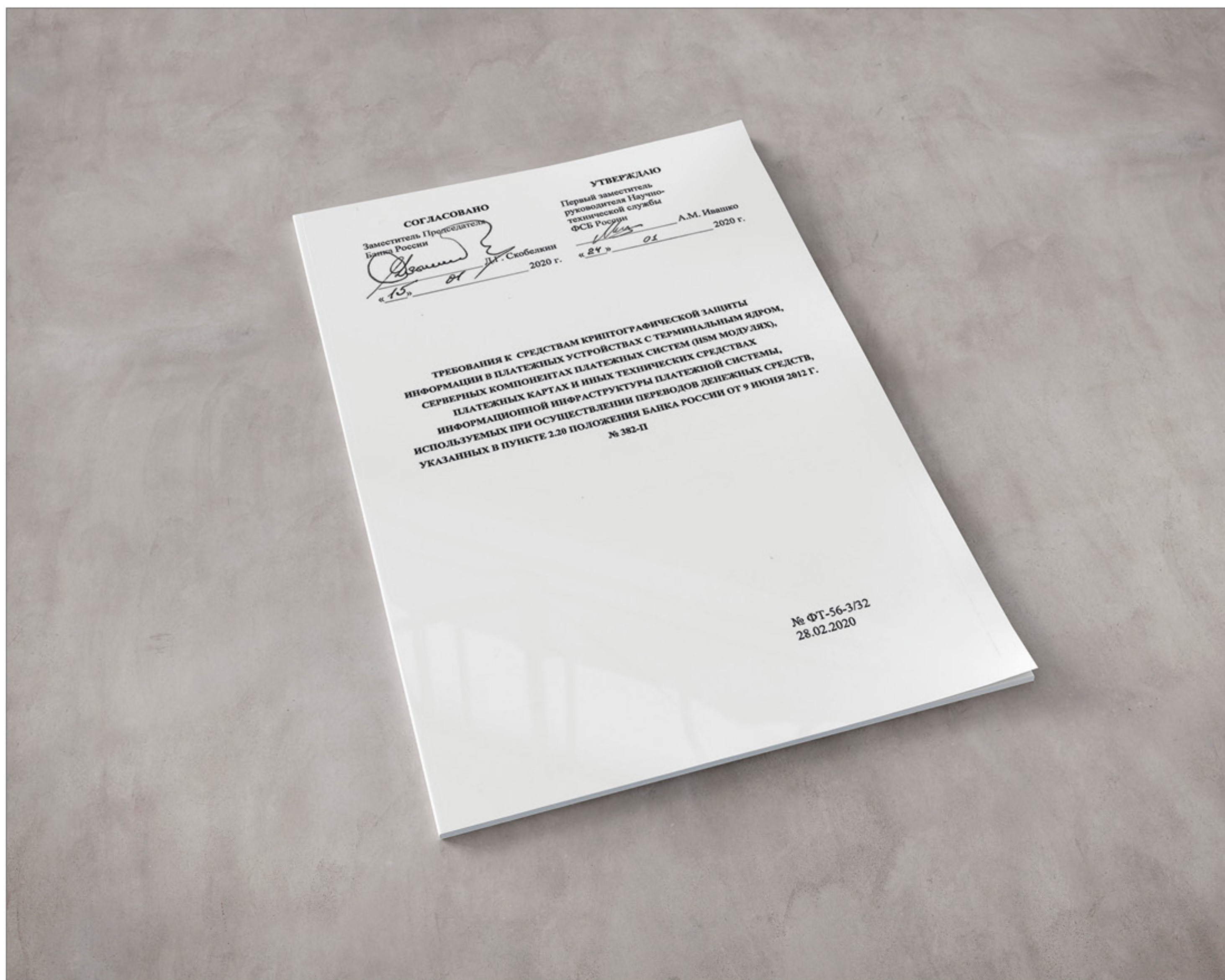
Данным пунктом, вступающим в силу с 1 января 2024 года, вносятся изменения в требования к обеспечению защиты информации при переводах денежных средств. Так, оператору значимой платёжной системы необходимо обеспечить использование в аппаратных модулях безопасности средств криптографической защиты информации (далее — СКЗИ), реализующих также иностранные криптоалгоритмы, прошедших оценку соответствия требованиям ФСБ России.

В соответствии с этим же пунктом с 1 января 2031 года вступают в силу изменения об использовании в аппаратных модулях безопасности СКЗИ, реализующих отечественные криптоалгоритмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.

Таким образом, во-первых, определён переход на отечественные шифровальные средства, а во-вторых, заложена поэтапность такого перехода.

НЕИЗБЕЖНОСТЬ ПЕРЕХОДА

При этом в законодательстве закреплена неизбежность перехода на отечественные шифровальные средства, что необходимо принимать во внимание участникам финансового сектора. Так как уже сейчас необходимо либо закладывать в будущий бюджет расходы на переоснащение в рамках данных нововведений, либо в настоящее время начинать переход на отечественные шифровальные средства, до того как данное требование станет обязательным.



ЕДИНЫЙ ПОДХОД

Рассматриваемые Требования во многом перекликаются с рекомендациями по стандартизации Р 1323565.1.012–2017. Информационная технология. Криптографическая защита информации. «Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации» (далее — Принципы).

Применение мер защиты основывается на тех же подходах, которые указаны в Принципах, однако добавлено положение относительно необходимости использования криптографических механизмов, отвечающих международным стандартам (ISO) с целью обеспечения совместимости с действующими криптографическими решениями.

УТОЧНЕНИЯ

Относительно применения датчиков случайных чисел Требованиями уточняется, что при выработке инициализирующей последовательности для ПДСЧ необходимо использовать либо ФДСЧ, реализованный в СКЗИ, либо последовательность полученную с СКЗИ, прошедшего оценку

соответствия требованиям по информационной безопасности по классу КВ в соответствии с действующими требованиями к СКЗИ. Отмечается, что в HSM для выработки первичной ключевой информации должен использоваться ФДСЧ.

Относительно выработки ключевой информации уточняется, что она должна производиться с использованием датчика случайных чисел, при этом в протоколах выработки общего ключа в криптографических протоколах должны использоваться датчики случайных чисел, удовлетворяющие положениям, описанным выше.

Требованиями зафиксировано, что используемая СКЗИ ключевая информация в незашифрованном виде может храниться только непосредственно в СКЗИ на протяжении установленного срока действия.

ПРО АУТЕНТИФИКАЦИЮ

В части аутентификации субъектов доступа уточняется, что использование паролей для аутентификации субъектов доступа (пользователей), являющихся физическими лицами и осуществляющих доступ к техническим средствам

информационной инфраструктуры платёжной системы, допускается только для локальной аутентификации СКЗИ. При этом для проведения локальной аутентификации с целью изменения настроек безопасности, а также загрузки/смены/уничтожения ключей (администрирования) требуется использовать:

- ♦ в платёжных устройствах с терминальным ядром (терминалах) не менее двух паролей (двойной контроль).

- ♦ в банкоматах, аппаратных модулях безопасности информационной инфраструктуры платёжных систем (HSM-модулях) и иных технических средствах информационной инфраструктуры платёжной системы как минимум два аутентифицирующих фактора (знание, владение).

Кроме того, в HSM критические функции управления ключами также должны выполняться под двойным контролем (т.е. при условии обязательной аутентификации не менее двух привилегированных пользователей). К критическим функциям управления ключами в обязательном порядке должны относиться функции формирования (загрузки) и резервирования локальных мастер-ключей HSM, предназначенных для защищённого хранения ключей держателей карт.

При аутентификации субъектов доступа, являющихся процессами и осуществляющих взаимодействие с СКЗИ, должен быть реализован криптографический механизм взаимной аутентификации.

ПРО ПЛАТЁЖНЫЕ УСТРОЙСТВА

СКЗИ для использования в платёжных устройствах с терминальным ядром (терминалы и банкоматы), аппаратных модулях безопасности информационной инфраструктуры платёжных систем (HSM-модулях), платёжных картах и иных технических средствах информационной инфраструктуры платёжной системы, должны разрабатываться в соответствии с Положением ПКЗ-2005, утверждённым Приказом ФСБ России от 9 февраля 2005 года № 66.

В дополнение к мерам, предусмотренным Принципами, к СКЗИ в платёжных системах должны предъявляться следующие требования:

- ♦ Для серверных устройств (HSM-модулей) должна быть обеспечена защита ключей пользователей от возможных намеренных попыток администратора их компрометации. При этом данная защита должна обеспечиваться как на логическом уровне, так и на инженерном уровне (защита от инженерного проникновения). Все каналы удалённого управления должны быть защищены криптографическим способом с использованием криптографических механизмов, утверждённых в качестве национальных стандартов

Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографических механизмов, имеющих положительное заключение ФСБ России по результатам их экспертных криптографических исследований. При этом при проведении платежей, для совместимости с текущей реализацией, допускается использовать иностранные криптографические алгоритмы.

- ♦ Для платёжных терминалов/банкоматов и платёжных карт должна быть обеспечена защита ключей от компрометации, в том числе способами инженерного проникновения. Все каналы удалённого управления должны быть защищены криптографическим способом с использованием криптографических механизмов, утверждённых в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографических механизмов, имеющих положительное заключение ФСБ России по результатам их экспертных криптографических исследований.

Два последних положения отражают ситуацию, при которой базовая модель нарушителя, приведенная в рекомендациях по стандартизации, расширяется за счет специфики информации и мер её защиты в платёжных системах. Кроме этого, эти положения уже определяют сами меры защиты, а не возможные атаки, приводящие к таким мерам защиты, тем более, что модель нарушителя в Требованиях описывается именно на основе перечня возможных атак нарушителя.

ТРЕБОВАНИЯ В СРАВНЕНИИ С ДРУГИМИ НОРМАТИВНЫМИ АКТАМИ

В Указании Банка России от 10 декабря 2015 г. № 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» содержится подробный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Так, в рамках рассматриваемых Требований наиболее сопоставимыми являются: угроза воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных; угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных; угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодей-

действия и каналов передачи данных; угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации.

При аутентификации субъектов доступа, являющихся процессами и осуществляющих взаимодействие с СКЗИ, должен быть реализован криптографический механизм взаимной аутентификации

Рассматриваемые Требования соответствуют Указанию Банка России от 10 декабря 2015 г. № 3889-У в части перечисленных угроз.

С точки зрения общих принципов построения модели угроз и нарушителя наиболее информативным является Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации Общие положения» (СТО БР ИББС-1.0–2014).

Основными источниками угроз информационной безопасности определены: работники организации банковской системы Российской Федерации, реализующие угрозы информационной безопасности с использованием легально предоставленных им прав и полномочий (внутренние нарушители информационной безопасности); работники организации банковской системы Российской Федерации, реализующие угрозы информационной безопасности вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками организации банковской системы Российской Федерации, но осуществляющие попытки несанкционированного доступа и нерегламентированные действия в рамках предоставленных полномочий (внешние нарушители информационной безопасности).

Указанный Стандарт распространяется на организации банковской системы Российской Федерации и устанавливает положения по обеспечению информационной безопасности в организациях банковской системы Российской Федерации. Соответственно и требования к разрабатываемой модели угроз и нарушителя являются наиболее общими.

Требования, в свою очередь, конкретизируют данные положения и содержат описание модели нарушителя для СКЗИ, используемых при осуществлении переводов денежных средств. Так, согласно Требованиям, СКЗИ должны противостоять атакам, при создании которых используются сведения об СКЗИ, об аппаратных средствах среды функционирования (АС СФ), о программном обеспечении среды функционирования (ПО СФ), а также сведения о платёжной информационной системе. СКЗИ должны противостоять как атакам, которые могут осуществляться из-за пределов контролируемой зоны посредством целенаправленного пассивного и/или активного воздействия на каналы связи технических средств информационной инфраструктуры платёжной системы, так и атакам, которые могут осуществляться нарушителем, имеющим непосредственный доступ к техническим средствам информационной инфраструктуры платёжной системы, посредством попыток несанкционированного доступа, в том числе с использованием методов инженерного проникновения, с целью компрометации ключа или искажения ПО СФ СКЗИ, АС СФ СКЗИ, ПО СКЗИ, АС СКЗИ и протоколов взаимодействия, а также атакам, реализуемым посредством использования штатных средств СКЗИ, специально разработанных АС и ПО, средств перехвата и проведения исследований информативных сигналов, средств, эксплуатирующих для несанкционированного

В случае появления на рынке платёжных устройств, отвечающих необходимым международным стандартам и прошедших оценку соответствия данным Требованиям, их внедрение в платёжные системы может происходить в штатном режиме

доступа недеklarированные (недокументированные) возможности и уязвимости ПО.

Также стоит отметить, что для обеспечения защиты информации с помощью СКЗИ в соответствии с Положением Банка России от 9 июня 2012 г. № 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», а также Положением Банка России от 17 апреля 2019 г. № 684-П «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» необходимо в случае наличия в технической документации на СКЗИ требований к оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, проводить такую оценку. Указанная оценка должна проводиться в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с федеральным органом исполнительной власти в области обеспечения безопасности.

Выводы

Подводя итог проведённого анализа (и проведя сопоставления с классами защищённости, описанными в Принципах), можно сказать, что Требования фактически постулируют следующие уровни обеспечения криптографической защиты информации для используемых платёжных устройств:

- ♦ класс KB — серверные устройства (HSM-модули);
- ♦ класс KC3 — платёжные терминалы/банкоматы;
- ♦ класс KC3 — платёжные карты.

СКЗИ таких классов в настоящее время уже используется в различных областях банковской индустрии Российской Федерации. В связи с этим многие специалисты по информационной безопасности уже имеют опыт внедрения и использования подобных средств.

Это означает, что в случае появления на рынке обсуждаемых платёжных устройств, отвечающих необходимым международным стандартам и прошедших оценку соответствия данным Требованиям, их внедрение в платёжные системы может происходить в штатном режиме без проведения дополнительного обучения специалистов по информационной безопасности.

Сергей ПАЗИЗИН

член редколлегии BIS Journal,
заместитель начальника Управления
по обеспечению информационной
безопасности ДБ Банка ВТБ (ПАО),
кандидат физико-математических наук



ПРО ДЕТАЛИ И ГЛАВНОЕ

РАЗВИТИЕ ОТРАСЛИ ИБ ВОЗМОЖНО
ТОЛЬКО ПРИ УЧАСТИИ ЭКСПЕРТНОГО СООБЩЕСТВА

Задача новой рубрики «Лидеры мнений» — провести своеобразный парад героев, представить крупным планом экспертное сообщество российской информационной безопасности. Перед читателями один за другим предстанут люди уважаемые, известные своей компетентностью, авторитетом и бесспорным влиянием на общественное мнение. В качестве первого героя мы пригласили нашего коллегу, внёсшего значительный личный вклад в становление и определение лица BIS Journal, создателя экспертной группы журнала Сергея Пазизина.

ФАКТОРЫ ВЛИЯНИЯ

— Сергей Владимирович, что сегодня влияет на формирование и развитие отрасли ИБ в первую очередь? Назовите несколько факторов.

— Первопричиной происходящих изменений является проникновение информационных технологий во все сферы жизни общества (производство, финансы, управление, социальное взаимодействие). Как следствие, возникают новые угрозы и необходимость противодействовать данным угрозам, остальные факторы вторичны.

— Назовите тогда главные, принципиальные проблемы, которые, на ваш взгляд, серьёзно тормозят развитие отрасли или заводят её в тупик.

— Из совсем очевидного — технологическое отставание отечественной ИТ-отрасли в части элементной базы, телекоммуникационного оборудования, системного и интеграционного ПО, СУБД. Когда мы рассматриваем угрозы на международной арене, это становится принципиальным.

Одной из причин такого отставания является короткий горизонт планирования отечественных компаний, в том числе работающих в сфере ИТ и ИБ-технологий, а также компаний — «потребителей» безопасности. За редким исключением крупные компании предпочитают не вкладываться в долгосрочные проекты. К тому же многие руководители воспринимают информационную безопасность и даже ИТ как некую обособленную функцию, такую, например, как охрану зданий. Уровень взаимодействия между ИТ, ИБ и бизнесом явно не соответствует современным вызовам.

Кроме указанных субъективных причин, есть и объективные: недостаток финансовых ресурсов для крупных инновационных проектов, ограниченность внутреннего рынка и, соответственно, высокий риск не окупить инвестиции.

По всему остальному я бы не сказал, что мы в тупике. Есть недостатки в регулировании, эффективности государственных проектов, не хватает квалифицированных кадров. Но появление и решение проблем, совершенствование — это естественные процессы развития. Я считаю, положительное движение здесь есть по всем направлениям.

ПРО ОБЩЕСТВЕННОЕ МНЕНИЕ

— Какую роль в процессе развития отрасли играет общественное мнение: конференции, форумы, отраслевые СМИ?

— Для развития отрасли необходима обратная связь — взаимодействие регуляторов с потребителями услуг и производителями, общественными организациями. Очень важно не растаскивать информационную безопасность

по ведомствам и сферам интересов. Наличие конференций, форумов, СМИ — одна из основ существования отрасли как единого целого.

— Сейчас популярны веб-конференции. Как вы считаете, вытеснят ли они очный формат?

— На очной конференции всё же другая атмосфера. Больше личного общения, возможности для неформального обмена мнениями. Поэтому, хотя дистанционный формат существенно экономит время на дорогу и будет, безусловно, развиваться, я бы не хотел, чтобы он полностью вытеснил очные мероприятия.

«РОССИЯ — РОДИНА СЛОНОВ»

— Сергей Владимирович, в последнее время часто приходится слышать, что российская банковская ИБ — лучшая в мире. Не повторяется ли история про «Россию — родину слонов»?

— На состояние информационной безопасности банковской системы России оказали влияние следующие факторы:

♦ Минимальное технологическое наследие в области защиты информации, что позволяло сразу внедрять современные решения. В качестве примера можно привести внедрение Банком России электронной подписи на основе открытых ключей в 1994 году, в то время как в мировой банковской системе продолжалось использование технологий предыдущего поколения. Например, международная система межбанковских коммуникаций SWIFT перешла на цифровую электронную подпись при взаимодействии с банками только в 2003 году. Также эффект «чистого листа» использовался при построении Национальной платёжной системы.

♦ Имевшийся в стране уровень образования, а также задел в обеспечении безопасности государственных систем.

♦ Высокий уровень криминального давления, который не позволяет относиться к защите информации легкомысленно.

♦ Наличие у Банка России полномочий регулятора, в том числе и в вопросах защиты информации.

И, наконец, банковской сфере повезло, что вопросами ИБ занимаются компетентные специалисты и руководители. Большое внимание вопросам ИБ уделяется лично председателем Банка России Э.С. Набиуллиной, а в работе ключевого мероприятия в области банковской ИБ — Уральского форума «Информационная безопасность финансовой сферы» регулярно принимают участие заместители председателя банка России. На Форуме FINOPOLIS на самом высоком уровне рассматриваются возможности применения современных цифровых

технологий в финансовом секторе. Поэтому сказанное мною ранее про непонимание роли ИТ и ИБ — это точно не про Банк России.

Сочетание указанных обстоятельств привело к тому, что российская банковская система — одна из наиболее устойчивых к кибератакам. Вместе с тем сравнение с другими странами не совсем корректно, так как различаются подходы к обеспечению ИБ. Недостаток осознания проблем безопасности на уровне руководителей компаний государство пытается компенсировать детальным регулированием, что по определению не может привести к успеху. Запускается давно знакомый российский механизм, когда строгость законов компенсируется необязательностью их исполнения. Поэтому ограничимся утверждением: если «слоны» родились в России, то именно в банковской системе как передовой отрасли в части применения ИТ и ИБ.

ПРО ЭКСПЕРТОВ

— Вы возглавляете на общественных началах экспертную группу BIS Journal. В чём вы видите её предназначение? Расскажите, пожалуйста, об этой деятельности подробнее?

— «Возглавляете», наверное, не совсем подходящее слово. Я был инициатором создания экспертной группы, так как в настоящее время явно не хватает качественной информации. Это относится не только к ИБ. Интернет и другие средства массовой информации захлёстывает поток хайпа, халтуры и часто откровенного бреда психически нездоровых людей. Это в целом объяснимо — основная масса читателей не является профессионалами в любой конкретной области. СМИ в погоне за кликами и рейтингом ориентируются на массовое сознание. Я думаю, многие заметили, насколько упал уровень новостных порталов после того, как интернет стал по-настоящему массовым. Поэтому, на мой взгляд, очень важно создавать условия для того, чтобы мнение профессионалов отрасли присутствовало в медиапространстве. Принадлежность автора к экспертной группе журнала — это знак качества предоставляемой информации.

Что касается «руководства» экспертами журнала, то я могу высказать замечания до публикации, но согласиться с ними или нет — право эксперта, за ним окончательное решение. И даже включение новых экспертов осуществляется при согласии участников экспертной группы. Лично я предпочитаю общаться с людьми, которые лучше меня разбираются в интересных мне вопросах.

— В журнале инициирована полемика «Смена парадигмы ИБ» (статьи А. П. Курило).

Эксперты высказывают разные мнения, а вы как считаете, правильно устроена наша отрасль или нет?

— Трудно не согласиться с Андреем Петровичем в оценке имеющихся проблем и с тем, что отрасль не имеет единого центра координации. В настоящее время важные решения в ИБ принимаются как результат взаимодействия различных групп интересов. Появление единого административного органа может разрушить имеющийся баланс и поэтому имеет смысл только в том случае, если возглавившие этот орган люди смогут подняться над интересами отдельных групп влияния и проводить разумную политику на благо всего общества.

Есть известная концепция, суть которой в том, что в период кризиса наиболее эффективна жёстко централизованная модель управления, а для успешного развития необходима свобода мнений, конкурентная среда. И если говорить о принятии решений, важных для отрасли, то необходимо развивать независимую экспертизу. Ключевые решения и законопроекты должны проходить публичное обсуждение. Необходимо учитывать мнение ведущих специалистов отрасли. И если создавать новый орган, то не как новую бюрократическую структуру, а как авторитетную площадку для обсуждения и принятия совместных решений. Что, в общем, не противоречит высказанным в статье предложениям.

— Если бы вы обладали достаточными полномочиями, что изменили бы в первую очередь? В каком направлении и как двинули отрасль?

— Дело здесь не в полномочиях, любые полномочия не снимают ограничений, связанных с контекстом, в котором приходится действовать. Это только наивные люди считают, что можно стать большим начальником и сразу решить все проблемы. Наиболее важным сейчас для отрасли я считаю формирование экспертного сообщества, и для работы в этом направлении не нужно иметь никаких особых полномочий — мы уже ведём её на базе журнала, и есть примеры, когда мнение наших экспертов учитывалось на самом высоком уровне.

ПРО РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД

— Как вы оцениваете перспективы применения подхода на основе анализа рисков в информационной безопасности?

— Для бизнеса подход на основе анализа рисков более понятен, чем ссылки на требования стандартов. Но возможность использования такого подхода ранее ограничивалась рядом объективных и субъективных причин. Во-первых,

меньше было взломов, риски ИБ для бизнеса представлялись чем-то эфемерным. Десять лет назад абсолютная величина рисков ИБ не шла ни в какое сравнение, например, с валютными рисками или другими операционными рисками. Соответственно, не было полноценного рискованного мышления в области ИБ — предложение принять риски безопасности воспринималось как попытка подставить. Во-вторых, не хватало данных и опыта для проведения анализа рисков.

К настоящему времени пришло понимание необходимости анализировать, обрабатывать и принимать риски ИБ. Поэтому работы по внедрению модели ИБ на основе анализа рисков в банковской системе я считаю своевременными. Анализ и принятие рисков является одним из механизмов взаимодействия ИБ, ИТ и бизнеса.

— Какие ещё особенности вы бы отметили в организации современной системы ИБ крупной компании?

— В настоящее время практически любое бизнес или ИТ-решение должно приниматься с учётом необходимости обеспечения ИБ. ИБ должна сопровождать внедрение новых сервисов с момента постановки задачи, участвовать в проектировании, разработке, внедрении и сопровождении соответствующих автоматизированных систем. В связи с высокой конкуренцией решения необходимо принимать в кратчайшие сроки. Поэтому, если мы говорим о банках, то сложность и разнообразие решаемых задач уже не позволяют свести процесс обеспечения ИБ к «механическому» соблюдению установленных правил. К этому добавляется необходимость предоставления современных сервисов безопасности, таких как услуги удостоверяющего центра, контроля утечек, анализа информационных потоков на предмет выявления вредоносного ПО, защиты рабочих мест, обработки инцидентов. Последние несколько лет в банках осуществляется переход от модели взаимодействия ИБ, ИТ и бизнеса, в которой ИБ устанавливает правила и контролирует их исполнение, к модели активного участия подразделений ИБ в формировании бизнес-процессов и принятии ИТ-решений, предоставлении сервисов безопасности.

ПРО ВТБ

— Насколько успешно данные преобразования идут в ВТБ?

— С 2017 года в банке осуществляется активная технологическая трансформация, проведены два крупных присоединения (Банка Москвы и ВТБ24). Поэтому необходимо было не только обеспечить соответствие модели ИБ новым угрозам и новым форматам взаимодействия ИБ, ИТ и бизнеса, но и принять участие в непрестом

процессе присоединений и при этом не приостанавливать процесс цифровой трансформации банка. Уже несколько лет у нас нулевой уровень потерь от кибератак на банк и нулевое время простоя критических систем банка в результате кибератак. Несмотря на такой уникальный результат, совершенствование процессов информационной безопасности продолжается. Банк развивается, и ИБ вместе с ним. В настоящее время идёт активное формирование новых направлений и привлечение в команду ИБ как опытных квалифицированных специалистов, так и молодых и амбициозных, которым, я думаю, есть чему научиться в нашем коллективе.

ПРО АУТСОРСИНГ

— Последнее время много говорят об аутсорсинговой модели в ИБ. Как вы видите её перспективы?

— Считаю, что применение аутсорсинга ИБ для компаний, имеющих собственную ИТ-инфраструктуру, достаточно ограничено. Аутсорсинг эффективен при внедрении и настройке приобретаемых средств защиты, когда содержать соответствующих специалистов в штате невыгодно, так как нет постоянных задач, чтобы их загрузить полностью. Вторая область, где привлечение внешних специалистов является целесообразным, — это проведение тестов на проникновение, помощь в противодействии атакам, проведение расследований по взломам. Здесь вопрос уже не столько в загрузке, сколько в наличии необходимой практики, которой внутри даже большой организации не всегда достаточно. Аутсорсинг может также помочь, когда необходимо срочно выстроить процессы ИБ с «нуля», например, когда речь идёт об обработке инцидентов. Во всех других случаях, если речь идёт о достаточно крупной компании, дешевле и эффективнее взять специалистов ИБ в штат организации. Кроме чисто экономических соображений, необходимо учитывать недостаточность полномочий внешних сотрудников, наличие ограничений по доступу к коммерческой, банковской тайне, персональным данным, недостаточность знания внутренних процессов компании.

ПРО КАРАНТИН И УДАЛЁНКУ

— Несколько месяцев назад отраслевая общественность была уверена: после карантина мир ИБ серьёзно изменится, по крайней мере, не будет прежним. Откуда взялась такая уверенность?

— Я как раз не отношусь к этой части ответственности. Карантинные мероприятия и переход на удалённую работу не привели к появлению принципиально новых задач в части

информационных технологий и безопасности. И удалённая работа, и «безофисное» обслуживание клиентов не являются порождением COVID-19. Пандемия лишь форсировала те процессы, которые уже шли в финансовом секторе.

Последние десятилетия возможности информационных технологий и средств обеспечения безопасности меняются настолько быстро, что наблюдается существенный разрыв между этими возможностями и реальным их использованием. Если вернуться опять же к технологии электронной подписи на основе открытых ключей, то она появилась десятки лет назад. Но при этом при заключении договоров между организациями до настоящего времени преобладал бумажный документооборот. Или взять ежедневную миграцию в час пик офисных работников. Как правило, в компаниях уже используется электронный документооборот, коммуникации осуществляются через почту, мессенджеры, с помощью ВКС и по телефону, что позволило многие рабочие места перевести на удалённую работу. Также карантинные мероприятия дали дополнительный импульс расширению использования облачных сервисов.

Сложившаяся кризисная ситуация приводит к необходимости слома необоснованных ограничений и перехода на новый уровень взаимодействия и организации работы. Эпидемия выступила катализатором изменений: те изменения, которые назрели, закрепятся после пандемии, а те, которые не лежат в тренде, быстро забудутся по окончании, даже если карантинные ограничения затянутся ещё на много месяцев. То есть первопричина изменений — не коронавирус, а новые технологические возможности.

— Можно ли сделать вывод из ваших слов, что вы сторонник ликвидации офисов и перехода на удалённую работу?

— Не совсем так. Непосредственное общение тоже очень важно, особенно для формирования команды, понимания общих целей. Я за смешанную систему. Когда я работал над диссертацией в очной аспирантуре, у нас на кафедре была одна небольшая комната на 4 или 5 рабочих столов. Все 15 человек собирались только на семинар по четвергам во второй половине дня, который проходил в отдельной аудитории. В другое время присутствовало не более 2–3 человек, которые приезжали встретиться с научным руководителем, обсудить вопросы с коллегами, провести занятия со студентами.

Понятно, что бизнес во многих случаях подразумевает более тесное взаимодействие, чем научная работа, но и средства коммуникации за 30 лет значительно изменились. Я знаю компании, которые эффективно работают, притом что сотрудники

вообще никогда не встречались, они даже живут в разных государствах. Как часто бывает в жизни, в данном случае нет универсального решения, которое подходит для всех. Главное, не создавать самим себе искусственных ограничений, развиваться и максимально использовать имеющиеся возможности, в том числе технические.

О БУДУЩЕМ

— Полностью с вами согласен — мир действительно быстро меняется. А какие конкретно изменения в ИБ нас могут ожидать в ближайшем будущем?

— Делать прогнозы — занятие неблагодарное. Тем не менее, думаю, не ошибусь, если скажу, что возможности применения криптографических алгоритмов далеко не исчерпаны. Это не только шифрование, блокчейн и электронная подпись, но и другие направления, которые не на слуху. Если обеспечение ИБ сравнить с домом — это будет дом из мусора (нагромождение разнообразных элементов разной прочности, зачастую мало сочетающихся друг с другом, с множеством подпорок и щелями, заткнутыми паклей). Криптографические элементы в этом здании будут стальными балками — единственным, на что можно положиться, но не всегда они имеют под собой твёрдую опору. Чем больше их будет, тем прочнее здание безопасности.

Одним из узких мест обеспечения ИБ по-прежнему остаётся задача аутентификации пользователя. Я хочу подчеркнуть — не устройства, а пользователя на устройстве. Задача аутентификации устройства эффективно решается криптографическими методами, с пользователем сложнее. Пароли никогда не были надёжным и удобным средством, а в условиях сплошного видеонаблюдения и скученности, распространения шпионских программ риски компрометации только растут. Растёт также количество информационных ресурсов, которыми мы вынуждены пользоваться, требующих аутентификации.

Кардинально проблема аутентификации может быть решена только на основе неотчуждаемых характеристик пользователя. Здесь пути только два: использование имеющихся биометрических характеристик или вживание искусственных меток (надеюсь, сможем обойтись первым вариантом). Появление надёжного и удобного способа биометрической аутентификации на персональном устройстве было бы настоящим прорывом. При этом передавать биометрические данные за пределы устройства не обязательно, так как аутентифицировать устройства мы уже умеем.

Необходимо также решать проблему доверенной программно-аппаратной среды. Здесь могут



Дискуссия «Быстро, дёшево, безопасно — выбираем два пункта, или как построить процесс разработки программного обеспечения в современных условиях» в рамках XII Уральского форума «Информационная безопасность финансовой сферы»

быть различные варианты: создание специальной защищённой области (как в смартфонах Samsung), использование сим-карты в качестве доверенного вычислителя (такие работы ведутся рядом отечественных компаний). Или идти путём жёсткого ограничения возможности загрузки программного обеспечения на устройства (как это делает компания Apple).

Будет расширяться использование облачных платформ. В текущих условиях дефицита квалифицированных кадров по профилю ИТ и ИБ, высокой стоимости приобретения и эксплуатации средств защиты многие организации не могут обеспечить необходимый уровень киберустойчивости. Для них переход к использованию облачных платформ — меньшее из зол, даже при всех их недостатках. В использовании сторонних облачных решений заинтересованы даже крупные организации, масштабы которых позволяют создавать собственные корпоративные облака и вкладывать достаточно средств в обеспечение ИБ. Кстати, для физических лиц облачная революция уже практически завершилась — информация о наших счетах, недвижимости, наша переписка, наши рабочие документы, маршруты передвижения, штрафы, личные фотографии, медицинские анализы и история болезни и т.д. — всё это уже хранится на неподконтрольных нам облачных ресурсах.

Переход большей части малого и среднего бизнеса тормозится лишь ассортиментом соответствующего предложения и частично регуляторными ограничениями. Поэтому необходимо научиться решать технологические вопросы защиты информации внутри облака, развивать сервисы безопасности, а также обеспечить юридическую защищённость личных данных и данных компаний.

Последнее время открываются также новые возможности по использованию «больших данных». Во-первых, появились сами массивы данных, во-вторых, технические возможности их обработки. Соответственно, открылось множество областей для применения результатов обработки больших данных и технологий машинного обучения, в том числе в интересах ИБ.

Будет изменяться нормативное регулирование, управление отраслью, будет расти роль ИБ и углубляться взаимопроникновение ИТ, ИБ и бизнеса. Когда меня спрашивают, почему так выросла потребность в специалистах ИБ, я отвечаю: разве вы не видите, что всё больше профессий осваивают «роботы», а ИТ-специалисты и безопасники нужны, чтобы обслуживать роботов. Потом роботы научатся сами себя обслуживать, и останутся только безопасники, чтобы присматривать за роботами...

— Спасибо!

Вопросы задавал
Игорь Некрасов



Тимур АИТОВ
член Совета
по финансово-
промышленной
и инвестиционной
политике, заместитель
председателя
Комиссии
по цифровым
финансовым
технологиям ТПП РФ

ЗАПИСАЛИ В ЗЛОУМЫШЛЕННИКИ

МНЕНИЕ ЭКСПЕРТА И КЛИЕНТА В ОДНОМ ЛИЦЕ

Платёжные карты, эмитированные российскими банками, хакеры не любят. А за что их любить? Средний остаток по картсчетам меньше, чем у карт стран Евросоюза, ведь россияне — люди небогатые. От этого и дамы памяти скомпрометированных российских карт, которые продают на различного рода малинах, дешевле европейских.

Но есть и другие причины. Известно, что российские карты в большей степени защищены. Нынче все российские банки эмитируют карты на чипах. По этой причине всё, что связано со скиммингом, в России практически отсутствует. Что касается транзакций CNP (Card Not Present) — без присутствия карт, то и здесь в России перешли на визовскую технологию подтверждения интернет-платежей 3-D Secure — тоже практика, не всегда присутствующая в европейской части мира, а в Америке её вообще нет.

ДАННЫЕ ФИНЦЕРТА

Вот и выходит, что уровень мошеннических транзакций в Европе и Америке существенно выше, чем у нас. Это наглядно подтверждают данные свежего отчёта ФинЦЕРТ ЦБ за 2019 год. ФинЦЕРТ указывает, что доля объёма операций без согласия клиентов (то есть мошеннических) в общем объёме операций составляет 0,0023% при целевом показателе Центробанка в 0,005%. 0,005% — это половина «базового пункта», если за базовый пункт принять 0,01%. Напомним, в Европе уровень фрода в банкоматах составляет три-пять б.п., а в торгово-сервисных предприятиях он ещё выше. Все эти цифры радуют глаз, но это всё в среднем — в общем огромном объёме транзакций.

Ситуация становится не столь радужной, когда начинаем разбираться с системами ДБО и вообще с CNP-транзакциями.

В этом же отчёте ФинЦЕРТ отмечает, что основную долю операций без согласия клиентов физических лиц, увы, составляют CNP-транзакции. В общем числе фрод-операций их доля 65% (по объёму похищенного — 52%), на втором месте с 28% по числу и 39% по объёму идут хищения в системах ДБО физических лиц. Остатки — 7% по числу и 9% по объёму — приходятся на мошенничества с банкоматами и терминалами. Самое печальное в том, что при общем объёме

похищенного в системах ДБО в 2,2 млрд руб. клиентам вернулся только каждый 14-й рубль. Всё остальное осело в карманах злоумышленников.

ДВА ДНЯ: МНОГО ИЛИ МАЛО?

Конечно, это неприятно, и, конечно, банки знают об этом. Конечно, много раз специалисты ИБ в банках, видя подозрительные транзакции, стремились эти подозрительные транзакции задерживать, что называется, «до выяснения». Тема много раз обсуждалась в сообществе, банковские ассоциации много раз писали письма регулятору, но вот, наконец, свершилось — принят нормативный документ (ст. 8, 161-ФЗ в новой редакции), в соответствии с которым банк имеет право задерживать «подозрительные» платежи на срок до двух дней. Зачем? Ясно зачем — затем, чтобы подробнее разобраться с платежом, возможно, связаться с клиентом, со счёта которого эти деньги уходят.

Два дня — это большой срок, но на практике оказалось, что и его чаще всего недостаточно. В эти два дня часто бывает невозможно «достучаться» до клиента. Безопасник во многих банках, как правило, один, подозрительных транзакций несколько десятков в день, и дозвониться до каждого клиента просто нереально. То ли клиент в отпуске, то ли по другим причинам исчез, но его рабочий телефон молчит.

Как было раньше? Раньше платежи «молчунов» просто автоматически проводились, деньги уходили. Но теперь, сказав «а», приходится получить в ответ «б» — теперь все задержки сразу попадают на карандаш в ФинЦЕРТ, который следит за ситуацией аккуратно — собирает информацию, сколько платежей и каких пролежали эти два дня. И если платёж был задержан, а по нему ничего вразумительного банк не сообщил, то этот платёж сразу попадёт в разряд мошеннических — без какого-либо дальнейшего разбора.

Рабочая схема выстроена простая: получателю платежа (к примеру, банку Икс) приходит сообщение, что платёж банка-отправителя платежа (банка Игрек) потенциально мошеннический, потому что он проведён без согласия клиента. Как банк Икс, так и банк Игрек должны внести согласно указанию ЦБ сведения об участниках транзакции — как об отправителе платежа, так и его получателе — в свои фрод-базы.

Что происходит при такой схеме? Например, получатель платежа — нормальный средний клиент, и отправитель, до которого не дозвонились, тоже нормальный клиент. Но они оба сразу подпадают под подозрение ФинЦЕРТа. Оба банка — Икс и Игрек — должны поставить на контроль обоих клиентов за создание потенциальной мошеннической схемы. Незаметная скромная галочка в рабочем отчёте банка отправителя, пометившего подозрительную операцию по новым правилам, превращается в жирный крест мошеннической транзакции, поставленный в отчёте ФинЦЕРТа.

А дальше всё — процесс пошёл. В отношении банка идут наказания и оргвыводы, связанные с тем, что банк не соблюдает требований нормативов, имеет излишние объёмы фрода и так далее. Таких наказаний в арсенале регулятора много.

КТО ВИНОВАТ И ЧТО ДЕЛАТЬ?

Ситуация складывается неприятная. Кто виноват и что делать?

Конечно, виноваты во всём банки — они просили и получили желанную задержку. Но теперь, увы, не знают, что с этим делать.

Некоторые эксперты предлагают: хорошо, если бы времени на задержку дали ещё больше, но при этом разделить всех клиентов по категориям. Например, старому клиенту, которого «хорошо знаю», присвоить определённый уровень (код) и маркировать как надёжного. Если он всё время платил нормально, но по какой-то причине в данный момент отсутствует, то, естественно, считать его мошенником не нужно.

Но появляются нюансы, говорят уже другие эксперты. Если клиент — это большая компания, у неё каждый день возникают новые клиенты. Новые клиенты создают новые риски — они неизвестны для этого платежа, стало быть, риски этого платежа неизвестного клиента достаточно высоки. Поэтому от «свежего» клиента требуется, чтобы он хотя бы один раз подтвердил, что он не мошенник. Если же он всё же не успевает по каким-то причинам сделать это первое подтверждение, то действительно придётся записывать его в мошенники по сложившейся схеме. В результате получается, что мошенников значительно больше, чем на самом деле. Ну и фрод-транзакций, соответственно тоже.

НЕКОТОРЫЕ РАЗНОГЛАСИЯ

Банки приводят цифры своей статистики по фроду — они, конечно, более благоприятные, чем данные ФинЦЕРТа. Так, за год на каждых 200 клиентов приходится один мошеннический платёж — таково среднее мнение служб ИБ. Такой же статистики они ожидают от ЦБ. По

факту же в отчёте ФинЦЕРТ цифры мошенничества получаются значительно выше. А раз так, значит, банки постоянно обманывают ЦБ и что-то скрывают.

Как поступить с этой деликатной ситуацией, пока никто до конца не знает. Но смягчить жёсткие меры безопасности от ЦБ хочется всем.

ВОЗМОЖНЫЙ ПУТЬ

Тема ИБ постоянно волнует не только банкиров. Один из возможных путей появился, когда мы обсуждали в Общественной палате вопросы безопасности ПО и ответственности за его небезопасность. Речь шла о любом ПО — и в системе органов госуправления, и на объектах критической инфраструктуры. По мнению многих экспертов, основная проблема не в активности и изворотливости хакеров, а в ошибках и уязвимостях, допущенных самими разработчиками ПО.

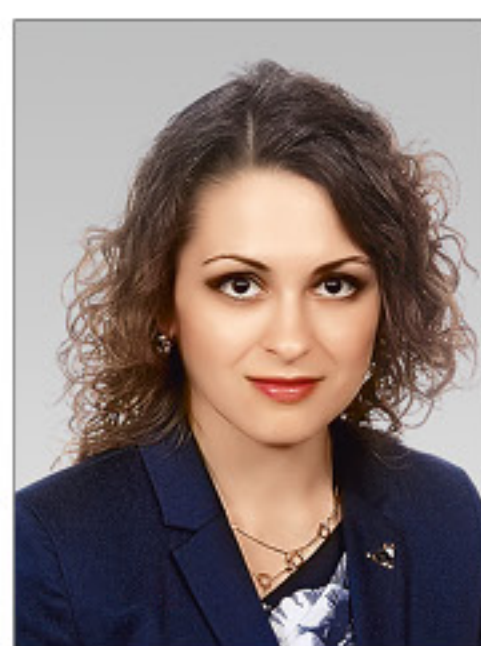
Продавать продукты научились, но тестировать не привыкли, говорили многие. Это понятно — тестировать дорого, да и за исправление ошибок банк заплатит ещё раз. Пришли к тому, что надо менять нынешнюю систему ответственности банка за фрод. Сегодня как? Банк отвечает своими средствами за фрод и поэтому всякий раз обвиняет клиента в нарушении его обязанностей — это пропустил, за тем недоглядел. Правильнее же, чтобы система ответственности была другая: банк отвечает только в том случае, если выстроенная система ИБ не подтверждена третьей стороной, которая обеспечивает безопасность платежей.

* * *

То есть если я — система безопасности — не подтверждена, виноват банк, а если подтверждена, то извольте вам лайабилити шифт — перенос ответственности. Схема должна быть такой: сертифицировался банк, обеспечил необходимый уровень безопасности, при обработке транзакции не нарушил регламентов — тогда однозначно виноват клиент, не сертифицировался, что-то важное нарушил — тогда вина банка. Таков современный риск-ориентированный подход в управлении событиями ИБ.

Принять этот подход или нет в будущем — прерогатива ЦБ. Будем надеяться, что именно так дальше и будет. Тогда банкам не придётся тратить на ИБ средства, несоизмеримые с потенциальными потерями. Ну а мы, банковские клиенты, будем чувствовать себя спокойнее и увереннее. Всегда приятно, когда злоумышленников становится меньше. И вдвойне приятно, когда тебя самого в эти злоумышленники не записывают.

И ЗАВЕДИТЕ КЛОНА...



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

Использовать защищаемые данные для целей тестирования — нельзя, или когда-то всё-таки можно?

ЧТО ТРЕБУЕТ РЕГУЛЯТОР

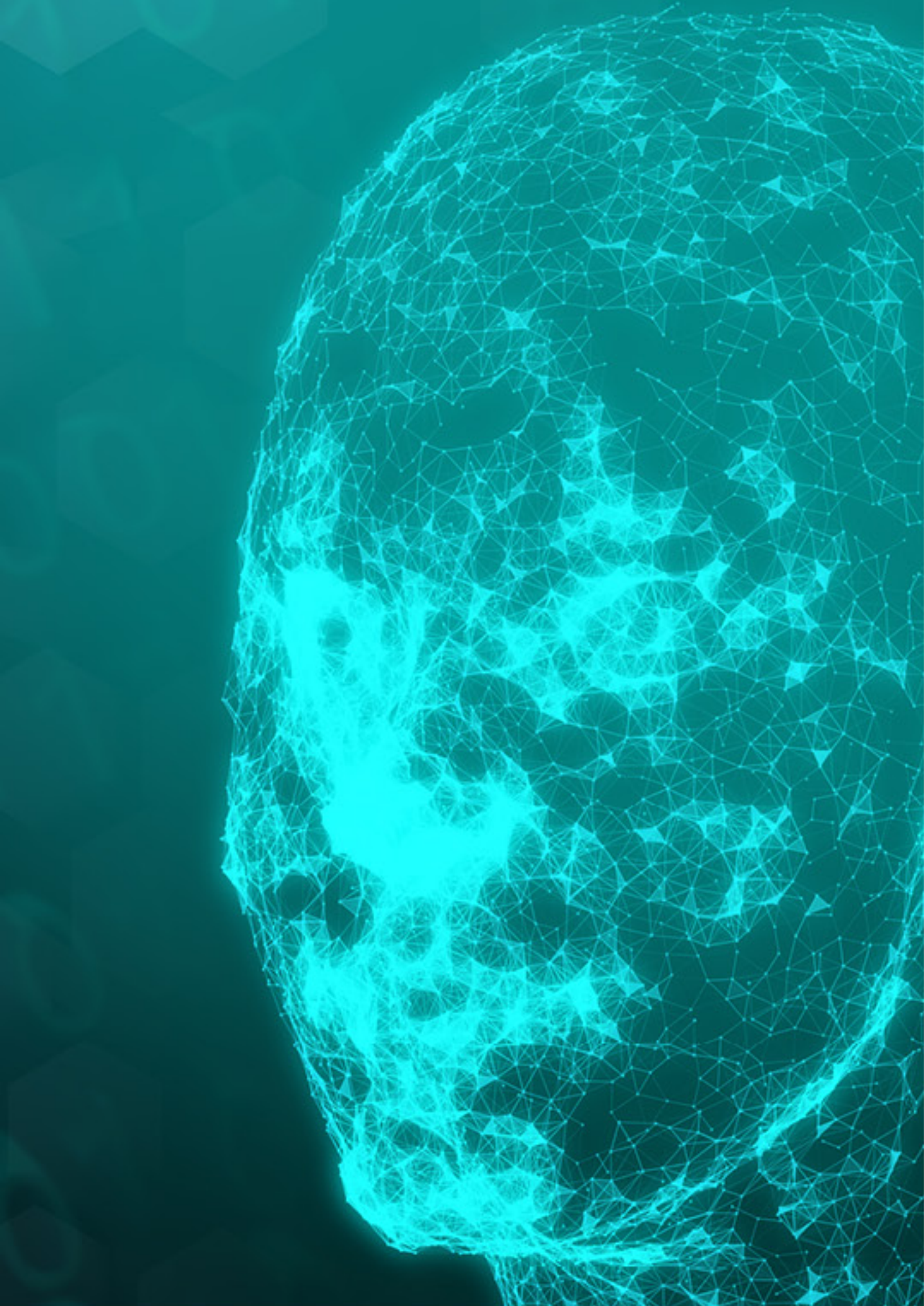
Центральный банк в своём ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», действующем с 1 января 2018 года, выдвигает следующие базовые требования.

В вычислительной сети финансовой организации должен быть выделен отдельный сегмент или группа сегментов, предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и (или) модернизации автоматизированной системы (далее — АС), в т.ч. тестирования программного обеспечения и средств вычислительной техники. Сетевое взаимодействие с иными

сегментами по инициативе сегмента разработки и тестирования должно быть исключено (раздел 7.3.1.2, пункты СМЭ.6, СМЭ.7).

При этом использование защищаемой информации в сегментах разработки и тестирования запрещается, за исключением случаев, когда речь идёт о конфигурационной информации, определяющей параметры работы АС (раздел 9.5, пункт ЖЦ.7).

Данные требования актуальны в том числе для контуров безопасности в области действия Положения 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» (Положение № 683-П), поскольку оно ссылается на ГОСТ Р 57580.1–2017. С 2023 года, видимо, будут актуальны и для Положения 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» (Положение № 382-П), если проект очередной его редакции, также содержащий отсылку к ГОСТ Р 57580.1–2017, не претерпит каких-то кардинальных изменений.

ЧТО МОЖНО НЕ ДЕЛАТЬ?

Популярная, но некорректная постановка вопроса. Правильнее говорить о том, когда и что именно делать нужно, потому как не каждое «попробовать» — это тестирование, к которому предъявляются приведённые выше требования.

Решающую роль при этом играет статус системы, в которой необходимо определить возможность использования защищаемых данных и решить проблему размещения в том или ином сегменте сети организации.

КОГДА РЕЧЬ ИДЁТ ДЕЙСТВИТЕЛЬНО О ТЕСТИРОВАНИИ?

Если АС не принята в промышленную эксплуатацию, для неё не проведены приёмосдаточные испытания, не подтверждено соответствие реализованного функционала заявленному изначально, например, в техническом задании, такая АС с формальной точки зрения непредсказуема, и допускать её взаимодействие с промышленным сегментом организации нельзя, поскольку это может привести к нарушению работы других систем, искажению и утечке защищаемых данных, особенно если работы по созданию и (или) доработке рассматриваемой АС проводятся с привлечением сторонних организаций. Это как раз тот случай, когда организация должна быть заинтересована в выполнении требования регулятора. Отказываться от этого ограничения можно только в крайнем случае, идентифицировав, оценив и соответствующим образом приняв все риски и возможные последствия.

Прежде чем принимать такое решение, необходимо в т.ч. просчитать трудоёмкость и стоимость мероприятий по созданию тестовых данных, например, путём обезличивания или перемешивания защищаемых данных, не ограничиваясь при этом качественной экспертной оценкой («долго», «сложно», «невозможно» — далеко не всегда это действительно так, если разобраться).

КОГДА РЕЧЬ ИДЁТ О ДИАГНОСТИКЕ И ТРЕБОВАНИЯ РЕГУЛЯТОРА НЕПРИМЕНИМЫ?

Если же АС прошла испытания и введена в промышленную эксплуатацию, то тестировать в ней, вероятнее всего, уже нечего, она не находится в процессе разработки, и указанные требования регулятора здесь вряд ли применимы. Скорее речь идёт о диагностике, когда, смоделировав ту или иную ситуацию, можно выявить причину сбоя или некорректного функционирования. В таком случае действительно важно как можно точнее воспроизвести «контекст» промышленной системы, в том числе использовать такие же обрабатываемые данные. Для этого целесообразно иметь «клон» диагностируемой системы, размещать её в том же сегменте, защищать, как и любую другую промышленную систему данного контура безопасности.



**Василий
ОКУЛЕССКИЙ**

эксперт BIS Journal,
кандидат технических
наук

«УДАЛЁНКА» КАК КЕЙС

ПРО КУСОЧЕК ВЕТЧИНЫ ДАЖЕ В САМОМ БОЛЬШОМ СВИНСТВЕ

Вот уже почти три месяца мы живём в «новой» реальности. Кто в одиночестве сидит в офисе и пытается работать шестнадцатью руками. Кто удалённо борется с сетью/связью и работает работу, как получается. Кто сидит в изоляции и ждёт не дожждётся хоть какой-нибудь работы.

В общем, жизнь течёт. Вирус продолжает нас пугать своей стабильностью, но жизнь всё-таки продолжается.

Ситуация подкинула много разных новых проблем с массовым удалённым доступом — «удалёнкой». Простое перечисление составит добрую статью — переход многих сотрудников на личные устройства, про безопасность которых можно только гадать, коллективное использование их разными пользователями — мужья, жёны, дети, каждый со своим набором приложений, а главное, конфликт использования — «кто сейчас»; массовое использование «тёмных» мессенджеров для делового общения, массовое использование непроверенных и недоверенных средств аудио/видеообщения, резкий всплеск мошенничества-социнженерии, всплеск атак по удалённым каналам...

Стало хорошим тоном говорить и писать о цифровизации, новых технологиях, которые спасут мир, а я, глядя на всё это, вспоминаю про бардак и автоматизацию и всё больше и больше убеждаюсь в старой истине — сначала нужен порядок, а потом уже автоматизация. О чём это я? Давайте попробуем оценить объективно (как у кого получится): чему нас учит / научил / не научил этот так называемый кейс.

В одночасье в совершенно невоенной обстановке нас как-то вынесло к проблеме, что на рабочих местах нас должно меньше быть, а бизнес при этом во всех своих проявлениях должен продолжать функционировать. Первое очевидное движение — максимально всех на «удалёнку». И что тут началось. Не хватает... Не хватает... Не хватает... забыли... не знали... не думали... а я думал по-другому... а где это написано?.. я за это не отвечаю... Знакомая картина? Потом всё как-то устаканилось и вроде бы стало даже хорошо.

Я не хочу рассуждать о том, что, может, кто-то и вовсе с «удалёнки» не вернётся, что надо в принципе пересматривать подход к организации деятельности — сейчас это популярный тренд (хайп?). Поговорим о классике. Поговорим о бумажной составляющей и информационной безопасности тоже.

Point 1. Мы не всегда точно и исчерпывающе знаем своё место в общей структуре бизнеса. И здесь собственно ибэшники в лучшем положении, чем многие другие — они постоянно доказывают, что они нужны.

Point 2. Часто, что делать в стрессовой ситуации, мы узнаём как-то мимоходом, по ситуации.

Вернёмся к анализу причин такого результата.

Анализ выполнения всех основных и вспомогательных бизнес-процессов на основе результатов анализа и определения функциональных ролей, их потенциальной загрузки, возможности совмещения отдельных ролей между собой, выделения групп ролей, запрещённых к совмещению с другими ролями. В результате возможна даже корректировка оргштатной структуры для оптимального распределения функциональных ролей между фактическими исполнителями.

Этот шаг обычно выполняют при подготовке внедрения системы управления правами пользователей. Типичной ошибкой/недоработкой этого этапа обычно бывает игнорирование/забывание вспомогательных и обеспечивающих функций/ролей, без которых немыслима работа «основных».

Удалённая работа показала, что во многих организациях, не только банковских, этот этап выполнен несколько формально, в результате чего остались части бизнес-процессов или обеспечивающих без исполнителей либо, наоборот, возникло дублирование одних и тех же функций в разных подразделениях. Особенно это явно заметно на стыках процессов ИТ и ИБ (настройка сети, её сегментирование, работа антивирусных средств, настройка и сопровождение МСЭ и подобных мест). Пока мы все рядом, эти нестыковки решаются сами собой при личном контакте, при удалённом взаимодействии так получается не всегда.

Следующий важный момент — наделение каждой функциональной роли необходимыми, но не излишними правами. Здесь очень важна строгая формализация этого процесса. При удалённой работе очень часто возникают ситуации срочной подмены или что-то похожее (заболел, нет связи, нет электричества, нет возможности восстановить технические средства и т.д.), и без формализации быстро сделать подмену очень непросто, в результате может пострадать основной бизнес-процесс.

К этим шагам вплотную примыкают вопросы документирования процессов, выполнения операций и отдельных действий, лёгкости восприятия этих документов, их читабельности и доступности. Только при правильном документировании процессов мы всегда, даже в самой стрессовой ситуации, сможем обеспечить своевременную замену/подмену участников процессов.

К таким процессам, безусловно, относятся два сильно привязанных к коронавирусу — предоставление удалённого доступа и перевод деятельности на резервные площадки. Недавний процесс перехода на «удалёнку» ясно показал, что там, где эти процессы были по шагам прописаны и отрепетированы, переход состоялся чётко и организованно, в минимальные сроки, где этого не было сделано заранее, там «бестолковость» долго не давала нормально начать работать по-новому.

Всё, о чём я написал выше, очевидные вещи, но самое благодарное — это доказывать очевидное. Пусть противники «бумажных» технологий продолжают поливать позором и нехорошими словами бумажные документы, но именно они до сих пор являются основой воспроизводимости и одинаковости выполнения процессов. Конечно, техническую безопасность никто не отменял, проверку уязвимостей — тем более, но в критических условиях надо понимать, что происходит, кто что делает, и уметь контролировать все эти действия.

Тут я услышал фразу, что хорошо прописанный и, главное, отрепетированный План Б становится просто одним из разделов Плана А.

Интересно, что правильно проведённая работа по выделению функций, ролей и формированию системы управления правами доступа имеет массу положительных побочных эффектов. Бизнес, оргштатная структура, система внутренних взаимоотношений, как горизонтальных, так и вертикальных связей становятся прозрачными, а значит, более эффективными и управляемыми становятся процессы, что в итоге снижает накладные расходы бизнеса.



Вторым следствием такой работы становится облегчение процесса автоматизации управления персоналом и правами доступа персонала, а значит, облегчает жизнь подразделениям информатизации.

К сожалению, это тот случай, когда надо было готовиться заранее. Теперь этот опыт можно применить только в будущем.

Какие уроки ещё можно извлечь из последних трёх месяцев?

Для меня и многих моих коллег ещё раз подтвердился тезис — не надо защищать информацию саму по себе, это бессмысленно, надо защищать БИЗНЕС и информацию как неотъемлемую часть его. Надо защищать доступность/непрерывность сервисов, поддерживать приемлемое качество услуг, при этом безопасность должна стать органической частью качества.

* * *

Друзья мои! Детально изучайте и документируйте свою деятельность. Тренируйтесь работать даже при самых невероятных предпосылках, повышайте свою стрессоустойчивость, находите кусочек ветчины даже в самом большом свинстве.

Июнь, 2020

«МЕНЯЙТЕ ВАШИ МНЕНИЯ, СОХРАНЯЙТЕ ВАШИ ПРИНЦИПЫ; МЕНЯЙТЕ ЛИСТЬЯ, СОХРАНЯЙТЕ КОРНИ»

КОРОТКОЕ ЭССЕ О КУСОЧКЕ ВЕТЧИНЫ В САМОМ БОЛЬШОМ СВИНСТВЕ



Сергей ВИХОРЕВ
советник
генерального
директора
ООО «ИТ-
Экспертиза»

Коронавирус, удалёнка при общении в мессенджерах научили краткости и концентрации мысли. Поэтому начну сразу, без предисловий, взяв, так сказать, быка за рога. А статья-то — актуальная. И тема про «новую реальность» — важна. Мне особенно импонирует тезис в самом конце о необходимости поиска кусочка ветчины даже в самом большом свинстве. Но об этом чуть позже. А сейчас вот о чём.

Как всегда, есть некое «но», которое позволяет взглянуть на проблему с другой стороны. О чём это я? А о выводе автора о том, что «не надо защищать информацию саму по себе, надо защищать бизнес», и далее: «Надо защищать доступность, непрерывность сервисов, поддерживать приемлемое качество услуг». Вроде бы всё правильно, но, на мой взгляд, акценты расставлены не совсем точно. Здесь проходит очень тонкая грань между темой обеспечения безопасности информации и обеспечения непрерывности бизнеса. Это два важных, соприкасающихся процесса, но это не одно и то же.

Да, важность защиты бизнеса как главная цель не обсуждается. И то, что информационная безопасность — только обеспечивающий вид, — тоже. Но для защиты бизнеса работают множество обеспечивающих структур: и физическая охрана, и структуры жизнеобеспечения, и общепит, и ещё много чего. Что из них важнее? Да все нужны! Как говорил великий классик: «Мамы всякие нужны, мамы всякие важны!» И если хотя бы одно звено не сработает — бизнеса не будет. Да, охрана защищает топ-менеджеров, а спецы от ИБ — ту информацию, которая важна для бизнеса.

Но информационная безопасность — это далеко не непрерывность бизнеса. И методы у них разные, и компетенции должны быть разные. Нельзя вешать все проблемы только на спецов от ИБ. «Беда, коль пироги начнёт печи сапожник, А сапоги тачать пирожник, И дело не пойдёт на лад¹...» (сколько же мудрости в русском эпосе!). Непрерывность бизнеса — это ближе к компетенции ИТ-специалистов, не ИБ-шников. А у этих

специалистов, как известно, патологическая неприязнь друг к другу. Для ИБ-шника лучшая информационная система та, которая отключена от электропитания и заперта в подвале на ключ. А для айтишника — когда все имеют доступ ко всему. Найти баланс между этими крайними точками сложно, но нужно. Хотя нельзя отрицать, что некоторые аспекты, например доступность информации, затрагивает и ту, и другую область. Но это говорит лишь о том, что должны быть слаженные, скоординированные действия двух служб, а не возложение обязанностей на какую-то одну. Поэтому здесь две проблемы: доступность сервисов и услуг — это к ИТ-специалистам, а доступность информации (ресурса) — к ИБ-специалистам. Только разделив роли, мы сможем добиться максимального эффекта. И это особенно актуально именно в период пандемии. Должно быть налажено очень чёткое взаимодействие. И вот тут мы переходим к тезису о кусочке ветчины.

Категорически не могу не согласиться с автором в том, что необходимо документировать процессы, необходимые для обеспечения деятельности бизнеса (именно бизнеса, а не информационной безопасности!). Да. Это помогает не только ИБ- и ИТ-спецам, но, главное, самому бизнесу, позволяет правильно структурировать деятельность. И это не потому, что я апологет «бумажной» безопасности (хотя это совсем и не безопасность, а область организации бизнеса!), а так требует жизнь. Если процесс правильно описан, отрепетирован и каждый участник процесса знает свой шесток, можно быть уверенным, что даже в самой критической ситуации, к которой можно отнести и переход на удалёнку в период коронавируса, интересы бизнеса не пострадают.

Истина всегда одна, а правда у каждого своя. Истину знает только Отче наш Иисус Христос, а мы все смертные. Можем только высказывать свою правду (или мнение?). А насколько эта правда близка к истине — решать вам, читатель, в силу своего разумения...

Р. С. А вы не обратили внимание на то, что стандарты по информационной безопасности и стандарты по непрерывности бизнеса находятся в разных классификационных группах?

¹ И. А. Крылов, «Щука и кот».

НОВЫЙ ИМПУЛЬС ИЛИ ДЕЗОРГАНИЗАЦИЯ?

ПЕРЕХОД НА УДАЛЁНКУ СТАВИТ ВОПРОСЫ
ГОСУДАРСТВЕННОГО МАСШТАБА



Тимур АИТОВ
член Совета
по финансово-
промышленной
и инвестиционной
политике,
заместитель
председателя
Комиссии
по цифровым
финансовым
технологиям
ТПП РФ

Тема организации удалённой работы банка сегодня актуальна, о ней многие пишут, многие рассказывают, но не всем удаётся рассказать и написать об этом занимательно и популярно и вместе с тем сохранить необходимую строгость и конкретность. Здесь как раз именно тот удачный случай, когда специалист в сфере ИБ (!) акkuratно, тонко и с юмором повествует обо всех основных проблемах. Ключевая мысль публикации в том, что проще переводить на удалёнку банк, в котором прописаны все регламенты, а там, где царит хаос, это сделать сложно — с этим спорить не будем.

Конечно, переводить нужно не всех сотрудников банков. В число запланированных «на удаление» вряд ли войдут сотрудники, которые обслуживают АРМ КБР, на рабочем месте придётся оставить и тех, кто управляет самой работой «удалёнщиков». Для перехода потребуется новый регламент — положение, устанавливающее, кого из сотрудников можно, а кого не следует отправлять на удалённую работу. Документ должен существовать в банке заранее, до проведения всех масштабных трансформаций.

Вспоминаю «Аэрофлот», который ещё пять лет назад, задолго до истории с пандемией, планировал перевод на удалёнку части своих сотрудников в Шереметьеве. В компании крупнейшего авиаперевозчика тогда разработали аж четыре документа — два обстоятельных положения и две методики для организации этого перехода. Любопытно, что многие сотрудники «Аэрофлота» тогда легко соглашались на дистанционную работу, несмотря даже на планируемое снижение зарплат «удалёнщиков» на 10–15%. Экономия собственно времени оказалась для многих более ценным подарком.

Обсуждая проблемы перехода, можно было бы, наверное, пофилософствовать на темы того, что цифровой мир более требователен к

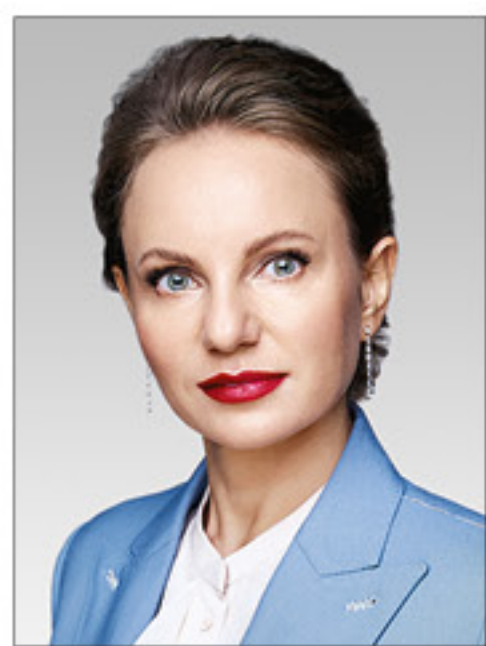
правильной организованности процессов, чем мир аналоговый. Или провести и другие параллели, например, о том, что мир дистанционной работы также более требователен к формализации бизнес-процессов, чем мир очного присутствия. Аналоговый мир (как и очный) допускает большую многовариантность и менее формализован — в одной и той же ситуации можно поступить так, а можно этак, а результат всё равно будет одинаковым. Цифровой же мир более детерминирован, он оставляет меньше пространства для маневра. С другой стороны, жёсткость цифрового мира обуславливает его большую хрупкость. И если в цифровой транзакции что-то пошло не так, она, скорее всего, не состоится. Зато в аналоговом мире транзакции гораздо более устойчивы к помехам.

Так что прощаться с аналоговым (и очным) миром не всегда будет просто.

Очевидно, что сам по себе переход на удалёнку имеет мало отношения к трансформации процессов аналоговой экономики. Скорее всего, это только создание цифровых копий (слепков) существующих реальных процессов, как, например, это делает цифровой сканер с аналоговой фотографией. Но потенциал и новые стимулы для движения вперёд к цифре, конечно, появляются.

* * *

Можно ли и нужно ли перемещать мозговые центры управления банками (или всей страной?) в регионы с меньшими зарплатами? Почему руководители крупных банков федерального значения должны обязательно жить в Москве? На эти и другие подобные вопросы акционеры банков должны сегодня иметь конкретные ответы. Организация удалённой работы — дело непростое для любого банка. Удалёнка может придать импульс в работе, а может и дезорганизовать всю его работу. Пожелаем банкам в этом успехов!



Татьяна ЖАРКОВА
генеральный
директор
Ассоциации ФинТех

ИГРА В ОТКРЫТУЮ. ВЫИГРЫВАЮТ ВСЕ!

ОТКРЫТЫЙ БАНКИНГ И ДАННЫЕ КЛИЕНТА:
БЕЗОПАСНОСТЬ — НА ПЕРВОМ МЕСТЕ

Приставка open (рус. «открытый») уже стала привычной, когда мы говорим о развитии сферы финансовых услуг: открытые данные, открытые API, открытый банкинг, открытое страхование и т.д. Трансформация финансовой системы обусловлена стремительным развитием технологий и меняющимися потребностями клиентов. Всё чаще решения о финансовых операциях принимают миллениалы — поколение, которое выросло со смартфоном в руках и привыкло к мгновенным результатам, быстрым операциям, «бесшовному» опыту: они хотят всё и сразу и не хотят зависеть от одного поставщика

или банка. Поэтому рынок банковских услуг превращается в маркетплейс, где клиенты набирают себе в «корзину» финансовые услуги независимо от того, кто их предоставляет — банки или небанковские организации. Ради лояльности клиентов и расширения собственных возможностей кредитные организации по всему миру активно внедряют концепцию открытого банкинга с помощью технологии открытых API (application programming interfaces — интерфейсы, позволяющие сторонним разработчикам интегрироваться с информационными системами банков и использовать данные клиентов с их согласия).

OPEN BANKING

ВОКРУГ СВЕТА

Согласно новому исследованию компании Tink (европейской платформы, которая объединяет 2,5 тыс. банков и финансовых организаций), в 2020 году доля тех, кто позитивно относится к открытому банкингу в Европе, составила 61 %. Кроме того, банки всё больше понимают важность взаимодействия с финтехами. По результатам опроса каждый пятый респондент (22 %) сотрудничает по крайней мере с одной финтех-компанией, а некоторые имеют до пяти таких партнёров. И чем активней развиваются технологии, тем больше становится совместных проектов. Так, за 2019 год большинство (69 %) европейских банков нарастили сотрудничество с финтехами, и ещё столько же указали развитие совместных решений среди приоритетных задач на следующий год.

Сейчас преимущества открытого банкинга и внедрения технологии открытых API, такие как увеличение числа сервисов и приложений, расширение клиентской базы, рост удобства и снижение затрат, банки уже распробовали.

Финансовые и нефинансовые организации всё чаще обмениваются технологиями, открывают доступ к своим системам и данным. И теперь во всём мире на первое место выходит вопрос обеспечения безопасности персональных данных клиентов.

Так, в Австралии с начала февраля вступили в силу правила работы с информацией клиентов (Consumer data rights, CDR) — они формализуют стандарты открытых банковских данных. В пилотном проекте участвовало четыре крупнейших кредитных организации страны, и с 1 июля 2020 года все банки обязаны сообщать клиенту, какую персональную информацию о нём они хранят, и давать право с его согласия передавать её третьим лицам.

Правительство Канады весной 2020 года приступило ко второму этапу реализации концепции открытого банкинга, и особое внимание уделяется обеспечению безопасности клиентских данных. Консультативный комитет по открытому банкингу (Advisory Committee on Open Banking) привлечёт заинтересованные стороны, чтобы разработать рекомендации

для улучшения защиты данных, изучить вопросы управления, контроля личных данных потребителей, конфиденциальности и безопасности.

В России открытый банкинг и технология открытых API также являются перспективным направлением развития сферы финансовых услуг. Согласно исследованию E&Y, 99,5 % наших граждан если не пользуются постоянно, то как минимум осведомлены о финтех-сервисах для денежных переводов и различных видов платежей. Над внедрением открытых API работают все ключевые игроки финансового рынка — регулятор, финтех-компании, небанковские организации и, конечно, сами банки, причём как самостоятельно, так и объединив усилия на площадке Ассоциации ФинТех (АФТ).

ЗАЧЕМ ПЕРЕДАВАТЬ СВОИ ДАННЫЕ

Ради комфорта и экономии времени клиент передаёт банковским или небанковским организациям часть работы со своими финансами и для этого предоставляет им необходимую информацию: Ф. И. О., номера счетов, список транзакций по счетам, остатки на счетах и др. Организации хранят эти данные и при необходимости обновляют, обмениваются, разрабатывают на их основе новые финансовые сервисы и приложения, формируют выгодные персональные предложения, используют для аутентификации. Как это происходит на практике?

Ассоциация ФинТех совместно с несколькими банками инициировала пилотный проект «Кредитование юридических лиц». Технически в процессе участвуют три стороны: первая — юридическое лицо, вторая — банк, в котором это лицо обслуживается, и третья — банк, в котором юрлицо хочет взять кредит.

Клиент заходит на сайт банка-кредитора, заполняет анкету и на шаге предоставления выписки по счёту выбирает из списка свой банк, который ведёт его расчётно-кассовое обслуживание (РКО), и нажимает кнопку «Дать согласие». Система перенаправляет клиента на сайт его банка, где он даёт своё согласие на предоставление выписки банку-кредитору на определённый срок, например, 1 месяц. Чтобы получить выписку, банк-кредитор сам запрашивает

данные в банке клиента, предъявляет согласие на доступ к информации, а банк клиента это согласие проверяет и выдаёт необходимые данные.

Таким образом, для клиента значительно сокращается алгоритм действий: ему не нужно идти в банк, распечатывать документы, ставить печать, не нужно даже заходить в интернет-банк и заказывать выписку в формате PDF.

В настоящее время разрабатывается несколько вариантов взаимодействия клиента с банком, в частности, возможность выдавать долгосрочное и краткосрочное согласие. При краткосрочном согласии клиент будет выдавать разрешение на использование данных для совершения только одной операции. При долгосрочном согласии — на полгода или год — клиент даст право сервисам, например, PFM (Personal Financial Management, рус. управление личными финансами), «заходить» в его банки с помощью открытых API и собирать всю необходимую для оказания услуг информацию.

Совместный пилотный проект предполагает, что клиент в режиме реального времени сможет контролировать и управлять доступом к своим данным: на сайте или в приложении своего банка он сможет посмотреть полный перечень организаций, которым выдавал согласие, с указанием, когда, кому и в каком объёме. Также клиент сможет отозвать ранее выданное согласие. И здесь возникает интересный момент: как гарантировать, что банк удалит уже полученные данные, и нужно ли это делать? Сейчас вокруг этого вопроса идёт дискуссия как в России, так и за рубежом.

КТО ОТВЕЧАЕТ ЗА СОХРАННОСТЬ ДАННЫХ?

Если учесть, что банки будут делиться информацией о своих клиентах с другими участниками среды открытых API, то и ответственность за обработку и передачу персональных данных и банковской тайны ложится на каждого — как на банки, так и на финтехи. Согласно «Концепции открытых API», разработанной на площадке Ассоциации ФинТех, право использовать данные получают только аккредитованные участники, при этом процедура аккредитации не должна создавать избыточные барьеры.

Чтобы финтех-компания, даже небольшая, получила право доступа к открытым API банков, она должна соответствовать определённым требованиям: техническим, то есть требованиям информационной безопасности, юридическим (чистота этой компании) и экономическим. Если финтех соответствует всем вышеперечисленным требованиям, ему выдаются

Согласно «Концепции открытых API», разработанной на площадке Ассоциации ФинТех, право использовать данные получают только аккредитованные участники

электронный сертификат и ключ, с помощью которых компания сможет обращаться к открытым API банков.

ДАННЫЕ И ЗАКОН

В России работу с персональными данными регламентируют Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006 года и Гражданский кодекс (статья о банковской тайне, её защите и передаче). Они обязательны для исполнения всеми компаниями, зарегистрированными в России, а также филиалами иностранных организаций.

Законы, акты и нормативы постоянно дорабатываются с учётом трансформации финансовой системы и появления новых технологий. Так, за последнее время вступил в силу Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»; принят ГОСТ «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций»; доработана нормативная база для работы с Единой биометрической системой; приняты поправки в Положение Банка России 382-П (о требованиях к обеспечению защиты информации при переводах денежных средств). И регулятор продолжает обновлять правовую базу и повышать информационную и цифровую безопасность финансового рынка.

Что касается стандартов и механизмов внедрения открытых API, они прорабатываются на площадке Ассоциации ФинТех совместно с ключевыми игроками российского финансового рынка. В августе 2019 года Наблюдательный совет АФТ одобрил «Концепцию открытых API», особое внимание в которой уделено вопросам информационной безопасности и аккредитации участников. В частности, сейчас на рассмотрении Банка России находится стандарт информационной безопасности открытых API.

КАК ДОСТУП К ДАННЫМ ОСУЩЕСТВЛЯЕТСЯ СЕЙЧАС

Пока из-за отсутствия регулирования, единых правил и стандартов обмена данными банки и финтехи вынуждены использовать технологию скринскрапинга (англ. screen scraping). Скринскрапинг — это сбор в автоматическом режиме информации, в том числе данных пользователей сайтов и приложений. Специальные программы эмулируют (то есть имитируют с помощью программных средств) работу пользователя в приложениях и собирают клиентские данные, включая историю операций и транзакций.

Такой подход подразумевает, что клиент оставляет свои авторизационные данные разработчику сервиса, использующего скринскрапинг,

Чтобы финтех-компания получила право доступа к открытым API банков, она должна соответствовать определённым требованиям: техническим, юридическим и экономическим

и не контролирует дальнейшее распространение и использование данных, надеясь лишь на порядочность разработчиков приложения и других участников финансовых процессов. Конечно, одного логина и пароля от вашего личного кабинета недостаточно, чтобы совершить транзакцию или операцию (как правило, для этого нужна двойная аутентификация — такая как СМС-код или push-уведомление), но достаточно, чтобы посмотреть все связанные аккаунты, историю и объём транзакций, наличие валютных счетов, задолженности, периодичность и суммы платежей и многое другое. Все эти данные используются, например, чтобы узнать кредитоспособность клиента или подобрать персональное предложение — при этом сам клиент не будет знать, что его данные были использованы. Встречаются случаи, когда юридические лица добровольно и осознанно предоставляют доступ к финансовой информации для упрощения ведения бухгалтерии и отчётности, тем не менее никто не отвечает за её сохранность.

Безопасное хранение и обмен данными при скринскрапинге обеспечить невозможно, в том числе из-за отсутствия единых требований безопасности или SLA (англ. service level agreement, рус. соглашение об уровне сервиса). SLA — это мини-договор между компаниями, который устанавливает параметры качества ИТ-услуг. А так как скринскрапинг подразумевает негласный сбор данных, то никакого договора и взаимной ответственности между источником информации и её конечным пользователем не существует.

* * *

И это как раз принципиальное отличие от открытого банкинга, где участники рынка делятся информацией осознанно, в заранее установленном объёме, с согласия клиента и в условиях обеспечения информационной безопасности. При этом все участники среды открытого банкинга берут на себя ответственность за использование и обмен данными клиентов. В итоге в «игре в открытую» выигрывают все: и конечные пользователи, и банки, и финансовая отрасль в целом.



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

НАШЕСТВИЕ МАЛЕНЬКИХ КОНТЕЙНЕРОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СТАЛКИВАЕТСЯ С НОВЫМ КЛАССОМ ВЫЗОВОВ

За последние 3–4 года «частные облака» полноценно пришли в технологические ландшафты организаций. Вместо «тяжёлых» гипервизоров и систем оркестрации их виртуализации реальностью стала волна «контейнеров» — сотен, тысяч и десятков тысяч небольших и «лёгких» виртуализированных машин.

Контейнеры работают по принципу «ничего лишнего» и используют специализированные операционные системы (например, облегчённую версию Linux — Core OS), а их жизненный цикл составляет часы-дни. Традиционные меры ИБ к ним применимы плохо. Например, антивирус внутри контейнера поместить невозможно.

«Контейнерное цунами» по времени совпало с цифровой трансформацией, когда свеженанятые команды разработки стали приносить инструменты с собой и оповещать о них безопасников постфактум.

В итоге в сетях организаций вместо мощных континентов (мейнфреймов) и крупных островов (виртуальных машин) появляются десятки тысяч «островков», которые постоянно появляются и исчезают и на которых обрабатываются чувствительные данные частями бизнес-приложений. Если нет дружбы безопасности с разработчиками, то безопасность и не знает, когда контейнеры появляются, и организация снова откатывается в каменный век безопасности, когда непонятно, что происходит в соседней подсети.

Как результат, безопасность сталкивается с целым рядом вопросов (вызовов). Только справившись с ними, можно будет спать спокойно и быть уверенными, что волна «контейнеризации» разработки, тестирования и эксплуатации приложений управляема с точки зрения безопасности. Рассмотрим ключевые десять вызовов.

Вызов № 1. Знать, что защищаешь (CIS Controls 1, 2) — необходимо научиться находить контейнеры и системы оркестрации контейнеризации для понимания, что происходит в сети — всего множества объектов защиты.

Вызов № 2. Знать, кто управляет — все обнаруженные системы контейнеризации (обычно Docker) должны находиться под контролем систем оркестрации (Kubernetes, OpenShift). Отдельные инсталляции контейнеров на рабочих местах относятся к инструментам администрирования, а также к инструментам доставки хакерских утилит с GitHub внутрь сети организации. Поэтому в соответствии с классическими политиками безопасности они удаляются или заносятся в чёткий и прозрачный реестр исключений.

Вызов № 3. Знать, кто отвечает (владелец) — все системы оркестрации должны иметь своего технического владельца (сотрудника), который предоставит бизнес-цель запуска такой системы и доступ для системы сканирования и контроля защищённости. Естественно, цели вроде «хотел помайнить криптовалюту» или «обучаюсь, но без согласования с руководством» недопустимы для большинства индустрий (но могут быть допустимы, например, в ИТ-компаниях).

Вызов № 4. Знать, где мы уязвимы (CIS Controls 3, 4 и 5) — знать, где у службы ИБ есть логический доступ к системам оркестрации, где какие



уязвимости найдены, как быстро их приоритизировать и поставлять эту информацию в смежные процессы (Patch Management, Change Management) для закрытия уязвимостей или принятия рисков. В том числе важны функции сортировки, тегирования, фильтрации и группировки уязвимостей, а также формирование отчётов по уязвимостям и в рамках ответственности конкретных сотрудников — технических владельцев систем оркестрации. Важна и возможность принятия тех или иных рисков техническими владельцами. Однако принятие риска должно быть разумным. Если система нуждается в чувствительной информации (клиентские данные, банковская тайна), то полномочий владельца ресурса может не хватить.

Вызов № 5 (CIS Control 6). Знать, что происходит — собирать события с систем оркестрации и анализировать активность контейнеров, а также сохранять события: а) независимо от администраторов систем контейнеризации, б) для возможных будущих расследований службы ИБ.

Вызов № 6. Понимать уровень развития — понимать степень соответствия

безопасности конкретной системы оркестрации (со всеми контейнерами внутри) разумным CIS-бенчмаркам и планомерно внедрять механизмы безопасности — политики конфигурации.

Вызов № 7. Общение с бизнесом — навскидку в 70 процентах организаций безопасность оценивают только после нахождения проблем, а значит, надо анализировать в первую очередь запущенные контейнеры. Автор намеренно не осветил проблемы, связанные с registry, continuous integration и др., так как коммуницировать бизнесу и разработчикам эффективно в первую очередь по фактам проблем в уже запущенных контейнерах — там реальные (а не возможные) уязвимости, сгруппированные и приоритизированные по конкретным ответственным. Кстати, при верной постановке работы такой ответственный может стать Security Champion — союзником подразделения безопасности в обеспечении безопасности контейнеризации.

Вызов № 8. Автоматизация — волатильность и многочисленность контейнеров потребуют внедрения тех или

иных автоматических систем контроля и выявления контейнеров.

Вызов № 9. Независимость — для расследования активностей администраторов систем оркестрации нужно собирать информацию о контейнерах и системе оркестрации в независимую систему контроля.

Вызов № 10. Нехватка экспертности по контейнеризации — специалисты по системам контейнеризации с 2018 года стали востребованы на рынке талантов с зарплатами исполнителей до 6–7 тысяч долларов (американские центры разработки в Санкт-Петербурге). Нужно обучать существующих специалистов, а также использовать OpenSource или коммерческие решения с базой уязвимостей и ошибок конфигурации.

* * *

В очередной раз информационная безопасность сталкивается с новым классом вызовов. И соответственно, у неё появляется ещё одна возможность стать ценной и интегрироваться в бизнес-функции.

Павел КАНН

эксперт BIS Journal, эксперт по безопасности приложений Swordfish Security

Отдельно хотелось заметить, что широкое распространение технологий контейнеризации также поднимает и различные смежные проблемы, и вызовы для ИБ. Так, будучи программными продуктами, системы оркестрации и контейнеризации порой сами приносят проблемы, которые были присущи программному обеспечению прежде. Эти системы точно так же состоят из компонентов, которые могут быть уязвимы к различным проблемам безопасности. Точно так же в этих системах могут быть установлены небезопасные настройки — доступа, сетевых параметров, правил. И, безусловно, сам исходный код таких систем тоже может содержать уязвимости.

При этом стоит понимать, что компрометация систем контейнеризации и оркестрации в максимуме способна нанести даже больший урон организации, нежели атака на одну выделенную систему, выполняющую бизнес-задачу. Это происходит в том числе и потому, что, получая доступ к одной из подобных систем, злоумышленник имеет возможность получить доступ ко многим другим системам, которые управляются или разворачиваются в инфраструктуре организации.

К сожалению, этим сложности и вызовы, стоящие перед командами информационной безопасности, не заканчиваются.

Ведь, если посмотреть на уровень ниже, в контейнерах заключены всё те же приложения, которые и раньше выполняли бизнес-функции для организаций, и необходимость проведения анализа защищённости этих приложений никуда не пропала. Как и прежде, необходимо следить, чтобы программное окружение было построено на защищённой базе, чтобы все компоненты программного комплекса, заключённые в контейнер, были максимально последней версии и не содержали общеизвестных уязвимостей и, опять же, чтобы программный код самих приложений был написан безопасным образом.

Ввиду критической нехватки специалистов в области систем контейнеризации и оркестрации в данный момент также наблюдается и специфическая нехватка экспертизы по безопасности таких систем — как построить оптимальную систему оркестрации, как наилучшим образом обеспечить защиту компонентов этой системы, какие основные угрозы существуют как для систем контейнеризации, так и непосредственно для контейнеров, содержащих приложения. И, наконец, как максимально продуктивно наладить обоюдную коммуникацию по вопросам безопасности между командами разработки, командами, внедряющими реализованные решения, и командой инфраструктурной безопасности.

BIS-КОММЕНТАРИЙ

Денис БАТРАНКОВ

эксперт BIS Journal, консультант по информационной безопасности Palo Alto Networks

BIS-КОММЕНТАРИЙ

«НУЖНО СРАЗУ ПЛАНИРОВАТЬ ЗАЩИТУ ЭТОЙ НОВОЙ ТЕХНОЛОГИИ»

ПРОБЛЕМА — В ЕЁ УДОБСТВЕ

Для многих безопасников тема защиты контейнеризации возникла внезапно, и её нужно срочно поднимать в организации, потому что программисты давно уже стали использовать сторонние контейнеры, которые по умолчанию содержат уязвимости. Контейнеры удобней, потому что они не тянут за собой всю операционную систему, как виртуальные машины. Поэтому контейнеры занимают места лишь мегабайты, а не гигабайты. При этом в них находятся уже все библиотеки, необходимые им для работы. И платформа контейнеризации предоставляет все остальные необходимые ресурсы. Обычно здесь применяется Docker, OpenShift и Kubernetes.

Многие последние утечки данных произошли из-за использования уязвимых контейнеров. Проблема, как и всегда, кроется в удобстве. Контейнеризация даёт возможность быстро поднять нужный для бизнеса сервис, и она лишена многих проблем обычных статических и динамических библиотек, которые раньше использовали: контейнеры легко масштабируются, контейнеры не конфликтуют с имеющимися библиотеками, и контейнеры доступны публично в различных репозиториях.

Компании используют продукты для защиты контейнеризации, самым продвинутым и известным является Twistlock (новое название Prisma Cloud), позволяющий решить следующие задачи:

- ♦ просканировать все контейнеры и нарисовать полный граф их взаимодействия и запомнить это состояние;

- ♦ проанализировать в реальном времени аномалии, которые возникают при взаимодействии контейнеров, и запретить это или оповестить администратора;

- ♦ проконтролировать соответствие международным требованиям по защите контейнеризации (compliance);

- ♦ проверить уязвимости контейнеров и показать, как их исправить;

- ♦ интегрироваться в процесс CI/CD;

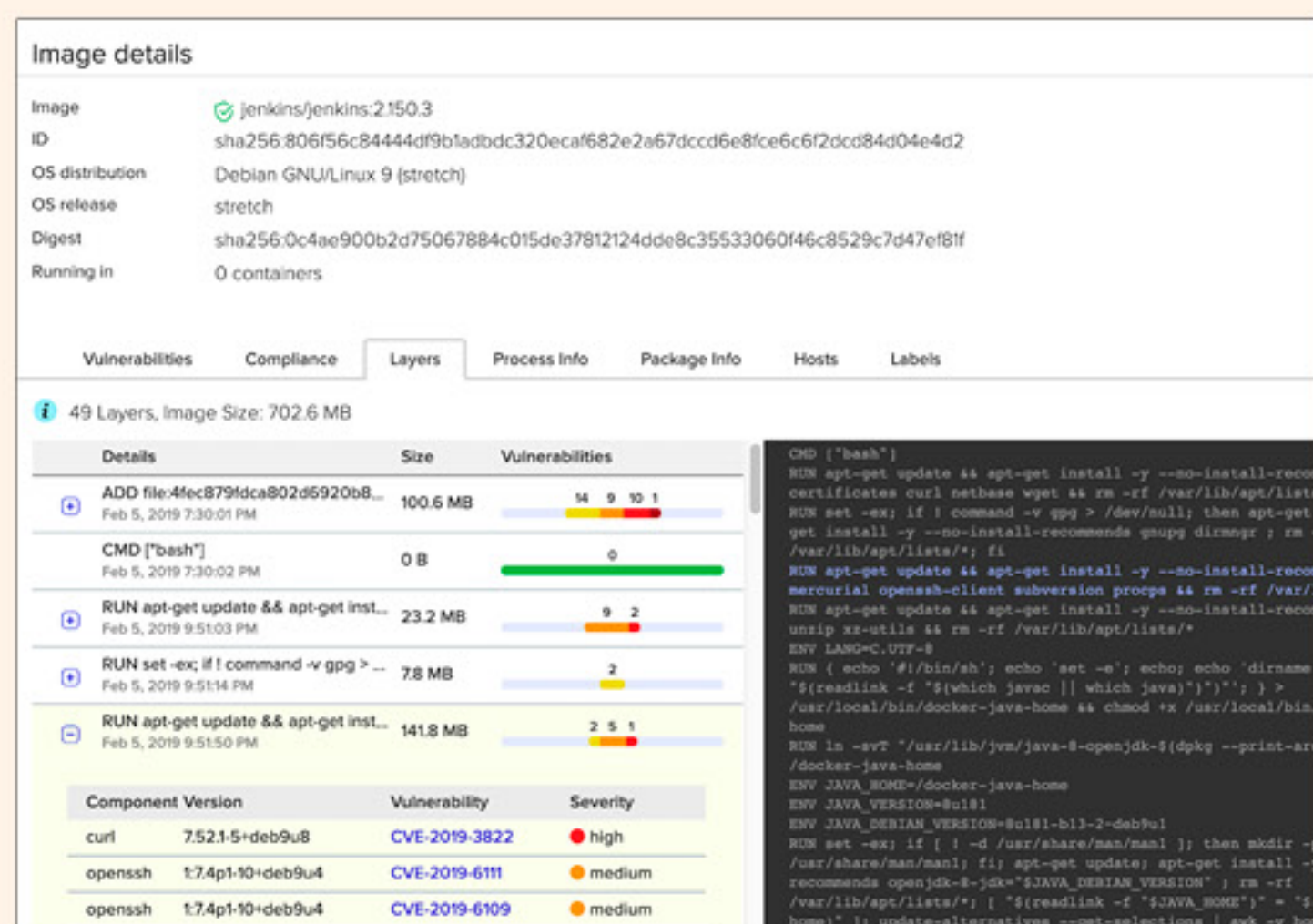
- ♦ разобрать инциденты и интегрировать события внутри Docker и Kubernetes с вашим SOC;

- ♦ защищать контейнеризацию как внутри компании, так и в облаках Azure, Amazon, GCP;

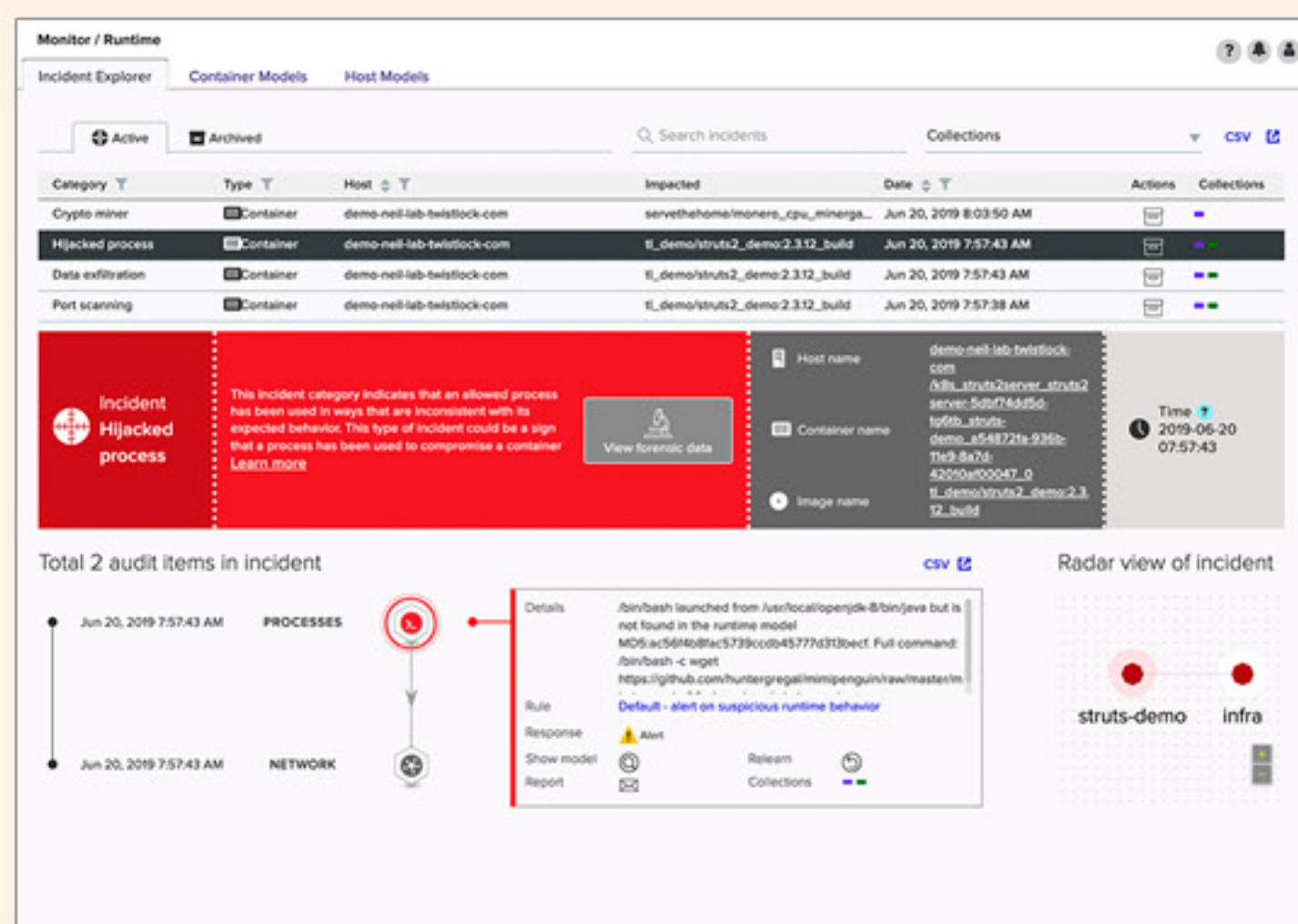
- ♦ защитить бессерверные технологии.

И защита бессерверных вычислений — важный момент. ИТ-разработчики не стоят на месте, поэтому нужно сразу планировать защиту этой новой технологии. В России ещё об этом не говорят, но за границей уже активно используют.

Смысл в том, что вы отправляете во внешний сервис функцию, которую надо этому сервису обсчитать. Очень похоже на то, как ставят задания в мейнфреймы. Допустим, это может быть разбор полей резюме для отдела кадров или подсчёт миллиона платежей для энергетической компании. Ей не нужно покупать виртуальные машины или контейнеры — она просто отправляет функцию с нужными значениями количества потреблённой электроэнергии и в ответ получает файл PDF. Поскольку такая задача требуется раз в месяц, то держать инфраструктуру ЦОД неэффективно, а запросить внешний сервис — выгодно.



Анализ уязвимостей в образе



Разбор инцидента

**Вей ТАЙ**

старший научный сотрудник
по анализу данных Tenable

**Илья ОСАДЧИЙ**

директор по развитию
ООО «Тайгер Оптикс»

**Никита ЦЫГАНКОВ**

руководитель направления
внедрения средств защиты
информации АО «ДиалогНаука»

РЕЙТИНГ ОСОБОГО НАЗНАЧЕНИЯ

КАК КИБЕРРАЗВЕДКА И BIG DATA ПОМОГАЮТ
ОЦЕНИВАТЬ КРИТИЧНОСТЬ УЯЗВИМОСТЕЙ
И ПРИОРИТИЗИРОВАТЬ ИХ УСТРАНЕНИЕ

В статье рассматривается подход компании Tenable к оценке критичности вновь публикуемых уязвимостей до публикации CVE и метрик CVSS, а также подходы к изменению критичности уязвимостей в зависимости от изменения ландшафта угроз и активности злоумышленников.

Исследования аналитиков компании Tenable, разработчика решений по управлению уязвимостями, показывают, что злоумышленники зачастую используют уязвимости сразу же после их публичного раскрытия. В случае угроз нулевого дня уязвимости используются ещё до того, как о них становится известно широкому кругу специалистов. В этой статье мы рассмотрим, как VPR, или рейтинг приоритетности уязвимости, уникальная разработка Tenable, может использоваться для приоритизации устранения уязвимостей ещё до их официальной публикации в реестре National Vulnerability Database (NVD).

ОТ ОБНАРУЖЕНИЯ УЯЗВИМОСТИ ДО ПУБЛИКАЦИИ CVE ID

NVD — это репозиторий уязвимостей, состоящий из множества наборов

данных, одним из которых является Common Vulnerabilities and Exposures (общепринятые уязвимости, CVE). NVD является одним из основных источников информации об уязвимостях для исследователей и специалистов по информационной безопасности. Информация об уязвимости в базе NVD включает её идентификатор CVE ID, описание, сведения о затронутых платформах, метрики CVSS (v2 и v3) и другие данные. Обычно организация, сообщаящая об уязвимости (так называемая CNA), присваивает ей идентификатор CVE ID сразу же при обнаружении. Затем CNA начинает подготовку описания уязвимости для публикации в NVD, в том числе результаты анализа влияния уязвимости на защищённость. Готовое описание CVE отправляется для публикации в базе NVD.

ЧТО ТАКОЕ «ПЕРИОД ДО NVD»

Процесс публикации CVE, описанный выше, может привести к задержке между первоначальным публичным раскрытием уязвимости и её публикацией в NVD. NVD подтверждает

существование такой задержки и указывает на следующее: «Дата 'Date Entry Created' в записи CVE указывает на день, когда идентификатор CVE ID был присвоен CVE Numbering Authority (CNA) или запись CVE была опубликована в реестре CVE. Эта дата не указывает на то, когда уязвимость была обнаружена, когда о ней сообщили вендору, когда она была публично обнародована или была обновлена в CVE».

В качестве примера «периода до NVD» рассмотрим уязвимость CVE-2019-17026. Изначально она была опубликована в Mozilla Security Advisory 8 января 2020 года, в NVD появилась 2 марта 2020 года и два дня спустя получила метрики CVSS. В данном примере «период до NVD» длился с 8 января до 2 марта и составил целых 55 дней.

СЕРЬЁЗНОСТЬ ПРОБЛЕМЫ «ПЕРИОДА ДО NVD»

Промежуток до NVD не является редкостью — 71 000 CVE были раскрыты в бюллетенях вендоров до того, как были опубликованы в NVD, что составляет половину всех CVE. В 2019 году у 5 300 CVE наблюдалось наличие периода до NVD.

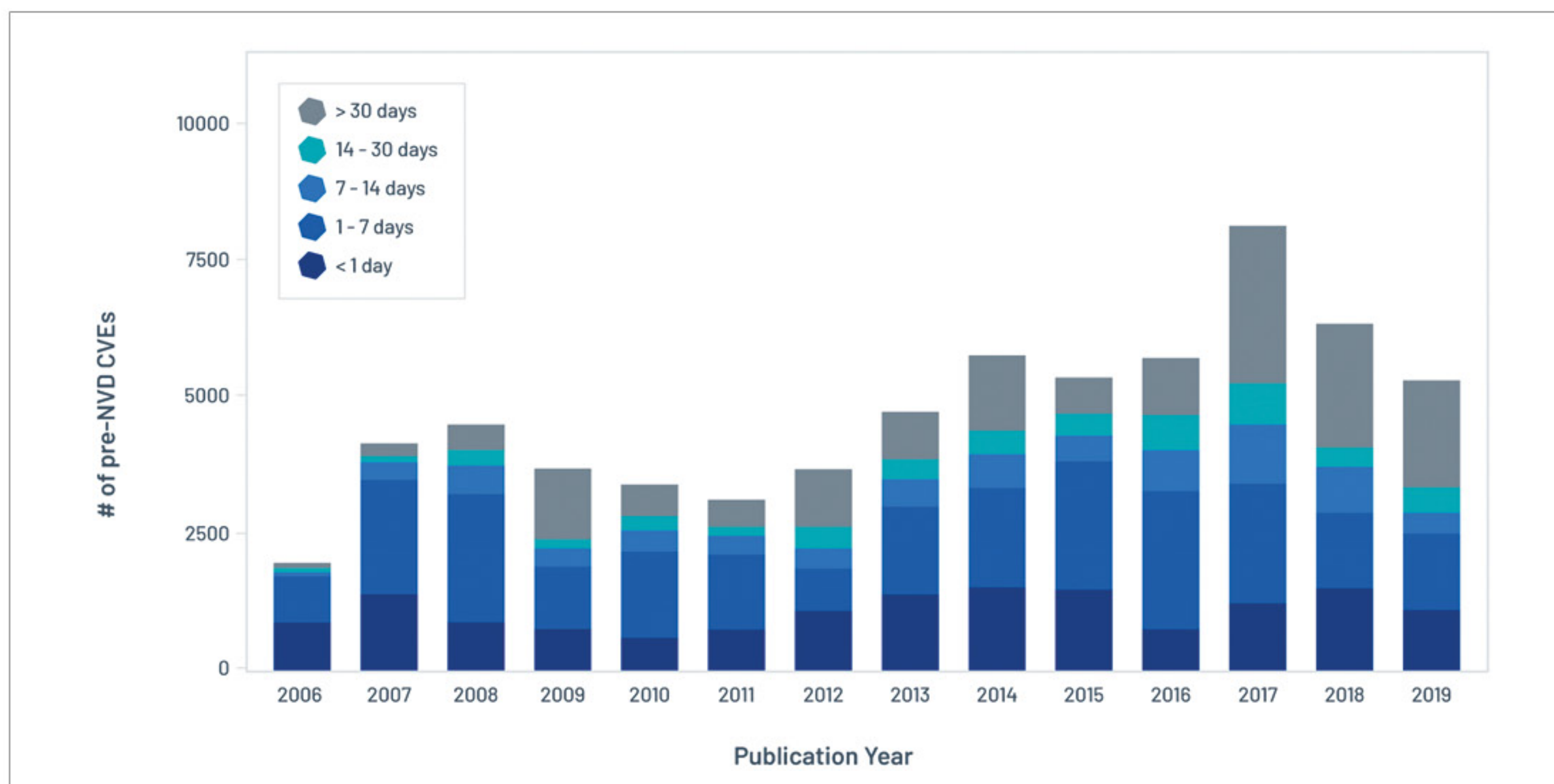


Рисунок 1. Количество CVE с периодом до NVD с 2006 года

В то время как «период до NVD» для некоторых CVE составляет один день, что приемлемо, анализ, проведенный Tenable, показывает, что для многих уязвимостей задержка существенна. На рисунке 1 приведено количество CVE с периодом до NVD с 2006 года, с разбивкой по годам и длительности задержки в публикации.

Из этого графика можно сделать следующие выводы:

- ♦ Начиная с 2013 года ежегодное количество CVE с «периодом до NVD» стабилизировалось на показателе в 5 000 единиц. Это означает, что в последние годы CNA стали более оперативно публиковать CVE.

- ♦ В последние годы стало более выраженным распределение длительностей задержки в публикации уязвимости. Значительная часть уязвимостей была опубликована с задержкой в 30 и более дней. Специалисты ИБ должны уделять внимание CVE со значительным периодом до NVD, поскольку такие уязвимости могут отрицательным образом сказаться на защищенности организаций.

АКТИВНОСТЬ ЗЛОУМЫШЛЕННИКОВ ДО ПУБЛИКАЦИИ В NVD

Очевидно, что злоумышленники не ждут публикации CVE для начала

активной эксплуатации уязвимости. Сравнение данных киберразведки со списком CVE с «периодом до NVD» показывает, что в отношении 5 400 из 43 000 CVE (12%), опубликованных с 2019 по 2020 год, наблюдалась активность злоумышленников ещё до публикации данных в NVD.

На рисунке 2 отражено распределение этих CVE по году публикации и «окну угрозы» до публикации в NVD. Значительное количество этих CVE активно использовалось злоумышленниками в течение как минимум 30 дней до их публикации в NVD. Поэтому любые системы, затронутые этими уязвимостями, оставались подвержены реальным атакам до того, как информация об уязвимости стала доступна в NVD.

КАК ПРИОРИТИЗИРОВАТЬ УСТРАНЕНИЕ УЯЗВИМОСТЕЙ ДО NVD С ПОМОЩЬЮ РЕЙТИНГА VPR

Устранение активно эксплуатируемых уязвимостей необходимо начинать как можно раньше. Как показало исследование, CVE из реестра NVD не являются наиболее актуальным источником информации для организации проактивного управления уязвимостями. Tenable решает эту проблему, получая

информацию об уязвимостях напрямую из бюллетеней более чем от 100 крупнейших вендоров. Для полученных таким образом уязвимостей Tenable рассчитывает рейтинг приоритетности уязвимости, или VPR.

Расчёт VPR для уязвимостей в «периоде до NVD» не является тривиальной задачей. Поскольку многие CNA не предоставляют метрики CVSS для уязвимости на стадии до NVD, оценка влияния уязвимости на их основе не всегда возможна. Для решения этой проблемы VPR комбинирует технологии машинного обучения и обработки натурального языка, что позволяет предсказать метрики CVSS.

Начиная с августа 2019 года Tenable проводит оценку критичности уязвимостей до их публикации в NVD с помощью модели VPR. Из 12 073 опубликованных уязвимостей 1 592 включали «период до NVD». По итогам анализа рейтинг VPR показал гораздо большую эффективность в оценке новых уязвимостей. Например:

- ♦ все 1 592 уязвимости получили рейтинг VPR до публикации в NVD;

- ♦ 84% уязвимостей с «периодом до NVD» получили рейтинг VPR в течение уже первых 24 часов, в то время как только 38% уязвимостей были опубликованы в NVD в тот же период;

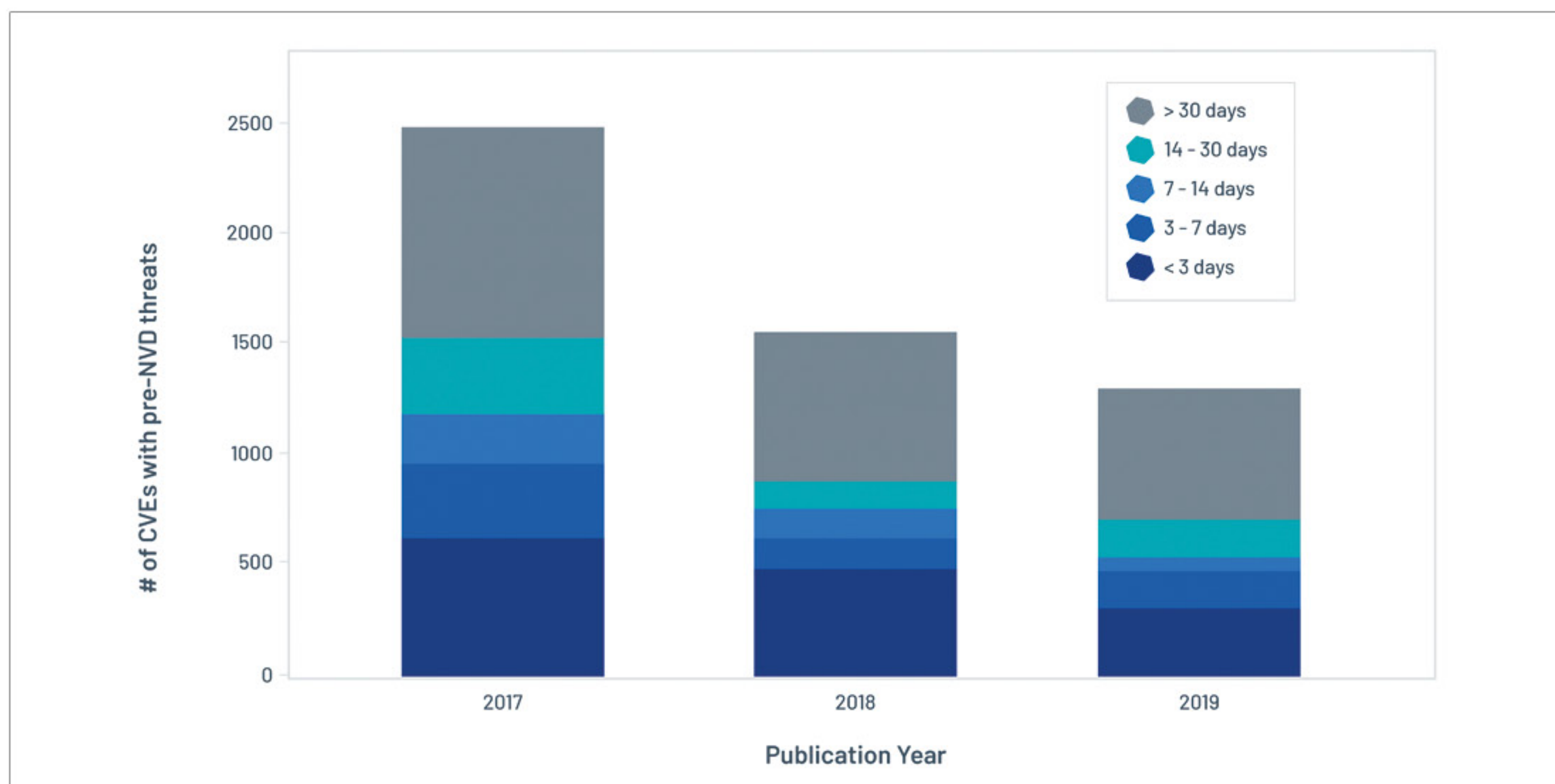


Рисунок 2. Количество CVE с активными угрозами до публикации в NVD. Разбивка по длительности «окна угрозы»

♦ 499 уязвимостей были опубликованы в NVD с задержкой в семь или более дней, в то время как только 101 уязвимость были присвоены рейтинги VPR за семь и более дней;

♦ 245 уязвимостей были опубликованы в NVD с задержкой более 30 дней.

Количество уязвимостей с «периодом до VPR» будет уменьшаться и далее по мере того, как Tenable будет получать данные об уязвимостях из всё большего числа бюллетеней вендоров.

ПРАКТИЧЕСКИЙ ПРИМЕР: CVE-2019-17026

В качестве примера в этой статье используется CVE-2019-17026. Вот как развивались события с этой уязвимостью:

♦ **8 января 2020 года:** CVE-2019-17026 был впервые опубликован в бюллетене Mozilla Security Advisory. Tenable опубликовал анализ уязвимости после её публикации и плагины,

позволяющие её детектировать. Они были опубликованы с рейтингом VPR 9,7, что отразило факт использования уязвимостей в нацеленных атаках.

♦ **Период с 8 января по 1 марта 2020 года:** дискуссии и исследования об эксплуатации этой уязвимости были зафиксированы во многих источниках, в том числе в Twitter, форумах злоумышленников, сайтах Dark Web и в технических блогах. Это привело к повышению рейтинга VPR до пикового значения 9,9 на этапе до публикации в NVD;

♦ **2 марта 2020 года:** CVE-2019-17026 был опубликован в NVD, и два дня спустя в результате анализа уязвимость получила оценку CVSSv3 8,8;

♦ **3 марта 2020 года и позже:** риск, связанный с этой уязвимостью, остаётся высоким. События, связанные с ней, были зафиксированы в прессе, Twitter, сайтах Dark Web, на пейст-сайтах и

т.д. В апреле появилась информация о том, что эта уязвимость использовалась АРТ-злоумышленником по имени DarkHotel для целей в Китае и Японии. Рейтинг VPR этой уязвимости остаётся критическим на момент публикации.

ВЫВОДЫ

В этой статье мы показали, что злоумышленники зачастую используют уязвимости ещё до публикации соответствующих CVE в реестре NVD. Учитывая имеющиеся задержки в публикации, специалисты ИБ не должны использовать NVD как единственный источник информации об уязвимостях. Рейтинг VPR, разработанный Tenable, оперативно оценивает новые уязвимости — 84% новых уязвимостей оцениваются алгоритмом VPR в течение одного дня с момента публичного раскрытия, и 93% оцениваются в течение одной недели.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

♦ опробовать VPR в действии можно, заказав пилот решений Tenable.io (в облаке) и Tenable.sc (на площадке заказчика): <https://www.tiger-optics.ru/get-demo/>

♦ узнать больше о предсказательной приоритизации Tenable и рейтинге VPR можно по ссылке Tenable Predictive Prioritization and VPR: <https://www.tenable.com/tenable-io/predictive-prioritization-demo>



Павел ЛУЦИК
директор по продажам и развитию
бизнеса компании КриптоПро

ПРОСТЫЕ РЕШЕНИЯ

ОПЫТ КОМПАНИИ КРИПТОПРО ПО ОРГАНИЗАЦИИ ЗАЩИЩЁННОГО УДАЛЁННОГО ДОСТУПА СОТРУДНИКОВ К КОРПОРАТИВНЫМ РЕСУРСАМ

В этой статье мы расскажем о том, как наша компания перешла на удалённый режим работы, в частности, об используемых нами механизмах организации безопасного удалённого доступа к рабочему месту с помощью продуктов КриптоПро и Microsoft, которые вы можете применить у себя как отдельно, так и в составе описанного далее пакета.

Для организации защищённого удалённого доступа мы используем два механизма — VPN-доступ и защищённый доступ к удалённому рабочему столу. Каждый из данных механизмов позволяет обеспечить защиту передаваемой информации в соответствии с требованиями законодательства РФ по информационной безопасности.

SSL/TLS VPN

Использование VPN позволяет предоставить и разграничить доступ к сетевой инфраструктуре компании. Для этих целей мы используем высокопроизводительный VPN-шлюз КриптоПро NGate и VPN-клиенты для Microsoft Windows, Apple macOS, Linux, а также iOS и Android (рис. 1).

REMOTE DESKTOP GATEWAY

Брокер удалённых подключений Microsoft Remote Desktop Gateway предназначен для получения доступа только к рабочим местам сотрудников на Microsoft Windows. Защита трафика

при этом обеспечивается установкой КриптоПро CSP на шлюз доступа и клиентские компьютеры (на которых запускается клиент удалённого доступа).

Оба варианта предоставляют возможность аутентификации пользователей по логину/паролю (через Active Directory) или с помощью сертификатов/смарт-карт. Для сервера используется серверный сертификат, который мы получили в нашем УЦ.

ПАКЕТ «ЗАЩИЩЁННЫЙ УДАЛЁННЫЙ ДОСТУП»

Для реализации описанных выше инструментов в вашей организации предлагаем вашему вниманию пакет «Защищённый удалённый доступ», который позволит вам реализовать защищённый удалённый доступ к корпоративным информационным ресурсам в соответствии с требованиями законодательства РФ по ИБ.

В состав пакета входят следующие компоненты, которые могут быть использованы как совместно, так и отдельно друг от друга:

1. Сертифицированный ФСБ России шлюз удалённого доступа КриптоПро NGate в виртуальном исполнении, включающий в себя бесплатную трёхмесячную лицензию на 50 одновременных подключений и реализующий удалённый доступ к произвольным ресурсам с применением российских криптографических алгоритмов. В качестве клиентского компонента может

использоваться любой браузер, поддерживающий ГОСТ (для подключения к веб-ресурсам), либо VPN-клиент КриптоПро NGate Client (для подключения к произвольным ресурсам, в том числе с мобильных устройств). По запросу возможно увеличение количества одновременных подключений и/или срока временной лицензии.

2. Сертифицированный ФСБ России криптопровайдер КриптоПро CSP 4.0/5.0, включающий в себя бесплатную трёхмесячную лицензию. Совместное использование данного криптопровайдера со службой Microsoft RDG (Remote Desktop Gateway), входящей в состав современных серверных ОС Windows, способно обеспечить защищённый доступ к удалённому рабочему столу ОС Windows по протоколу RDP с применением российских криптографических алгоритмов. В качестве клиентского компонента для подключения к удалённому рабочему столу используется входящая в состав ОС Windows команда MSTSC.

3. Сертификат аутентификации сервера (необходим для функционирования шлюзов КриптоПро NGate и Microsoft Remote Desktop Gateway), предоставляемый бесплатно и удалённо на три месяца. По запросу сертификат может быть выдан на более длительный срок. Подробности получения сертификата шлюза можно прочитать тут: <http://tlsca.cryptopro.ru>. Сертификат этого удостоверяющего центра уже включён в дистрибутивы

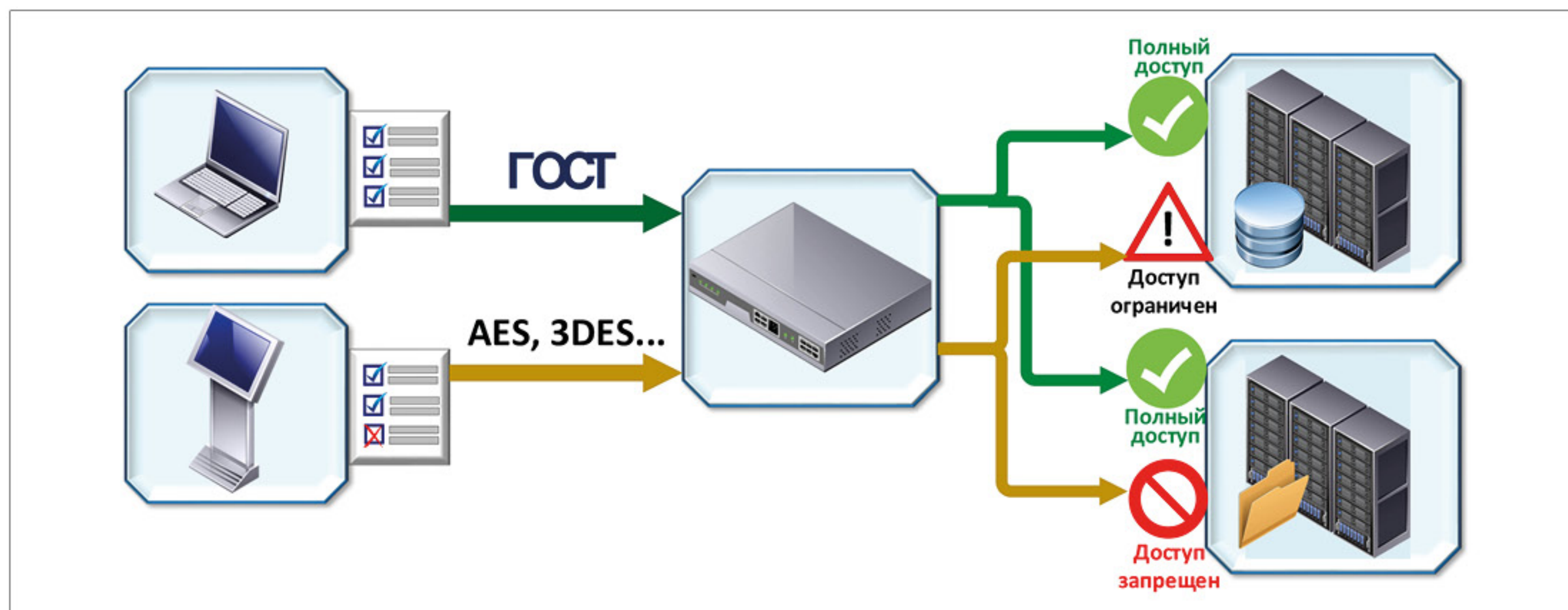


Рисунок 1. Использование VPN позволяет предоставить и разграничить доступ к сетевой инфраструктуре компании

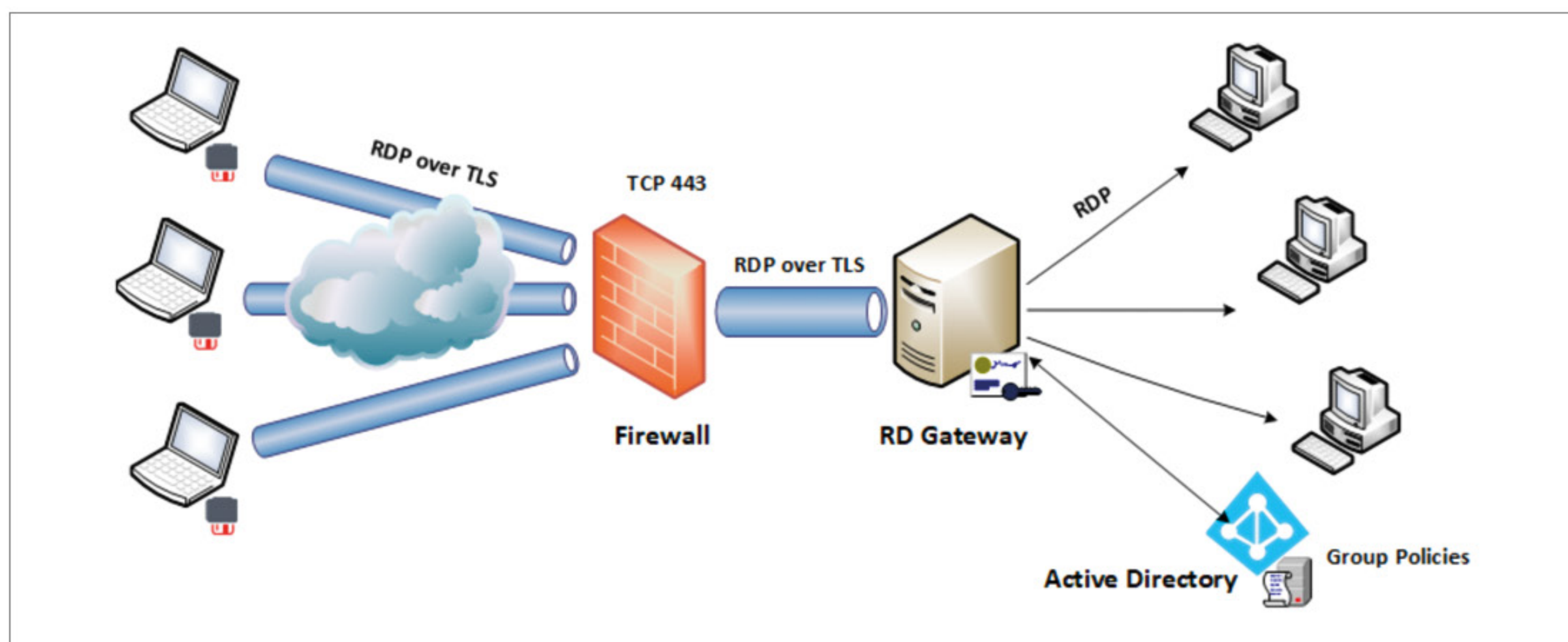


Рисунок 2. Брокер удалённых подключений Microsoft Remote Desktop Gateway предназначен для получения доступа только к рабочим местам сотрудников на Microsoft Windows. Защита трафика при этом обеспечивается установкой КриптоПро CSP на шлюз доступа и клиентские компьютеры

КриптоПро CSP, поэтому пользователям не придётся самостоятельно настраивать доверие к сертификату шлюза.

Предлагаемые для удалённого доступа компоненты нетребовательны к системным и аппаратным ресурсам и могут быть оперативно развёрнуты специалистами организации по документации. В случае необходимости в дальнейшем возможно проведение бесшовной миграции шлюза КриптоПро NGate с виртуального исполнения на более производительное и отказоустойчивое аппаратное, с сохранением настроек и политик безопасности.

Предоставляемый пакет будет особенно полезен следующим организациям, для которых удалённый доступ должен быть защищён в соответствии с требованиями законодательства по ИБ:

- ♦ государственным органам и подведомственным организациям для организации доступа к государственным и муниципальным информационным системам;
- ♦ операторам персональных данных для организации доступа к информационным системам персональных данных;
- ♦ субъектам критической информационной инфраструктуры (КИИ) для

организации доступа к значимым объектам КИИ;

- ♦ финансовым организациям для организации доступа к информационным системам.

* * *

При организации удалённого доступа предлагаем также воспользоваться рекомендациями отечественных регуляторов (Банк России, ФСТЭК России, НКЦКИ) по мерам обеспечения информационной безопасности на время удалённой работы, опубликованными на их официальных сайтах.

СДЕЛАНО В РОССИИ, СЕРТИФИЦИРОВАНО ФСТЭК

ПЛАТФОРМА USERGATE ДЛЯ МАСШТАБИРУЕМОЙ И МНОГОВЕКТОРНОЙ ЗАЩИТЫ ЗОКИИ

Ключевыми факторами, влияющими на техническую и организационную политику обеспечения информационной безопасности (ИБ) на предприятиях и в организациях России стали:

- ♦ понятие критической информационной инфраструктуры (КИИ) и требования 187-ФЗ;

- ♦ общепромышленные требования таких регуляторов как ФСБ и ФСТЭК к оборудованию для защиты информации на значимых объектах КИИ (ЗОКИИ).

Речь идёт о том, что наряду с банальными для профессионалов требованиями к обеспечению конфиденциальности информации, её целостности и доступности, наши главные регуляторы в сфере безопасности выдвигают:

- ♦ жёсткие требования к сертификации средств защиты информации в ЗОКИИ, которые должны проводиться в форме приёмки или испытаний в соответствии с 184-ФЗ «О техническом регулировании»;

- ♦ возможность гарантийной и технической поддержки оборудования и систем ИБ ЗОКИИ российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических и (или) юридических лиц, равно как и возможность осуществления модернизации упомянутого оборудования систем организациями, удовлетворяющими тем же требованиям (приказ ФСБ № 196 от 6 мая 2019 года).

Говоря проще, регуляторы выводят обеспечение ИБ ЗОКИИ на колею импортозамещения.

В связи с этим для наших читателей будет интересным знакомство с компаниями, для которых прилагательное «российская» не является маркетинговым инструментом, а наполнено конкретным содержанием.

ЧТО ПОЗВОЛЯЮТ РЕШЕНИЯ USERGATE

Российская компания «Юзергейт» стартовала на рынке ИБ в 2001 году и сегодня предлагает ИБ-платформу, позволяющую:

- ♦ сформировать на предприятии или в организации систему обнаружения вторжений в корпоративную ИТ-инфраструктуру;

- ♦ отражать DoS-атаки;

- ♦ обеспечить антивирусную защиту и автоматически реагировать на неизвестные угрозы;

- ♦ организовать проверку электронной почты для защиты от рекламного спама и разных видов мошенничества (анализируются письма на любых языках, а также сообщения в графических форматах);

- ♦ осуществлять административный контроль использования Интернета, обеспечивая блокировку посещения потенциально опасных ресурсов, а также сайтов, не связанных с работой (если это необходимо);

- ♦ использовать технологию VPN для объединения удалённых офисов

единой защищённой сетью и обеспечения безопасного доступа сотрудников компаний с распределённой структурой к корпоративным ресурсам на основе применения единых настроек безопасности в сети филиалов.

Технологии, используемые в UserGate, соответствуют современной концепции SOAR (Security Automation, Orchestration and Response), позволяя анализировать поведение различных процессов, выявлять риски и автоматически обеспечивать на основе этого анализа адекватную реакцию, обеспечивая защиту от угрозы или просто от аномального поведения на самой ранней стадии.

Работа функций безопасности UserGate основана на постоянном взаимодействии с Центром Безопасности компании, что позволяет поддерживать минимальное время реакции на разнообразные современные угрозы.

ОДОБРЕНО ПРОФЕССИОНАЛАМИ

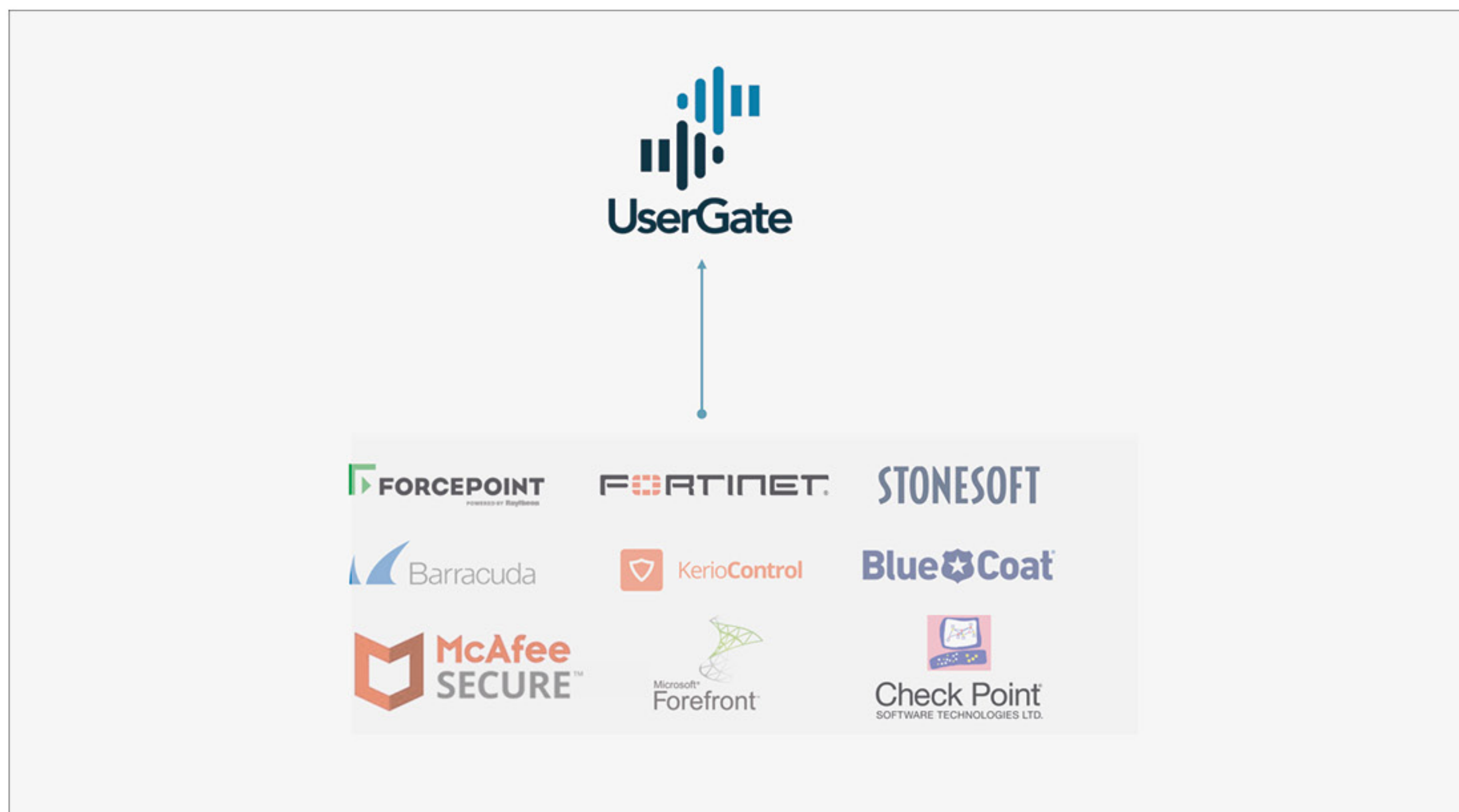
Предложение компании «Юзергейт» получило одобрение как открытого международного профессионального сообщества, так и регулятора, стоящего на страже «корпоративных» государственных интересов.

И если выход в финалы и победы в ряде конкурсов под эгидой зарубежных изданий — это во многом рекламная составляющая маркетинга, то сертификация ФСТЭК — это серьёзная и обоснованная заявка на замещение зарубежного ИБ-оборудования на отечественных объектах КИИ.

Сертификат ФСТЭК России № 3905 подтверждает соответствие UserGate требованиям, установленным в следующих документах:

- ♦ Требования по безопасности информации, устанавливающие уровни

Технологии, используемые в UserGate, соответствуют современной концепции SOAR, позволяя анализировать поведение различных процессов, выявлять риски и автоматически обеспечивать на основе этого анализа адекватную реакцию



Возможности замещения зарубежных аналогов решениями на базе платформы UserGate

доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (ФСТЭК России, 2018) по 4 уровню доверия;

- ♦ Требования к межсетевым экранам (ФСТЭК России, 2016);

- ♦ Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016);

- ♦ Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016);

- ♦ Требования к системам обнаружения вторжений (ФСТЭК России, 2011);

- ♦ Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012).

- ♦ Требования 17 и 21 приказов ФСТЭК для обработки персональных данных 1–4 категорий.

СДЕЛАНО В РОССИИ, РАБОТАЕТ НАДЕЖНО

Решения линейки UserGate могут быть приобретены в виде виртуального готового образа для VMware, Hyper-V и прочих систем виртуализации или в виде программно-аппаратного комплекса (ПАК).

Компания уделила внимание созданию собственной платформы, не основанной на использовании чужого исходного кода и сторонних модулей

Разработчики компании предпочли отказаться от «интеграции» собственного предложения на основе «лучших в отрасли продуктов» от десятков поставщиков и open source-решений, «экономя» за счёт этого на стоимости приобретения. Вместо этого компания уделила внимание созданию собственной платформы, не основанной на использовании чужого исходного кода и сторонних модулей. Это позволяет обеспечивать высокое качество продукта, надежность работы, а также удобства для развития платформы UserGate и её адаптации для сложных проектов.

UserGate работает на базе специально созданной и поддерживаемой операционной системы, а также на специально спроектированных аппаратных устройствах, позволяющих обеспечить наибольшую эффективность и скорость обработки трафика.

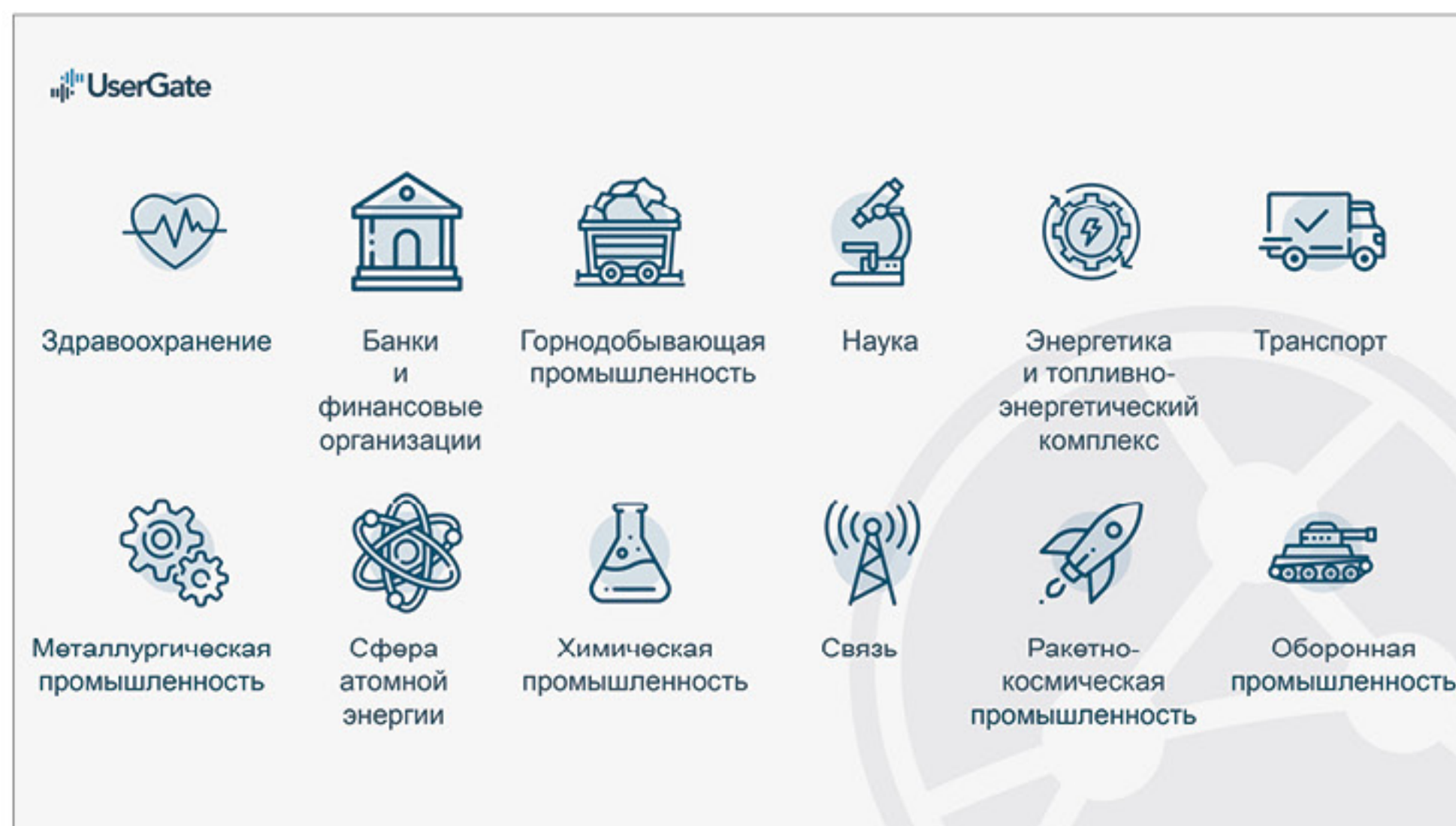
В обновленной версии операционной системы UGOS появилась возможность настроек защиты промышленных системы управления (АСУТП, SCADA).

Для организации антивирусной защиты заказчик может использовать либо известный отечественный антивирус Касперского, либо антивирус UserGate, который менее требователен к ресурсам аппаратной платформы и достаточно эффективен согласно актуальной сигнатурной базе.

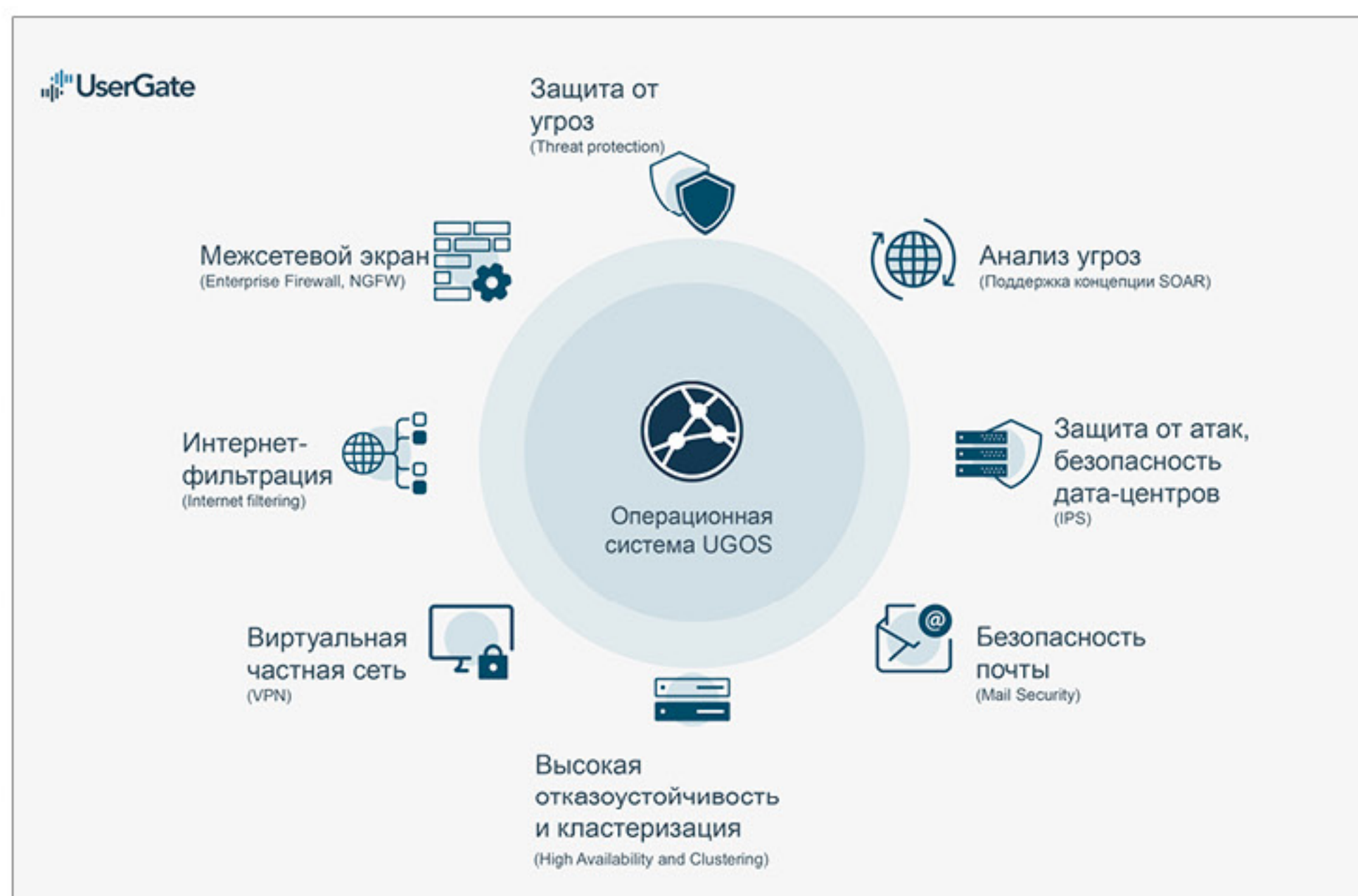
ПАК и UserGate — это 6 видов аппаратных платформ собственной сборки на территории России.

Решения UserGate поддерживают возможность кластеризации, а также режим высокой доступности (High Availability).

Кластеризация позволяет применять к разным узлам единые настройки, политики, библиотеки, сертификаты,



Сферы применения решений на базе платформы UserGate



О решениях на платформе UserGate

сервера авторизации, группы пользователей и т.д.

Функция High Availability позволяет кардинально снизить риски, которые могут возникать в связи со сбоями в работе аппаратного обеспечения, поддерживающего систему UserGate: при необходимости система устанавливается на парных узлах и обеспечивается автоматическое переключение нагрузки между ними в случае сбоев.

СДЕЛАНО В РОССИИ, РАБОТАЕТ ПО ВСЕМУ МИРУ

На основе собственной операционной системы UGOS и аппаратных платформ реализуются ИБ-решения

UserGate, обеспечивающие комплексную безопасность корпоративных сетей разного масштаба.

Партнёрская сеть компании насчитывает более 300 системных интеграторов в более чем 40 странах мира.

В России пользователями решений UserGate являются множество предприятий малого и среднего бизнеса, подразделения государственных структур регионального и федерального масштаба, образовательные учреждения.

Компанией реализовано несколько десятков крупных проектов по внедрению решений на основе платформы UserGate.

В мае этого года компания провела свою очередную партнёрскую конференцию, на которой были представлены её новинки:

- ♦ плата-ускоритель Катунь с функцией SSL-брокера;
- ♦ новая аппаратная платформа UserGate C;
- ♦ новая, ориентированная на сегмент АСУТП, аппаратная платформа UserGate X;
- ♦ система анализа инцидентов безопасности и мониторинга событий UserGate Log Analyzer (UserGate LogAn);
- ♦ система централизованного управления UserGate Management Center (UserGate MC).

Разработка своих аппаратных платформ была вновь обозначена на конференции 2020 года как одно из приоритетных направлений для развития компании.

* * *

Тесная работа «Юзергейт» со ФСТЭК в сфере сертификации своей продукции позволяет с помощью оборудования компании не только строить системы защиты ЗОКИИ, соответствующие действующим жёстким требованиям ФСБ и ФСТЭК, но и нормативным документам в сфере ИБ отраслевых регуляторов в финансовой сфере, топливно-энергетическом комплексе, в «оборонке» и иных сферах хозяйства.

Сертификация ФСТЭК позволяет использования решения на основе платформы UserGate в составе автоматизированных систем до класса защищённости 1Г, информационных системах персональных данных (ИСПДн) и государственных информационных системах (ГИС) до 1 класса (уровня) защищённости включительно.

Собственные аппаратные платформы, представленные для включения в Реестр российской радиоэлектроники Минпромторга, позволяют создавать высокопроизводительные системы, повышать доверие отечественных заказчиков и укреплять независимость компании от мировой политической и экономической конъюнктуры.



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.



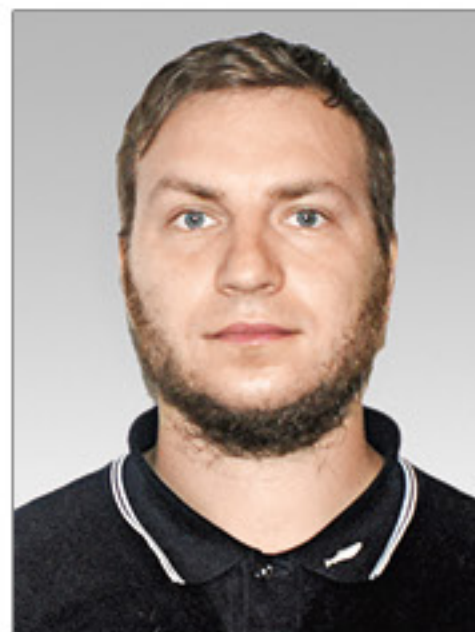
**Kaspersky®
Endpoint Security
для бизнеса
Универсальный**

kaspersky

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



Иван МЕДЕННИКОВ
группа компаний ЦРТ



Сергей СМЕРНОВ
группа компаний ЦРТ

ОПЯТЬ ПОБЕДА!¹

РОССИЙСКАЯ ТЕХНОЛОГИЯ РАСПОЗНАВАНИЯ РЕЧИ
ОТ ГРУППЫ ЦРТ ПРИЗНАНА ЛУЧШЕЙ В МИРЕ

Научная команда группы ЦРТ (входит в экосистему Сбербанка) одержала победу в самом сложном из направлений международного конкурса на распознавание речи с нескольких микрофонов в условиях естественной обстановки CHiME Speech Separation and Recognition Challenge (CHiME-6), существенно опередив решения лидеров в развитии методов распознавания речи — Университет Джонса Хопкинса (США), Университет науки и технологии Китая, Технический университет Брно (Чехия) и др.

УСЛОВИЯ КОНКУРСА ИЗМЕНИЛИСЬ

Проводившийся уже в шестой раз конкурс по разделению и распознаванию речи CHiME ставит для участников задания по распознаванию естественной разговорной речи на английском языке в повседневной домашней обстановке. При этом задача с каждым разом усложняется: в этом году, впервые в истории данного конкурса, помимо направления по распознаванию заранее сегментированной (разделённой) речи, было добавлено задание, где перед непосредственно распознаванием требовалось разделить аудиопоток на сегменты в соответствии с принадлежностью аудиопотока тому

или иному говорящему (провести диаризацию²). Команда ЦРТ принимала участие в решении обоих заданий, но основное внимание обратила на задачу более сложного направления — распознавания несегментированной речи.

Речевые данные для конкурса были записаны в условиях двадцати реальных домашних ужинов, состоящих из общения на свободные темы четырёх знакомых между собой людей (двух хозяев и двух гостей) в процессе приготовления пищи и непосредственно за ужином. Каждый раз записывалось 24 канала дальних³ микрофонов в трёх различных помещениях. На таких записях присутствуют отрезки, где слышна одновременная речь 2–4 человек, присутствуют реверберация и интенсивный шум: звон приборов, льющаяся из крана вода, гул кондиционера, шаги, смех, что значительно усложняет распознавание речи. Проблема выделения речи и её последующего распознавания в таких сложных условиях получила название cocktail party problem (проблема коктейльной вечеринки). Полученные записи были разделены на три набора образцов: для обучения, настройки и итогового тестирования представленных решений.

² Диаризация — процесс разделения входящего аудиопотока на сегменты в соответствии с принадлежностью аудиопотока тому или иному диктору

³ Дальним микрофоном называют микрофон, удалённый от диктора не менее чем на 2 м

Базовое решение для задачи диаризации, предложенное организаторами конкурса, было основано на наиболее широко используемом в настоящее время подходе — кластеризации скрытых представлений диктора (эмбедингов). Первым этапом в данном способе является выделение речевых сегментов при помощи детектора активности речи (VAD). Далее осуществляется разбиение сигнала на интервалы по 1,5 с с шагом 0,75 с, для каждого из которых считаются мел-кепстральные коэффициенты (MFCC) и извлекаются х-векторы — наиболее широко используемые сейчас эмбединги дикторов. Эти х-векторы разбиваются на 4 группы, соответствующие дикторам в сессии, при помощи вероятностного линейного дискриминативного анализа (PLDA) и алгоритма агломеративной иерархической кластеризации (AHC). Наконец, подряд идущие интервалы, соответствующие одному диктору, соединяются вместе. Этот подход даёт довольно большую ошибку диаризации (DER), составляющую около 63 %, что не позволяет применить алгоритм управляемого разделения источников (GSS), который продемонстрировал лучшие результаты при решении задач предыдущего конкурса CHiME-5.

ПРИНЦИПИАЛЬНО ИНОЙ ПОДХОД

При попытке совершенствовать предложенное базовое решение с помощью использования улучшенного

¹ «GoldenVOICES из России» (BIS Journal №1/2020), «Россияне победили на чемпионате мира по... идентификации!» (BIS Journal №1/2019)

Для оценки качества диаризации применяют следующие оценки (чем меньше значение данных показателей, тем более качественным считается диаризация):

DER — Diarization Error Rate

DER вычисляется сопоставлением результата диаризации с эталонной разметкой.

$$DER = (T_{fa} + T_{miss} + T_{spkr}) / T_{speech}$$

где T_{fa} — false alarm time (время, когда система переоценивает количество дикторов),

T_{miss} — miss time (время, когда система недооценивает количество дикторов),

T_{spkr} — error time (время, когда предполагаемый диктор не сопоставлен с эталонным),

T_{speech} — общее время аудиофайла.

JER — Jaccard Error Rate

JER основан на индексе Jaccard, показателе сходства, который используется для оценки результатов систем сегментации изображений. JER показывает насколько пересечение результата диаризации и эталонной разметки отличается от их объединения. Он похож на DER, но при этом одинаково взвешивает вклад каждого диктора, независимо от того, какое количество речи он на самом деле произнёс.

34-слойного экстрактора х-векторов Wide ResNet (WRN), обученного на данных VoxCeleb и замены агломеративной иерархической кластеризации на более эффективный алгоритм спектральной кластеризации (Spectral Clustering), сотрудникам ЦРТ удалось снизить ошибку диаризации с 63 % до 47 %, что всё ещё было недостаточно для эффективного применения алгоритма GSS. Ключевым недостатком подхода, основанного на кластеризации эмбедингов, является его принципиальная неспособность выделять одновременную речь нескольких дикторов. В ходе анализа выяснилось, что доля одновременной речи в представленных записях значительна, поэтому вышеописанный подход даже в идеальном случае не способен снизить ошибку диаризации ниже 25,6 %.

Российской командой был предложен принципиально иной подход, названный Target-Speaker Voice Activity Detection (TS-VAD), или детектирование активности целевого диктора, способный выделять одновременную речь нескольких дикторов. При таком подходе входные признаки MFCC преобразуются четырёхслойной свёрточной нейронной сетью (CNN), а затем подаются на четыре параллельных блока Speaker Detection (SD), имеющих общие параметры. Каждый SD-блок представляет собой двухслойную двунаправленную нейронную сеть с блоками долгой краткосрочной памяти LSTM (BLSTM), в котором

дополнительным входом является i-вектор (более простой по сравнению с х-векторами вид эмбедингов), соответствующий диктору. Затем объединённые выходы четырёх SD-блоков передаются на ещё один слой BLSTM, за которым следуют четыре параллельных полносвязанных слоя и двухклассовые слои softmax. Четыре пары выходов модели TS-VAD представляют

вероятности наличия или отсутствия каждого диктора в конкретный момент времени (рис. 1).

Для повышения эффективности работы TS-VAD в условиях многоканального сигнала была предложена многоканальная TS-VAD модель (TS-VAD-MC) в которой скрытые представления SD для каждого из дикторов, извлечённые из одноканальной TS-VAD модели по

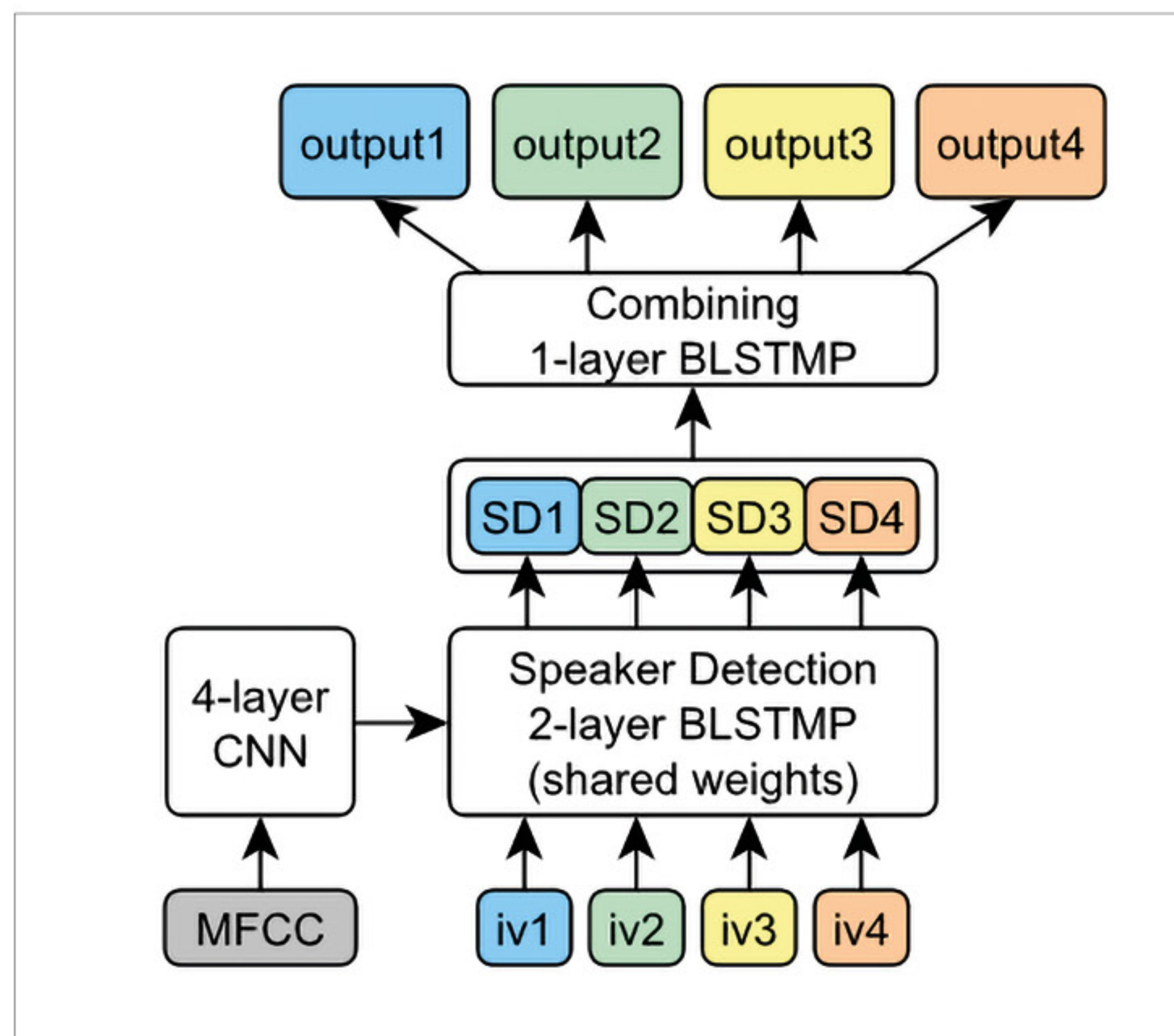


Рисунок 1. Схема предложенной одноканальной TS-VAD модели

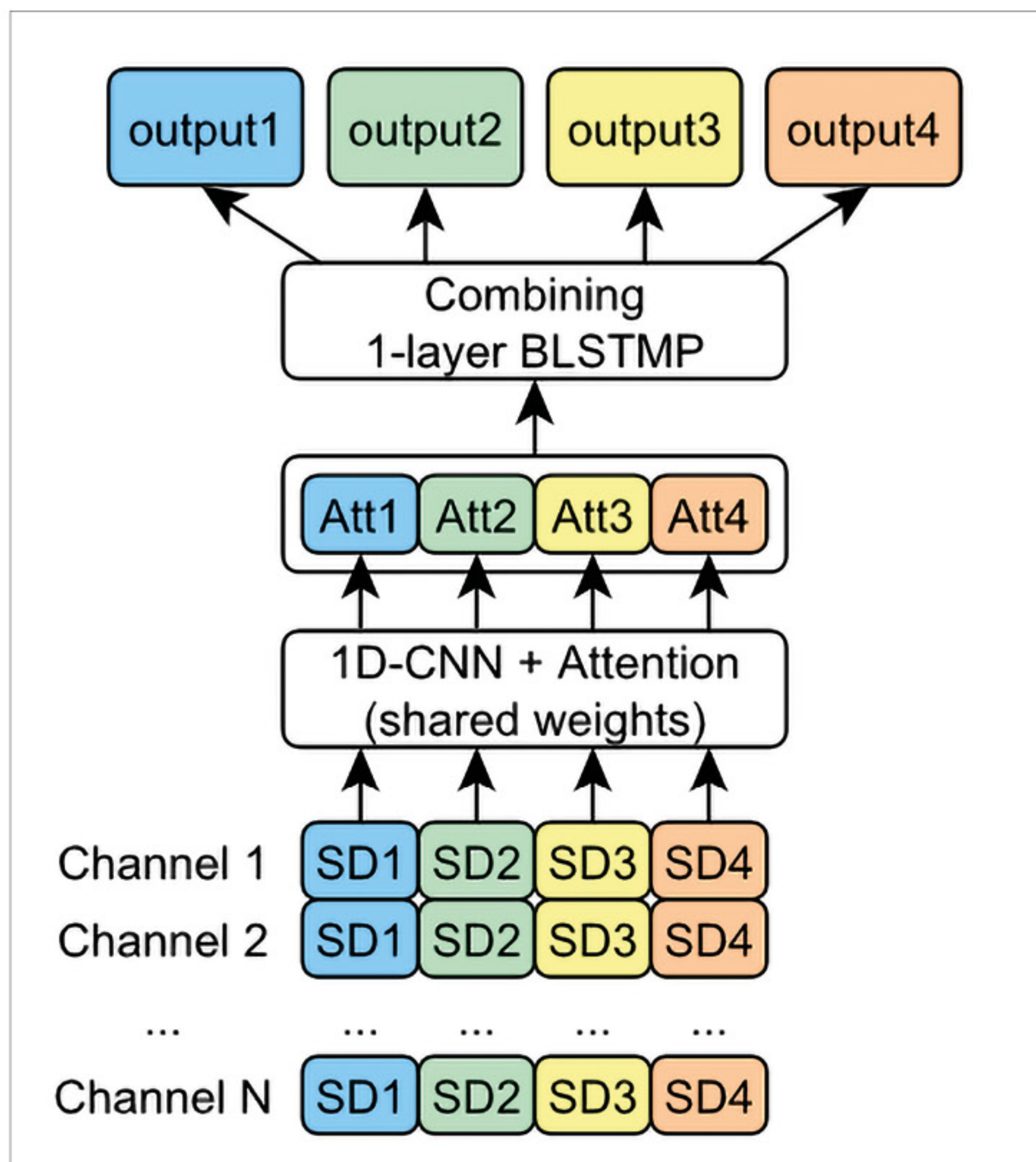


Рисунок 2. Схема предложенной многоканальной TS-VAD модели

10 каналам, комбинируются при помощи одномерной свёртки и простого механизма внимания. Результат этой комбинации подаётся в BLSTM слой и затем, как и в одноканальной модели, используется 4 слоя, отвечающие за бинарную классификацию наличия/отсутствия речи каждого из дикторов (рис. 2).

Ключевым фактором для предложенного TS-VAD подхода является точность оценки *i*-векторов для каждого диктора. Чтобы подсчитать точные *i*-векторы, требовалась хорошая диаризация, а, чтобы получить хороший результат диаризации, нужны, в свою очередь, точные *i*-векторы. Поэтому был использован итеративный подход к оценке *i*-векторов, схема которого представлена ниже. Для начальной итерации *i*-векторы для каждого диктора были построены на основе улучшенных *x*-векторов (WRN), вместо агломеративной иерархической диаризации АНС использовалась спектральная кластеризация SC, PLDA-score для сравнения *x*-векторов были заменены косинусным расстоянием (рис. 3).

Использование такого алгоритма позволило существенно улучшить показатели точности распознавания DER и JER по сравнению с базовой моделью как на наборе образцов, на котором можно было настраивать систему (development

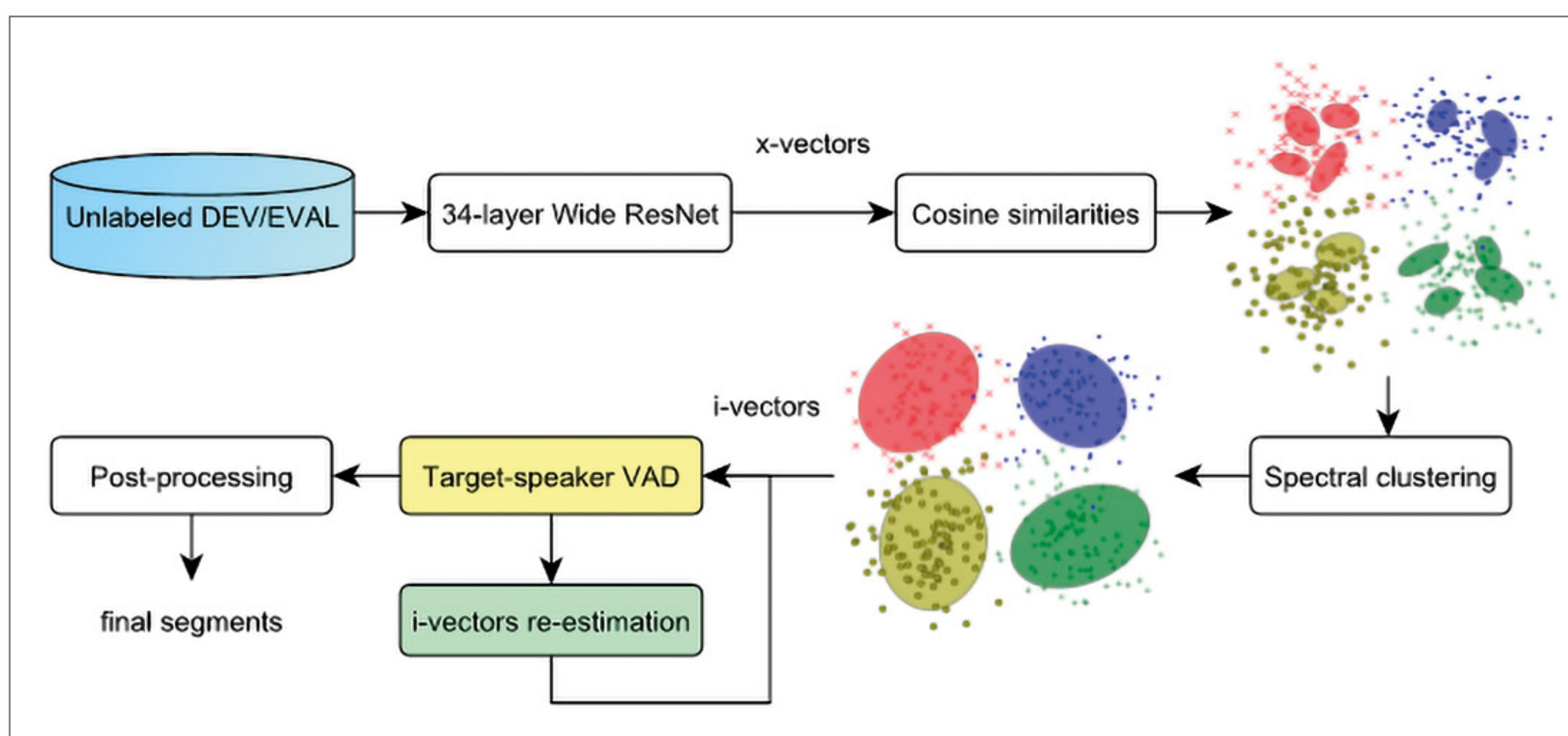


Рисунок 3. Общая схема алгоритма решения по распознаванию речи, представленного командой ЦРТ

	DEV		EVAL	
	DER	JER	DER	JER
x-vectors + AHC	63.42	70.83	68.20	72.54
WRN x-vectors + AHC	53.45	56.76	63.79	62.02
WRN x-vectors + SC	47.29	49.03	60.10	57.99
+ TS-VAD-1C (it1)	39.19	40.87	45.01	47.03
+ TS-VAD-1C (it2)	35.80	37.38	39.80	41.79
+ TS-VAD-MC	34.59	36.73	37.57	40.51
Fusion (best DER)	32.84	36.31	36.02	40.10
Fusion (best WER)	37.30	36.11	41.40	39.73

Рисунок 4. Полученные результаты различных методов, которые исследовала российская команда

set, DEV), так и на наборе для итогового тестирования (evaluation set, EVAL), что наглядно видно в приведённой таблице сравнения результатов различных исследованных методов (рис. 4).

СНИЖЕНИЕ ОШИБКИ

Как видно из таблицы, предложенный метод существенно снизил ошибку диаризации по сравнению с базовым решением на основе кластеризации дикторских эмбедингов. Полученная в итоге диаризация оказалась достаточно качественной для применения алгоритма GSS: по сравнению с GSS на идеальной диаризации, распознавание было хуже всего на несколько процентов по показателю WER. Далее было проведено обучение акустической модели на

наборе данных, состоящем из записей, полученных с использованием четырёх версий GSS с различными настройками, использована симуляция комнаты и другие возможности, включённые в базовое решение. Основная акустическая модель состоит из 9-уровневой сверточной нейронной сети (CNN), за которой следует 8-уровневая факторизованная нейронная сеть с временной задержкой (TDNN-F), использующая в качестве входных данных 80-мерные log Mel filterbank или gammatone filterbank. Также были использованы другие методы улучшения акустической модели, которые обеспечили дополнительное снижение показателя WER (рис. 5).

С ОТРЫВОМ ОТ КОНКУРЕНТОВ

Команда ЦРТ одержала победу в решении задачи второго направления со значительным отрывом от конкурентов (результат команды ЦРТ по показателю WER составил 43 %, результат команды, занявшей второе место — 68 %). Особенно стоит отметить то, что другими участниками соревнований выступали ведущие университеты мира, лидеры в развитии методов распознавания речи: университет Джонса

Хопкинса, научно-технический университет Китая, университет Падерборна, университет Брно, в то время как коммерческие компании обычно не принимают участия в подобных конкурсах (рис. 6).

Качественная обработка несегментированной речи позволит, к примеру, вести грамотное протоколирование совещаний, где говорят сразу несколько дикторов, а интеллектуальная речевая аналитика позволит автоматизировать работу контактных центров: распознавать спонтанную речь, классифицировать голосовые обращения, выявлять соблюдения скрипта, делать выводы об удовлетворенности клиента и качестве диалога, а значит — существенно оптимизировать работу современных контакт-центров ретейла, e-commerce, телеком, других отраслей.

Качественное распознавание речи отдельных дикторов, при этом перебиваемой шумами, позволяет выводить сервисы из разряда инновационных в повседневное применение, совершенствуя бизнес и упрощая нашу жизнь.

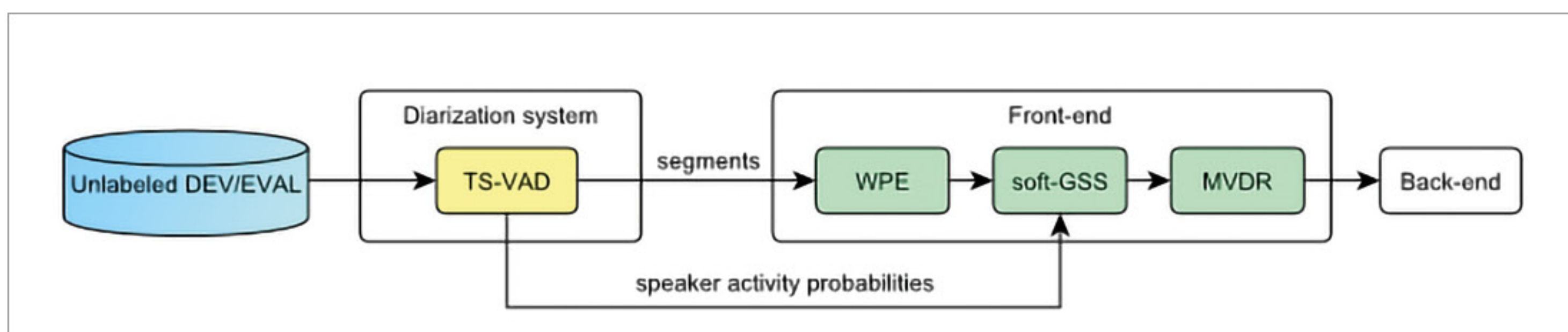


Рисунок 5. Общая схема акустической модели, предложенной командой ЦРТ

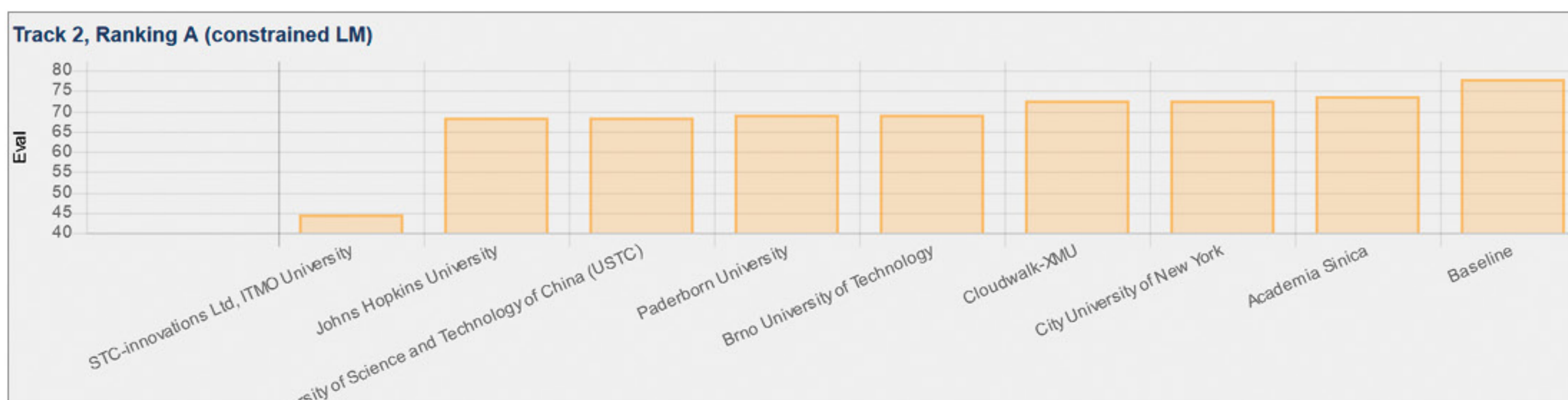


Рисунок 6. Итоговые результаты решения задачи второго направления по показателю WER, где меньшее значение показывает лучший результат (данные с официальной страницы результатов <https://chimechallenge.github.io/chime6/results.html>)

**Валерия МЕЩЕРЯКОВА**

студентка факультета журналистики МГУ им. М. В. Ломоносова

ИССЛЕДУЕМ ВИРУСЫ... АГРЕССИИ

ЗАЩИТА СОЦИАЛЬНЫХ СЕТЕЙ ОТКРЫВАЕТ
БЕЗОПАСНИКАМ НОВЫЕ ГОРИЗОНТЫ

Информационная безопасность в социальных сетях — тема сравнительно новая. Но не неожиданная, и уже достаточно разработанная. С 2018 года в ИПУ РАН при поддержке Российского фонда фундаментальных исследований ведётся работа над проектом с говорящим названием: «Разработка социокриберфизической системы мониторинга разнородного Интернет-контента в целях противодействия проявлению агрессии, давления и других форм деструктивного

воздействия на индивидуальное и групповое сознание пользователей». В проекте участвуют учёные из разных областей от социологии до IT и медицины.

Корреспондент BIS Journal Валерия Мещерякова встретила с участниками команды. На повестке дня: проблемные области информационной безопасности в социальных сетях, блокировка Telegram, востребованность специалистов по ИБ в связи с новыми реалиями и другие.

Сергей МЕЛЬНИКОВ, аналитик проекта

«ТЕХНОЛОГИИ ПОДДЕЛКИ НА КОНЕ»

О РАБОТЕ БЕЗОПАСНИКОВ

При реализации и внедрении социальных сетей существует несколько заинтересованных сторон, в том числе:

1. Разработчики соцсетей и различных сервисов на их базе.
2. Пользователи, которые во время пандемии стали уделять соцсетям больше времени.
3. Аналитики, которые изучают опубликованные в сетях материалы для своих целей.

В соответствии с этими направлениями требуются специалисты по информационной безопасности, которые могут и должны на всех этапах жизненного цикла работы выполнять свои обязанности.

Разной информации стало больше, её нужно анализировать и обрабатывать.

Ряд аналитических задач специфичны именно для специалиста по безопасности. Следует выделять как классические задачи по защите информации — обеспечение конфиденциальности, целостности и доступности информации в социальной сети, так и новые, в том числе проведение анализа и прогноза состояния социальной сети, её элементов и поведения участников информационного процесса. Анализ подлежат сообщения, связи, динамика коммуникационного обмена. Нужны толковые ребята и девушки, двоечники в таких постановках не слишком востребованы.

Социальные сети, конечно, будут бурно развиваться. Забот у ИБшников будет прибавляться. Это и традиционные (ключи, пароли, идентификаторы,

вирусы, социнженерия и проч.), и постепенно появляющиеся новые сущности. Я бы выделил две важные, которые могут серьёзно повлиять на ландшафт ИБшных задач:

1. биометрия;
2. производство и распознавание фейков.

О ПРОБЛЕМАХ СОЦСЕТЕЙ

Если говорить про фейки, то сегодня хорошо видно, что технологии подделки голоса, фото, видео, авторского стиля текста и близкие к ним развиваются семимильными шагами. Технологии (и особенно их внедрение!) распознавания фейков тоже развиваются, но, на мой взгляд, пока заметно отстают.

Поэтому скоро в области ИБ будет интересная история!

Какие именно виды опасностей подстерегают общество в сети? По этому вопросу я бы предоставил трибуну социологам и психологам. Со своей стороны отмечу возрастающий объём информации, который циркулирует в социальных сетях, и необходимость реализации формализованных методов обработки информации применительно к ним.

О БЛОКИРОВКЕ TELEGRAM

Я достаточно далёк от этой проблематики, но как мне представляется,

закон Яровой оказался в целом весьма полезен. Блокировка Telegram — это недалёковидная глупость. Если бы после запрета последовали конструктивные шаги в рамках какого-то плана, тогда это можно было бы понять. А поскольку ничего нет, то и говорить не о чем.

По поводу разблокировки. Можно предположить, что пришли к какой-то договорённости. Возможно, «техническая невозможность» предоставлять ключи переписки Telegram по запросу госорганов стала менее абсолютной.

По тематике нашего проекта отмечу, что в Telegram способы проявления агрессии ограничены, так как использования чатов, где можно обсудить материалы канала, почти нет. Это тоже вопрос к социологам, только собственно агрессия кого-то одного — это его личное дело. Страшно, когда эта агрессия доводится до широкой аудитории и заражает её. По Марксу, идея становится материальной силой, когда овладевает массами. А у социальных сетей технические средства для этого как раз имеются.

Анастасия ИСХАКОВА, руководитель проекта

«ВЫЯВЛЯЕМ ДЕСТРУКТИВНЫЙ КОНТЕНТ»

О ПАНДЕМИИ

Никто не ожидал, что этой весной мы все останемся дома, но это случилось. Понятно, что Интернет-трафик вырос в разы. При этом пользователи заметили, что популярные платформы подстроились под новый формат активности пользователей: ввели удобные интерактивные функции, дали возможность делать тематические отметки по ситуации в мире и т.д.

ОБ ОПАСНОСТЯХ

Что касается злоумышленников, то они всегда активно «работали» в соцсетях. В данной ситуации их можно разделить на подгруппы:

1. предлагают товары и услуги, например, средства защиты, лекарства и даже вакцины (в целом изменился только сам «товар»),
2. делают ложные провокационные «вбросы» недостоверных общественно значимых новостей, которые сейчас называют фейками.

Так как распространение такой информации с 2019 года преследуется по закону, конечно, востребованность специалистов для поиска и установления нарушителей возросла на фоне пандемии и массовых фейков, целью которых являются паника, перевертывание данных, пропаганда и подрывание доверия к органам власти.

Распространение недостоверных новостей происходит стремительно,

лавинообразно, используются популярные мессенджеры. Именно в этом сложность поиска первоисточника — правонарушителя, который первым запустил недостоверный пост. Этим в том числе занимаются и специалисты в области ИБ. Также группы специалистов, включая и специалистов по ИБ, занимаются недопущением таких явлений в принципе — разрабатывают превентивные меры, которые не допустят фейки до пользователя.

В виртуальной среде пользователю может быть нанесён различный вред:

1. моральный — травля, унижение, агрессия, пропаганда, введение в заблуждение;
2. физический — следствие форм морального давления, проявляющееся в ухудшении физического состояния пользователя;
3. финансовый — попрошайничество, обманы, выведывание информации, взломы аккаунтов.

Каждый злоумышленник имеет собственную цель в виртуальной среде. Что касается первых двух пунктов, то борьба с ними сложна, так как и проявление такого вреда сложно формализуемо, слабо доказуемо и редко подвергается огласке. В нашем Институте проводится сложная комплексная работа с привлечением специалистов в области социологии, психологии, медицины, математики, IT, одной из задач

которой является автоматизация выявления фактов агрессии, давления, унижения в Интернете.

О ПРОЕКТЕ

Чтобы не терять пользователей и быть актуальными и востребованными, социальные сети подстраиваются под реалии общества. Наличие мошенников и злоумышленников нежелательно для ресурсов — это отпугивает людей и снижает доверие, поэтому многие соцсети разрабатывают и внедряют системы распознавания подозрительного поведения. Данное направление очень широкое, оно затрагивает много неправомерных, некорректных форм поведения, фильтрацию контента и т.д. Например, в рамках нашего проекта ведётся разработка актуальных интеллектуальных алгоритмов, выявляющих контент, деструктивно влияющий на состояние пользователя в Интернете — это также является одним из направлений модернизации и развития социальных сетей. С применением машинного обучения мы создаём алгоритмы выявления различных видов контента, который может негативно влиять на состояние человека. Это и текст, и графические изображения, и звуковые потоки. Комплексный подход позволяет отрабатывать разнородный контент и выявлять искомые экземпляры.

Ирина КУЛАГИНА, социолог проекта, доцент кафедры философии и права СурГУ

«РЕЧЬ ИДЁТ НЕ О ЦЕНЗУРЕ»

О ПРОБЛЕМАХ В ВИРТУАЛЬНОМ МИРЕ

В отличие от окружающего мира, где мы легко ориентируемся, в социальных сетях и мессенджерах нельзя определить не только то, от кого именно исходит та или иная информация, но и какова её социальная значимость и можно ли ей доверять. Допустим, вы видите человека определённого типа в определённых социальных условиях. Вы можете защититься от него так. Сказать: «Я игнорирую такой тип людей и любую информацию, идущую от него». А в сети привычные маркеры идентификации отсутствуют, поэтому в любом случае придётся сперва прочитывать текст (поскольку сразу не можете его отсеять). Это и есть главная проблема современных пользователей: социальные отношения есть текст.

Пользователю сложно определить откуда исходит опасность/агрессия в интернете, а также понять, выражает ли человек свою позицию либо чужую. Например, сейчас очень распространены обороты «как бы», «с высокой долей вероятности», «по оценкам экспертов» и т.п., которые отражают интенсивность воздействия на сознание пользователя сети. На самом деле, сознание человека умеет исключать некоторые элементы из восприятия и тем самым изменять процесс понимания текста. И вот вы уже верите в эту информацию, игнорируя даже то, что она была подана как сомнительная.

Это значительная проблема, ведь не у всех есть навыки квалифицированной интерпретации текста, как и навыки критического анализа информации.

Есть такая разновидность мировоззрения — мифологическое. Это мировоззрение часто определяет сознание человека. В итоге мы не оцениваем достоверность аргументов, не ищем истину, а просто расфасовываем полученную информацию в две кучки: это похоже на то, что я уже знаю, совпадает с моей позицией, а это — нет. Так, вторую кучку наше сознание сразу с готовностью рассматривает как

недостоверную, не требующую анализа, нелегитимную. И, поверьте, так действуют очень многие люди, ведь мифологическое мировоззрение есть у каждого, а противостоять его давлению надо ещё научиться.

Резюмируя главные проблемы, связанные с социальными сетями:

1. Любая информация подаётся в чистом виде, иной раз она лишена даже редакции самим автором и выглядит как поток чьего-то сознания. Часто информация в социальных сетях не подвергается модерированию, а значит, именно обыденному пользователю необходимо научиться её фильтровать и воспринимать.

2. Проблема авторства, источника информации и её достоверности. В электронной коммуникации чаще всего мы не имеем сведений об авторе сообщения и его целях, часто не владеем тезаурусом (предметным словарём), не можем понимать, о чём он говорит, а значит, привычно замещаем его высказывание своей интерпретацией. Это одна из проблем наших современников, игнорирующих чтение литературы, решение философских вопросов, и ориентированных на чтение социальных стримов.

3. Социальное давление или проблема толпы. Ещё Гюстав Лебон писал, что человек присоединяется к мнению большинства, чтобы сохранить себя. А большинство в социальных сетях обеспечено кем? Как правило, это может быть 3–4 человека, изредка 10–20. Однако, как это часто видно при контент-анализе, на самом деле это не большинство, а просто количественное преимущество сообщений (созданных этими 3–4 людьми). Таким образом, в электронной коммуникации человек не видит реальной статистической картины, ему кажется, что раз так много написано и в одном ключе — такова и есть картина мира. А то, что противоречивые мнения не высказаны, или отмодерированы, или остались в меньшинстве в потоке манипулирующих сообщений, — это ему не видно.

О ПРОЕКТЕ

Я участвую в проекте как социолог, а социология — наука, занятие безоценочное. Вот возникла потребность классифицировать проявления агрессии, и мы в первую очередь должны понимать, что демонстрация агрессии — неотъемлемая часть психологии человека и животных, она несёт и защитную функцию, служит маркером манипуляций над сознанием людей.

Когда мы анализируем проявления агрессии в концентрированном виде (для исследования), мы выявляем манипулятивные приёмы, которые применяют участники коммуникации. Например, мы уже знаем, что существуют разные типы пользователей:

- ♦ открытые (можем их найти в реальной жизни), с конкретной личностной позицией, очевидными данными, указывающими на их реальность в социальных отношениях за пределами электронной коммуникации;

- ♦ трудно определяемые либо не идентифицируемые, анонимные, «по папе».

Агрессия часто связана либо с потребностью в манипуляциях сознанием других людей («провокативная»), либо с проявлением внутреннего, часто не осознаваемого или просто вырывающегося из-под контроля состояния индивида. Нам кажется, что избранный для использования в электронной коммуникации тип пользователя связан с определённым типом его поведения. Полагаю, что анонимизированных пользователей стоит отслеживать и контролировать, так как именно они способны к генерации социально-опасных процессов, социально-психологическому давлению, подстрекательству к противоправным и антисоциальным действиям.

Одна из задач исследования — обнаружить условия для агрессивных манипуляций информацией, чтобы в дальнейшем заставить пользователей обратить внимание на необходимость критического мышления в отношении любой информации в социальных сетях. Особенно это актуально для детской неокрепшей психики, некритического сознания,

подверженного той самой мифологической картине мира, где есть только удобная и понятная пользователю истина.

О БУДУЩЕМ СОЦИАЛЬНЫХ СЕТЕЙ

Говоря о ближайшем будущем, учёные должны предвосхищать размах информационных манипуляций в условиях, когда возрастает значение социально изолированных форм повседневности. Посмотрите, ведь в пандемии, например, растёт роль электронной коммуникации, а её приоритет над традиционным общением становится очевидным. Вопрос сегодня должен стоять не о цензуре, хотя человечеству не известно ни

одного государства, где цензура исчезла, где утрачен контроль за осуществлением манипуляций над массовым сознанием, сферой социальной коммуникации.

Ограничения в адрес социальных мессенджеров и сетей часто носят культурно-исторический и социально обусловленный характер, позволяя охранять те стереотипы и установки, от которых зависит поддержание порядка и устойчивое развитие данного типа социальной организации.

Мы должны готовить людей к первичной установке на логическую фальсификацию суждений социальных сетей и мессенджеров — проверке на ложь, установке, что любое суждение

изначально следует воспринимать как не истинное, фейковое, чтобы в дальнейшем находить способы убедиться в том, что есть достаточно условий для доверия или недоверия.

Здесь мы должны смотреть шире и видеть не только политические задачи государства в охране своего стабильного существования, но и потребность в культурной защите от деградации, манипуляции детским сознанием, игнорировании потребностей в развитии критической формы мышления, разжигании ненависти и детерминации агрессии, бунта или насилия как единственного способа решения социальных задач.

Роман МЕЩЕРЯКОВ, научный консультант проекта

«БЕЗОПАСНИКИ ОСВОЯТ МНОГО НОВОГО»

ОБ ИБ И ПАНДЕМИИ

Специалисты по информационной безопасности являются важным элементом в системе защиты информации в социальных сетях. На их плечах лежит ответственность за сохранение персональных данных, конфиденциальной информации. При этом необходимо понимать, что важно не только защищать конкретную информацию в текущий момент времени, но и предполагать атаки на пользователя, проводить аналитическую работу по потенциальным уязвимостям. Очевидно, когда количество пользователей увеличивается, возрастает и нагрузка на специалиста по защите информации. С другой стороны, специалисту по информационной безопасности требуется расширение спектра навыков, которые нужны для работы: знание основ искусственного интеллекта, работы с большими данными, основ психологии и социологии, а также аналитики.

ЧТО ЖДЁТ СОЦИАЛЬНЫЕ СЕТИ

Прогнозировать развитие социальных сетей — дело неблагодарное. Я считаю, что социальные сети будут и дальше проникать в жизнь человека: встраиваться в повседневность, заменяя собой

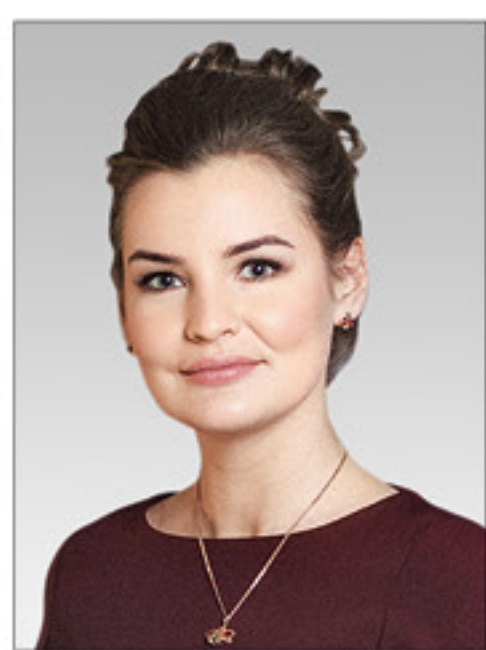
привычные действия. Речь не только об общении, но и об использовании торговых и банковских сервисов, индустрии развлечений, играх, радио, телевидении, а также об увеличении объёма удаленной работы и дистанционном обучении. Я, например, использую социальные сети для решения некоторых рабочих вопросов. Конечно, так делать неправильно, и я не рекомендую, но эффективно.

Основные опасности подстерегают пользователя на этапе общения и выбора собеседника — будь то конкретный пользователь или официальный ник организации или коллектива. Легко можно попасть на разводилу, который, используя фальшивую информацию, может воздействовать на человека и принуждать/убеждать/просить/требовать/уговаривать совершить нежелательные действия или войти в плохое состояние. Используя методы социальной инженерии, можно получить доступ к аккаунту и от имени пользователя вести беседы и формировать общественное мнение, в некоторых случаях можно получить доступ к конфиденциальным данным, включая банковские сведения. Ряд пользователей провоцирует других на агрессию для достижения больших показателей кликабельности, переходов, лайков и других

показателей активности. Очевидно, что данные показатели могут быть монетизированы, а негатив драки кошки с собакой вызывает более активную реакцию, чем кошечка на дереве.

ОБ ИДЕЕ ПРОЕКТА

Классификация и оценивание агрессивных комментариев и постов — это отдельная сложная задача. При этом формализация проводится на уровне как ключевых слов, так и семантических отношений. Ещё одним из способов оценивания являются количество и качество ответов, которые характеризуют степень тяжести агрессии. Обобщённо цель исследования можно сформулировать как разработку подходов и методов определения агрессии в сети интернет. Вместе с тем важно не только выявлять агрессию, но и противодействовать ей. Чем раньше агрессия обнаруживается, тем больший шанс мирного разрешения противоречий без перехода на личности и угрозы. Необходимо помнить, что в любой ситуации мы должны оставаться людьми. Сотрудники соцсетей в проект привлекаются как в роли экспертов, так и в роли подопытных, на которых определяется степень возникающей агрессии при просмотре сайтов.



Дарья САВЕНКОВА
руководитель
направления
Управления
противодействия
кибермошенничеству
Сбербанка

ТЕЛЕФОННЫЙ РАЗВОД

В БОРЬБЕ С МОШЕННИКАМИ-«ЗВОНАРЯМИ»
НЕОБХОДИМ КОМПЛЕКСНЫЙ ПОДХОД

Россияне всё чаще жалуются на звонки от неизвестных, которые представляются сотрудниками различных банков, медицинских учреждений, госструктур, рассказывают о компенсациях и подозрительных операциях.

Сначала они просят назвать номер карты «для зачисления компенсации», что обычно не вызывает подозрений, а на следующий день — сообщить «номер заявки, который пришёл вам с

номера телефона банка» для зачисления денег на счёт, и так далее. Эти неизвестные — телефонные мошенники.

Используя практически любой информационный повод для звонка, преступники массово вооружаются телефонами и начинают атаку на граждан. Масштабы такого мошенничества поражают. В условиях, когда практически все граждане пользуются банковскими цифровыми продуктами, злоумышленник просто может наугад

перебирать номера телефонов. Если один человек сразу положит трубку, то другой, более доверчивый и менее финансово грамотный, выдаст мошенникам всю необходимую им информацию.

КЛЮЧЕВЫЕ ЦИФРЫ

По данным МВД России, в 2019 году было совершено почти 300 тысяч преступлений с использованием различных информационных технологий, что на 68,5% больше, чем за аналогичный период 2018 года. На 130% чаще стали регистрироваться преступления, связанные с использованием банковских карт. И на 91% возросло количество мошенничеств с применением мобильных телефонов.

Согласно статистике правоохранителей, за пять месяцев 2020 года число киберпреступлений в России выросло на 85%, а количество преступлений, совершённых с использованием пластиковых карт, — в шесть раз.

ПРЕСТУПЛЕНИЕ БЕЗ НАКАЗАНИЯ

Только совместно со службой кибербезопасности Сбербанка правоохранительным органам удалось в 2019 году ликвидировать 31 такую преступную группу, 82 подозреваемых задержано. Однако прилагаемые со стороны банка усилия и кропотливый труд полиции не решают комплексной проблемы, а именно того, что в нашей стране до сих пор фактически нет ответственности за киберпреступления.

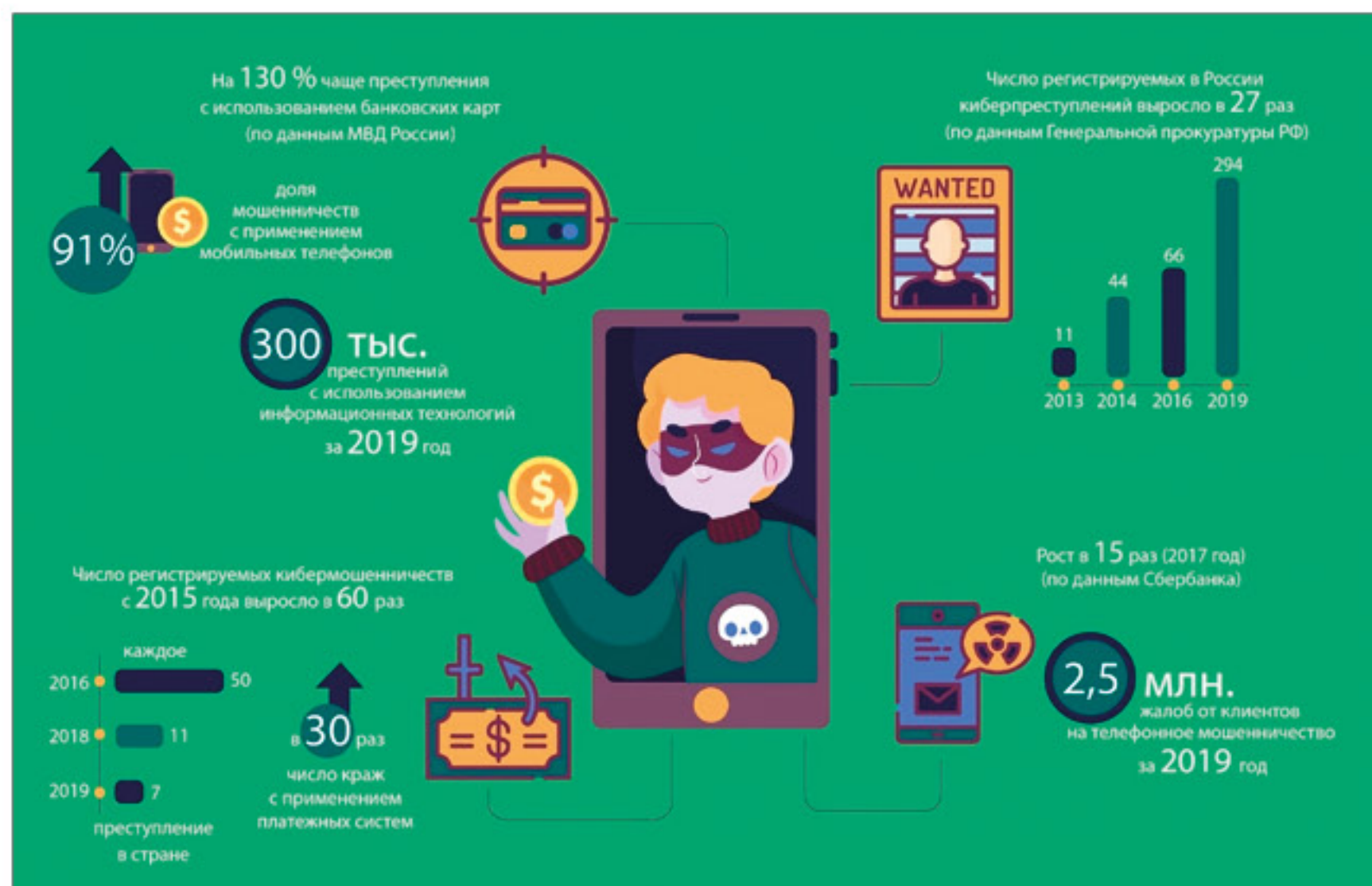
Российские суды относятся к ним крайне либерально: совершить ограбление банка с автоматом в руках и вынести три миллиона в сумках — это до 15 лет лишения свободы, а вывести с банковской карты три миллиона через интернет — два года условно. Таким образом, даже у тех, кто изначально не был настроен на криминальные действия, может возникнуть соблазн попробовать новый лёгкий способ «заработать» деньги.

ЗВОНОК ИЗ ТЮРЬМЫ

На территории мест лишения свободы действуют целые кол-центры. Только в 2018 году в учреждениях уголовно-исполнительной системы было изъято 56 249 единиц средств связи¹. Вопрос о незаконном использовании сотовой связи в местах лишения свободы вызвал острую дискуссию, когда в январе этого года депутаты внесли в Госдуму законопроект № 876381–7².

¹ <https://sozd.duma.gov.ru/bill/876381-7>

² «О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории учреждений, исполняющих уголовные наказания в виде лишения свободы, и мест содержания под стражей».



Динамика роста киберпреступности в России

Очевидно, что одна из главных причин данной инициативы — преступления, которые совершают заключённые с помощью мобильных телефонов.

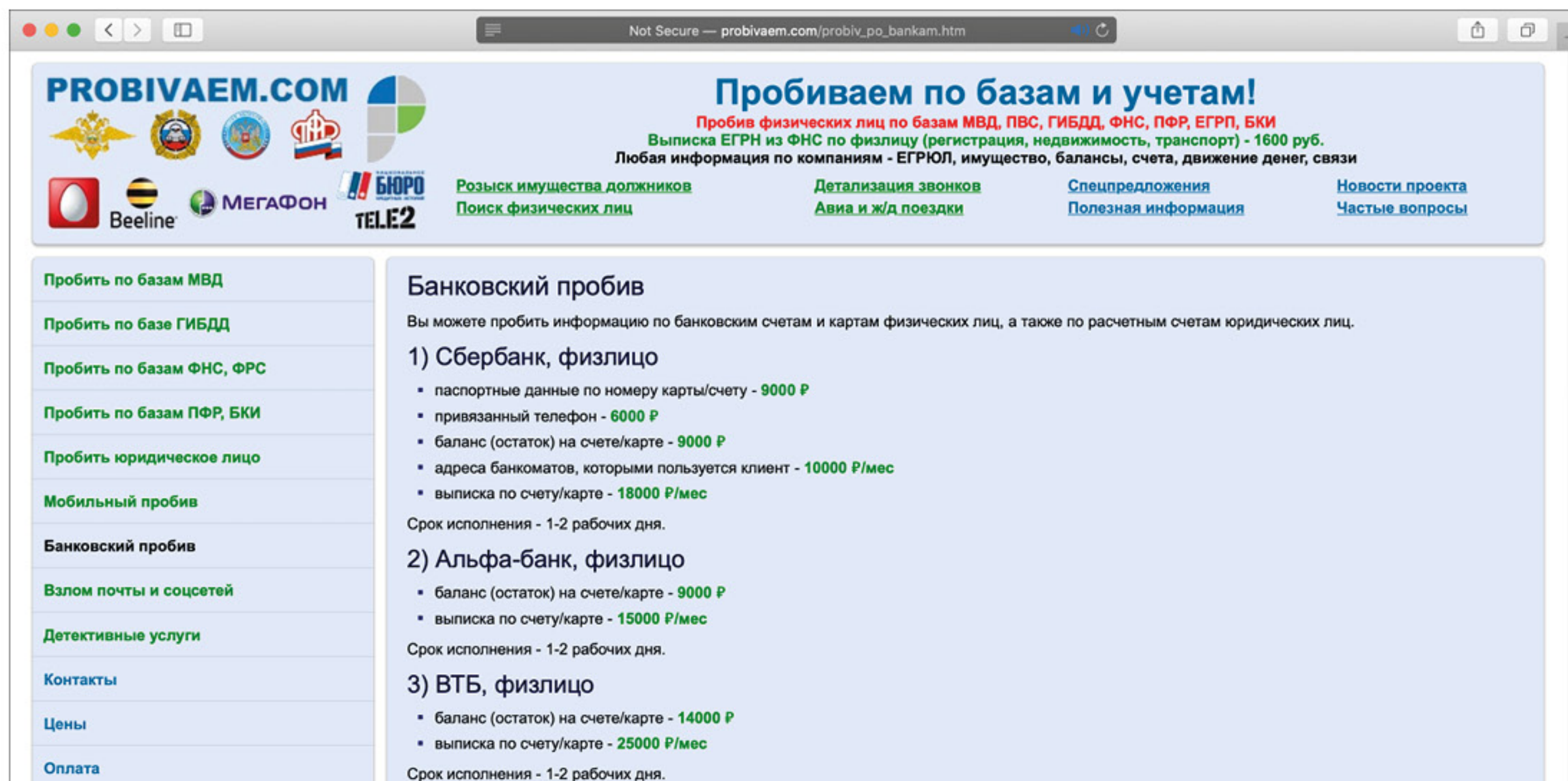
Примеров много, но наказания редки и не соответствуют масштабам преступлений. Так, в минувшем апреле вынесен приговор начальнику отдела колонии в Оренбурге, который обеспечивал осуждённых преступников телефонами и незарегистрированными сим-картами, а также предоставил комнату для телефонных звонков. Решением суда организатор признан виновным с назначением наказания в виде штрафа в доход государства в размере 50 000 рублей и лишением права занимать должности в органах ФСИН России на срок два года.

ИНФОРМАЦИЯ КАК ОТМЫЧКА

Зачастую от пострадавших можно услышать следующее: «Ко мне же обратились по имени и отчеству, сообщили достоверные сведения обо мне, и здесь я подвоха не увидел...»

Действительно, чтобы войти в доверие к жертве, злоумышленники меньше спрашивают, а больше говорят сами: называют анкетные и паспортные данные, номер карты и даже остаток по ней! При желании такую информацию можно купить в даркнете, на хакерских форумах или заказать «пробив» в телеграм-каналах. Но и сами пользователи оставляют слишком много следов в интернете: пересылают фотографии своих карт, сканы паспортов и другую важную информацию в социальных сетях и мессенджерах.

Учитывая, что доступ к персональным данным стал практически свободным, мошенник уже не обращает особого внимания на то, кого и на сколько ему обворовать. Небольшими



Мошеннический ресурс по сбору данных банковских клиентов

суммами красть даже выгоднее, поскольку ставка на массовость телефонных звонков делает своё дело и в конечном счёте приносит большие заработки.

Очевидно, мошенникам известно, что, если размер причинённого ущерба меньше 2500 рублей, привлечению к уголовной ответственности они не подлежат³. И это позволяет им при наличии большого объёма данных практически безнаказанно массово обворовывать граждан на мелкие суммы.

КАК ПРЕДОТВРАЩАТЬ?

Самый действенный метод борьбы с телефонными мошенниками — это информирование граждан. Предупреждён — значит вооружён.

Чтобы не попасться на уловки злоумышленников, достаточно помнить несколько простых правил.

Во-первых, не действовать по указке позвонившего. Помнить, что бесплатный сыр бывает только в мышеловке.

Во-вторых, не спешить называть данные своей банковской карты или переводить деньги.

В-третьих, уточнять информацию, позвонив по номеру горячей линии организации, сотрудником которой представляется позвонивший. Обязательно посоветоваться с близкими, не принимать необдуманных решений. Помнить,

что задача мошенников — не дать жертве всё обстоятельно обдумать⁴.

ЧТО В МИРЕ

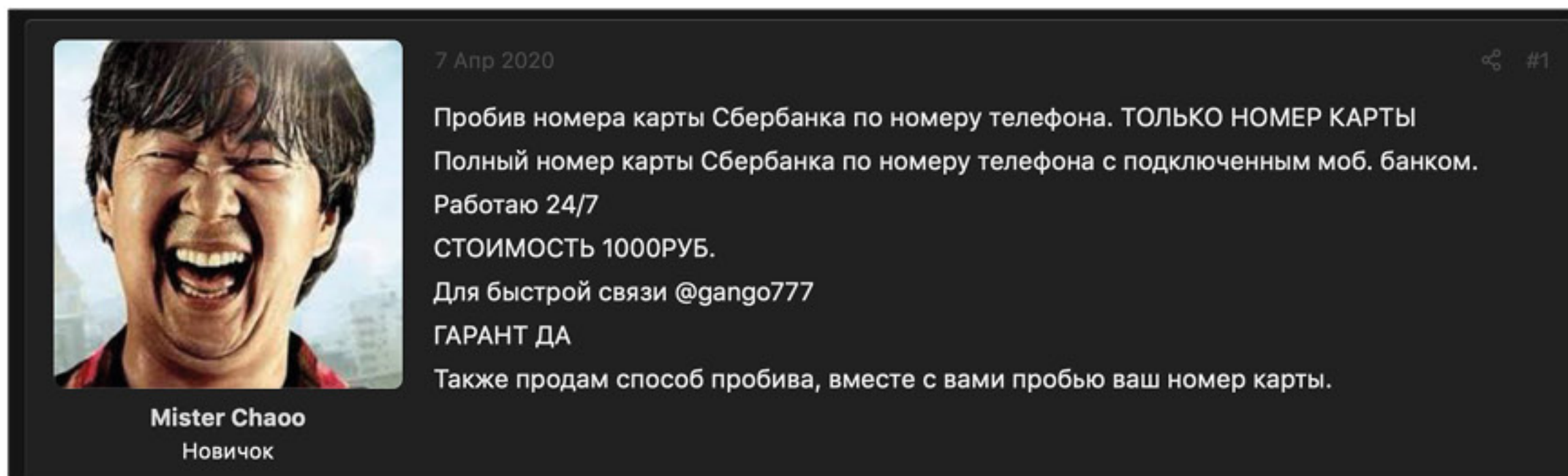
Проблема телефонного мошенничества актуальна не только для России — у неё мировой масштаб. Как правило, злоумышленники используют ограниченный набор схем, суть которых одна — получить конфиденциальные данные, а затем украсть деньги.

Кража личности. 21 января 2020 года Центр по рассмотрению жалоб на преступления в интернете ФБР опубликовал предупреждение о том, что мошенники стали использовать поддельные порталы и веб-сайты с заявлениями о приёме на работу для кражи личной информации, включая данные платёжной карты у потенциальных кандидатов. Согласно данным Центра, мошенничество, направленное на соискателей работы в США, с начала 2019 года неуклонно растёт. Потери жертв в среднем составляют около 3000 долларов США.

Подмена номера. Мошенники используют технологию так называемого спуфинга: так, чтобы на телефонах высвечивались номера администрации социального обеспечения или других официальных учреждений. Иногда они даже используют имена настоящих служащих этих агентств.

³ Мелкое хищение чужого имущества стоимостью более одной тысячи рублей, но не более двух тысяч пяти сот рублей путём кражи, мошенничества влечёт административную ответственность по ч. 2 ст. 7.27 КоАП РФ.

⁴ Более подробно ознакомиться с правилами безопасности можно на сайте Сбербанка: https://www.sberbank.ru/ru/person/dist_services/cybersecurity



Мошеннический ресурс по сбору данных банковских клиентов

Разновидность этой схемы была зафиксирована в Сингапуре: пользователи биткоин-банкоматов звонили по номерам, наклеенным на машинах. Теперь в Сингапуре может быть зарегистрировано не более трёх номеров на одного абонента (вне зависимости от оператора связи).

А в Германии ежедневно происходят сотни случаев мошенничества с «лжеполицейскими», когда мошенники выдают себя за сотрудников полиции и выманивают у людей деньги.

В одной только земле Северный Рейн-Вестфалия в 2018 году фальшивые полицейские «заработали» больше 7 млн евро. По данным Федерального управления уголовной полиции, особенно часто жертвами аферистов становятся пенсионеры.

Так, 89-летней Элизе из Аугсбурга позвонили из «государственной канцелярии»: на дисплее отобразился номер полиции «110». Ей рассказали о коррумпированном работнике банка и потребовали, чтобы женщина сняла со своего счёта 15 000 евро, которые якобы являются фальшивыми, и отдала полицейскому. Пожилая женщина выполнила все требования. Она настолько доверилась звонившему, что даже ничего не рассказала своей дочери. Человека, который пришёл за деньгами, удалось выследить по геолокации телефона. Его задержали и приговорили к 26 месяцам тюрьмы.

ЧТО ДЕЛАТЬ?

Решением рассматриваемой проблемы озадачены как бизнес-сообщество, так и государство.

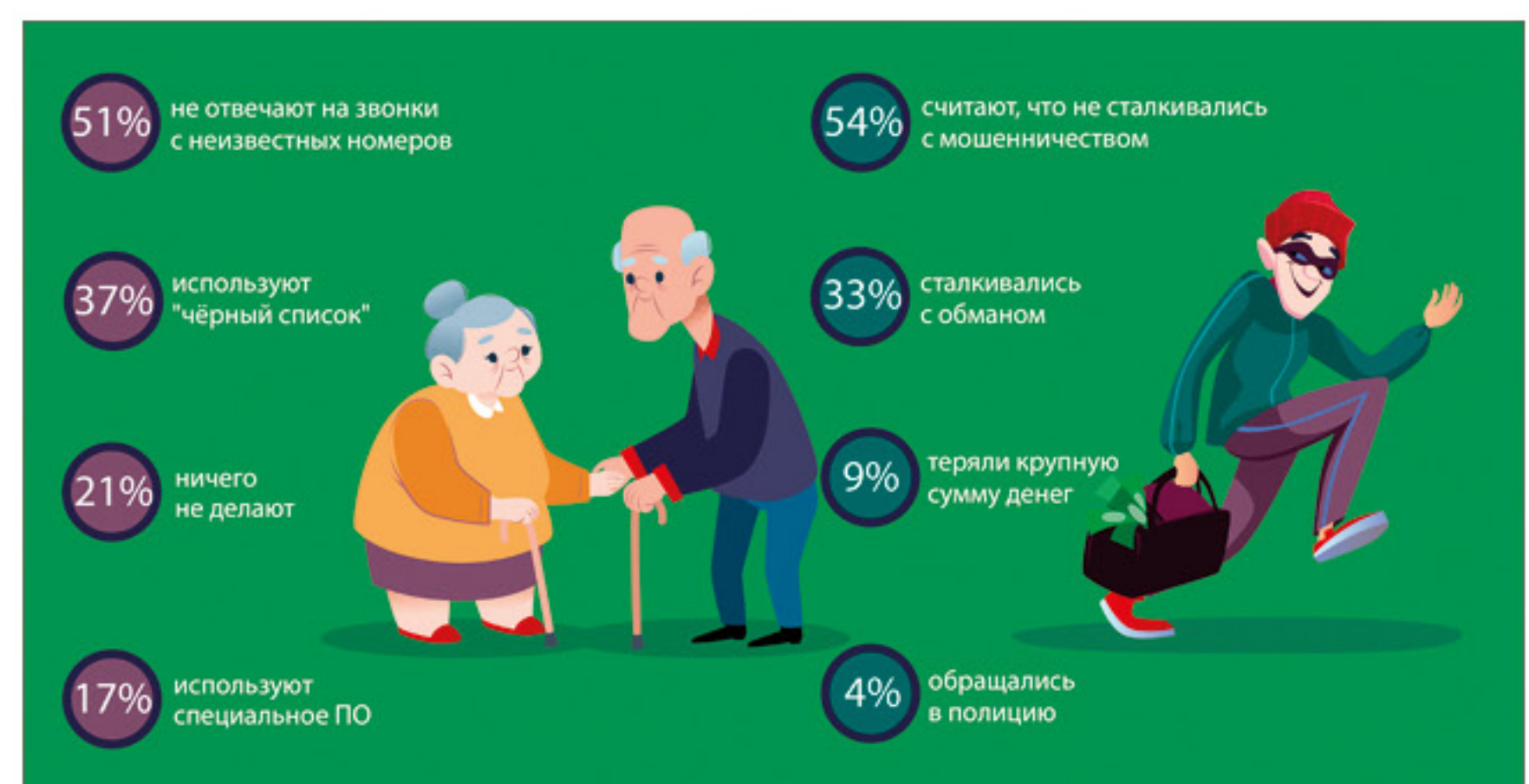
Так, 17 апреля 2020 года первый замглавы комитета Совета Федерации по обороне и безопасности Владимир Кожин в ходе заседания палаты сообщил о планах подготовить и внести в период весенней сессии Государственной думы РФ поправку в Уголовный кодекс РФ об ужесточении ответственности за киберпреступления. В ответ на это предложение спикер Совета Федерации Валентина Матвиенко поручила подготовить поправки в Уголовный кодекс РФ для

ужесточения борьбы с кибермошенничеством. Разработать поправки должны комитеты Совета Федерации по обороне и безопасности, а также по конституционному законодательству и госстроительству.

Увеличение количества телефонных мошенничеств требует активизации работы правоохранительных органов, в том числе и по совершенствованию законодательной и нормативной базы, позволяющей выстраивать наиболее эффективные алгоритмы выявления, раскрытия и расследования киберпреступлений.

Для быстрой и эффективной поимки киберпреступников важно наладить взаимодействие между банками, операторами мобильной связи, интернет-провайдерами и правоохранительными органами.

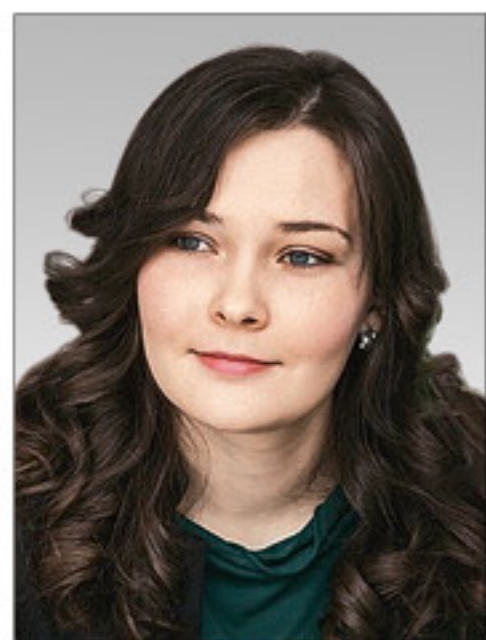
Решать проблему нужно комплексно, и, конечно, необходимо повышать уровень финансовой грамотности населения, организовывать массовые кампании по информированию о случаях мошенничества, создавать на государственном уровне эффективные подразделения, специализирующиеся на борьбе с такого рода преступностью.



Способы защиты от телефонного мошенничества и его последствия

КЛИЕНТЫ ЗНАЮТ МАЛО. ПОЧЕМУ?

ОЦЕНКА КАЧЕСТВА ИНФОРМИРОВАНИЯ КЛИЕНТОВ БАНКОВ ОБ АКТУАЛЬНЫХ УГРОЗАХ ИБ



Ольга ЛИМОНОВА
психолог
ООО «Антифишинг»

С каждым годом в России становится больше людей, у которых украли деньги с банковского счёта. Используя социальную инженерию, киберпреступники воздействуют на своих жертв, заставляя их сообщить конфиденциальную информацию или выполнить другие действия, приводящие к хищению средств.

Поскольку явление носит массовый характер, Центральный Банк РФ и банки пытаются защитить своих клиентов. Для этого они разрабатывают различные методические указания и брошюры, добавляют оповещения на сайты онлайн-банкинга и в мобильные приложения. Все эти оповещения решают одну задачу: предупредить клиентов об опасности, рассказать о том, как не стать жертвой мошенников.

Однако, несмотря на эти мероприятия и на бодрые отчёты на ИБ-конференциях, количество мошеннических инцидентов в финансовой сфере не уменьшается. Причиной этого может быть либо отсутствие достаточного количества оповещений, либо их неэффективность.

Мы выяснили, как обстоят дела с информированием об актуальных угрозах ИБ с точки зрения клиентов банков. Представляем результаты проведённого исследования.

КЛИЕНТСКАЯ БЕЗОПАСНОСТЬ КАК ЧАСТЬ СЕРВИСА

Безопасность — один из важнейших критериев, по которым клиенты выбирают банки. Однако,

несмотря на значимость этого критерия, информирование об угрозах до сих пор не является обязательной составляющей взаимоотношений банков с клиентами. Косвенным фактом, подтверждающим это, является отсутствие авторитетных российских исследований, посвящённых анализу качества информирования банками клиентов об актуальных ИБ угрозах и новых видах мошенничества.

Качество клиентского обслуживания прямо пропорционально удовлетворённости клиентов. Высокая удовлетворённость означает, что качество обслуживания находится на высоком уровне. Именно поэтому в качестве критерия уровня информирования в нашем исследовании мы использовали оценку, которую давали клиенты.

Ценность такого подхода для банков состоит в том, что удовлетворённость клиентов является важным конкурентным преимуществом, способствуя развитию кредитной организации и увеличению прибыли. Таким образом, информирование об угрозах — неотъемлемая часть клиентского сервиса, реализуемого в рамках операционной стратегии банка (рис. 1).

В идеале качество информирования должно соответствовать ожиданиям клиентов или опережать их.

ОПЫТ СТОЛКНОВЕНИЯ КЛИЕНТОВ С МОШЕННИКАМИ

В данном исследовании приняли участие более 100 человек из Москвы и Санкт-Петербурга. Среди опрошенных было 43,9% женщин и



Рисунок 1. Удовлетворённость клиентов является важным конкурентным преимуществом, способствующим развитию кредитной организации и увеличению прибыли. А информирование об угрозах — неотъемлемая часть клиентского сервиса, реализуемого в рамках операционной стратегии банка

56,1 % мужчин. Средний возраст респондентов составляет 32 года. Все являются клиентами одного и более российских банков. Принадлежность к конкретным банкам не указывается, поскольку была поставлена задача собрать «среднюю температуру по больнице» и избежать негатива по отношению к какому-либо конкретному кредитному учреждению.

Согласно результатам опроса, более 55 % респондентов имели опыт общения с мошенниками, причём 7 % из них столкнулись с реальными хищениями денег со своих банковских счетов.

Основные виды мошенничества, с которыми респонденты сталкивались и смогли вспомнить (повторные инциденты не засчитывались):

- ◆ Телефонный фишинг (звонки от «сотрудников банка», «покупателей» с Авито и т.д.) — 37,3 %;
- ◆ СМС-фишинг — 11,2 %;
- ◆ Сообщения от взломанных социальных страниц знакомых — 6,5 %;
- ◆ Предложения в реальной жизни от «серых» промоутеров — 2 %;
- ◆ Фишинговые сайты — 2 %;
- ◆ Блокировка SIM-карты по ложному заявлению об утере — 1 %;
- ◆ Скиммер — 1 %.

Способы борьбы с мошенниками, которые использовали респонденты:

- ◆ игнорирование;
- ◆ обрыв контакта/общения;
- ◆ высмеивание/троллинг;
- ◆ нецензурная брань;
- ◆ уверенное общение;
- ◆ информирование, что «денег нет»;
- ◆ запрос информации по счёту/карте/договору;
- ◆ проверка счёта через личный кабинет;
- ◆ блокировка или перевыпуск банковской карты;
- ◆ звонок в банк, друзьям или близким;
- ◆ жалоба администрации на скомпрометированные страницы в социальных сетях с последующей блокировкой;
- ◆ отказ от использования банковского мобильного приложения;
- ◆ заявления в службу безопасности банка.

Из описанных способов противодействия мошенникам мы видим, что респонденты используют самые разные варианты поведения. Большая их часть соответствует рекомендациям ИБ, но также наблюдаются и малоэффективные стратегии. Проактивные методы борьбы использует меньше четверти людей, в то время как большинство предпочитает стратегию игнорирования даже без занесения «надоедающих номеров» в «чёрный список».

При этом на вопрос о том, какие меры информационной защиты респонденты знают, были даны следующие ответы:

- ◆ Не знают, затруднились ответить — 19,6 %;
- ◆ «Не быть тупым», «никому не верить» — 9,3 %;
- ◆ Не раскрывать никому конфиденциальные данные — 26,1 %;
- ◆ Хороший пароль — 24,3 %;
- ◆ Двух-трёхфакторная аутентификация — 23,3 %;
- ◆ Антивирус — 14 %;
- ◆ Использование сложных паролей — 13 %;
- ◆ Использование биометрии — 12,1 %;
- ◆ Регулярная смена паролей — 9,3 %;
- ◆ СМС-оповещения — 9,3 %;
- ◆ Не записывать пароли и не хранить их в доступных местах — 6,5 %.

Здесь самым важным и даже настораживающим является то, что около 20 % респондентов затрудняются назвать хотя бы один метод информационной защиты, а ещё около 10 % выдают не самые конструктивные варианты, не имеющие отношения к реальной защите. Это говорит о том, что значительная часть взрослого населения в крупнейших городах нашей страны плохо проинформирована и особо уязвима для действий мошенников.

Из хорошего можно отметить, что около 10 % респондентов показали глубокие познания в мерах безопасности, указывая более технически сложные способы защиты.

На вопрос, какие меры защиты клиентов, о которых вы знаете, используются вашим банком, были получены следующие ответы:

- ◆ Не знают, затруднились ответить — 35,5 %;
- ◆ Двухфакторная аутентификация — 23,3 %;
- ◆ СМС-код — 14 %;
- ◆ Пароли — 12,1 %;
- ◆ Контрольный вопрос/слово — 6,5 %;
- ◆ Ограничения размеров операций — 4,6 %;
- ◆ Страховка — 4,6 %;
- ◆ Биометрия — 3,7 %.

В отличие от предыдущих опросов здесь увеличилась доля людей, которые либо не знают об используемых методах, либо затрудняются их назвать. Количество упомянутых способов защиты также резко снизилось.

ОЦЕНКА КАЧЕСТВА ИНФОРМИРОВАНИЯ БАНКАМИ О МОШЕННИКАХ

Среди респондентов в службу безопасности банка обращались только 24,3 %. Среди основных причин обращения: разблокировка карты, финансовые хищения, блокировка фишинговых сайтов, подозрение на взлом личного кабинета, разблокировка денежного перевода,

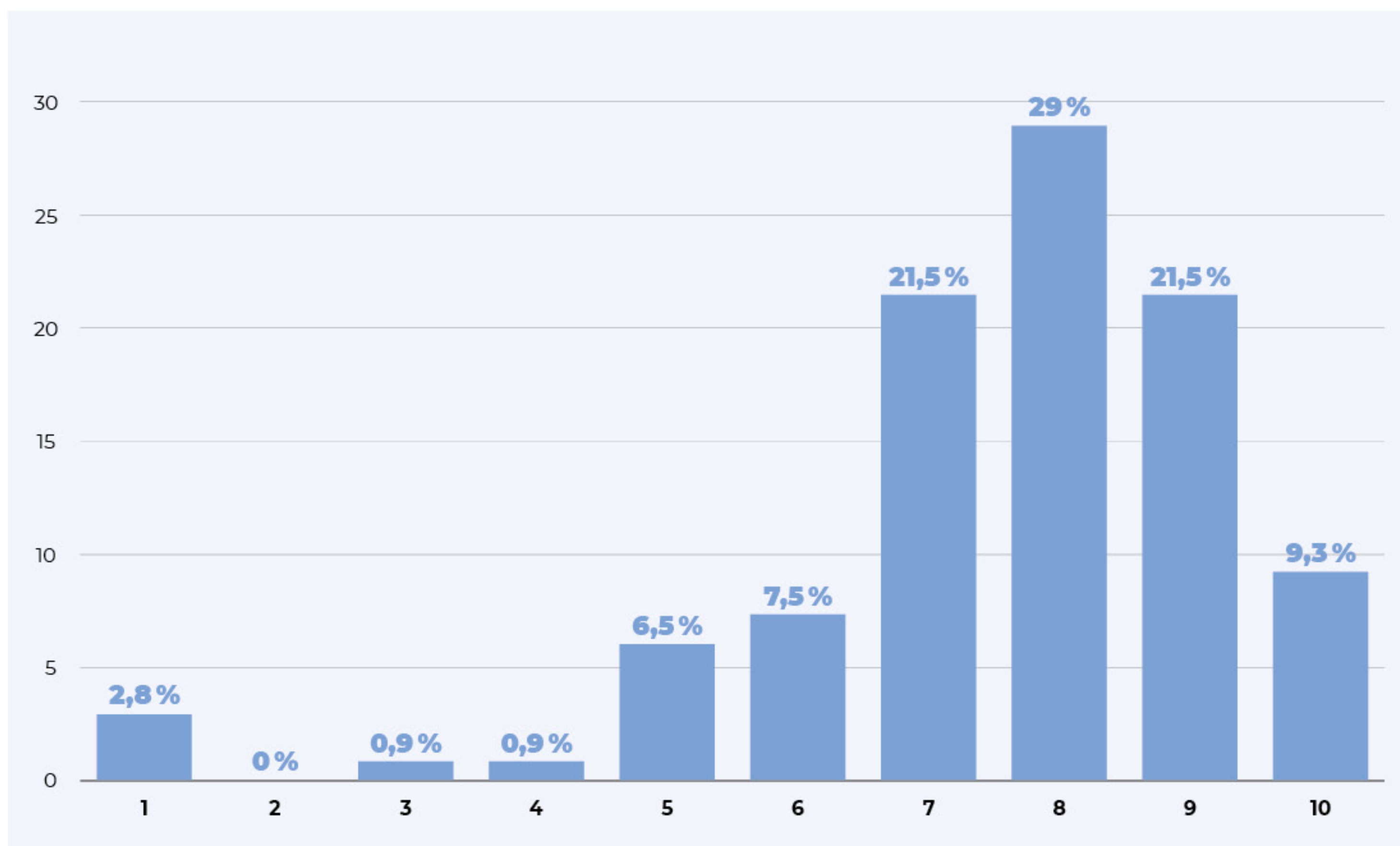


Рисунок 2. Оценка защищённости обслуживаемого банка

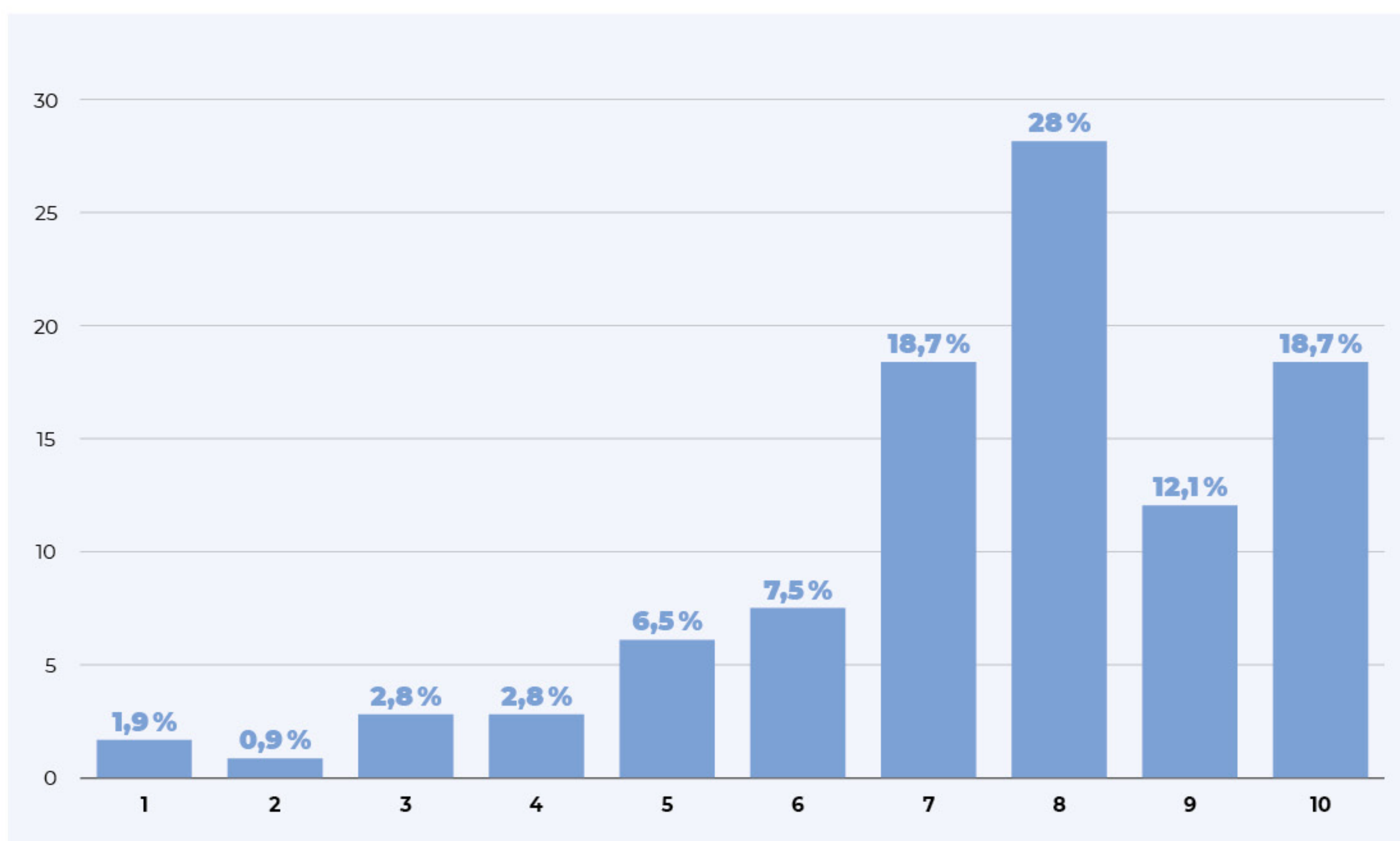


Рисунок 3. Оценка работы службы безопасности обслуживаемого банка

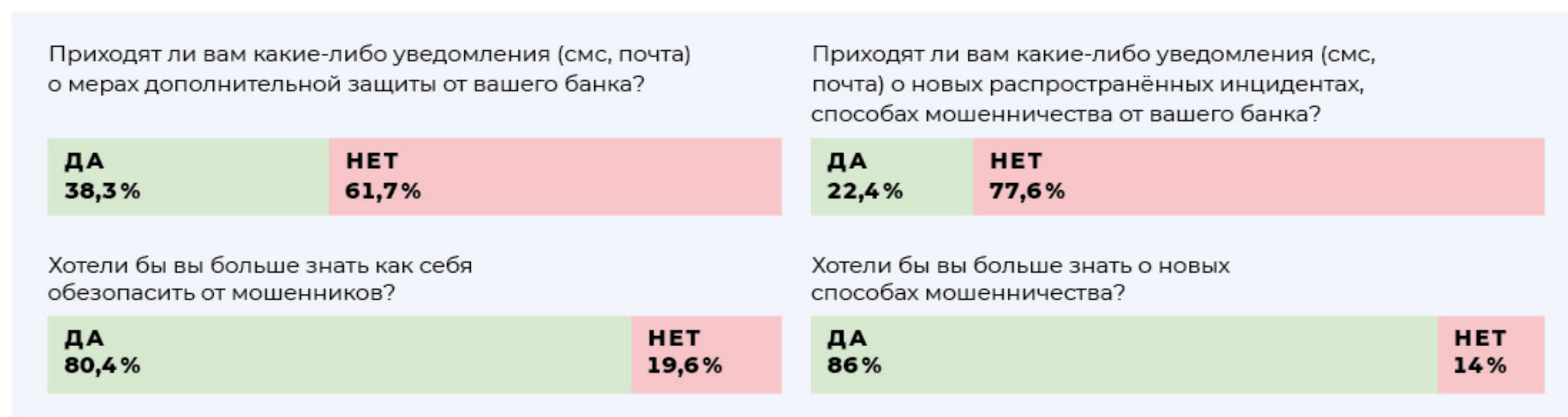


Рисунок 4. Получают ли клиенты от банков информацию о мерах дополнительной защиты и новых видах мошенничества, а также хотели бы они получать такую информацию

сообщение о попытках мошенничества (менее 5 %).

По десятибалльной шкале респонденты оценили защищённость своего банка следующим образом — рис. 2.

Распределение оценок работы службы безопасности обслуживающего банка оказалось приблизительно аналогичным — рис. 3.

Средняя оценка защищённости банка и работы службы безопасности составляет 7,5 из 10 баллов. При этом те, кто обращался в службу безопасности, оценивают её чуть ниже — на 7 баллов.

Далее мы решили выяснить, получают ли клиенты от банков информацию о мерах дополнительной защиты и новых видах мошенничества, а также хотели бы они получать такую информацию — рис. 4.

Получается, что большая часть клиентов по неустановленным причинам оказывается вне сферы информирования банков, хотя потребность в получении таких оповещений ярко выражена.

Возможными причинами сложившейся ситуации можно назвать неэффективную форму подачи информации и каналы её распространения. И если первая причина требует дополнительного качественного анализа информационных материалов, то проблему с каналами распространения мы смогли зафиксировать путём ещё одного опроса. Наш вопрос звучал так: «Какими банковскими ресурсами вы пользуетесь чаще всего: ходите в отделения, ищите дополнительную информацию на официальном сайте или в мобильном приложении?» Полученные ответы представлены на рис. 5.

Исходя из представленных данных очевидно, что самым посещаемым ресурсом банков являются их мобильные приложения, которые и должны быть главным каналом информирования клиентов об угрозах ИБ и противодействии мошенникам.

Частота	Физическое отделение	Сайт	Мобильное приложение
Никогда	14 %	25,2 %	3,7 %
Раз в год	34,6 %	15 %	0,9 %
Несколько раз в год	37,4 %	27,1 %	3,7 %
Раз в месяц	8,4 %	14 %	6,5 %
Несколько раз в месяц	2,8 %	10,3 %	12,1 %
Раз в неделю или больше	1,9 %	5,6 %	29 %
Раз в день или больше	0,9 %	2,8 %	43,9 %

Рисунок 5. Ответы на вопрос: «Какими банковскими ресурсами вы пользуетесь чаще всего: ходите в отделения, ищите дополнительную информацию на официальном сайте или в мобильном приложении?»

ЗАКЛЮЧЕНИЕ

Оповещение клиентов об угрозах информационной безопасности является значимым фактором повышения качества обслуживания, способствует росту удовлетворённости и повышает их лояльность. Кроме того, своевременно отправленные уведомления о способах противодействия мошенникам уменьшают число инцидентов, способствуют росту доверия и снижают финансовые и репутационные риски.

Чтобы средства, направляемые на проведение информирования, не оказались потрачены впустую, следует выбирать каналы распространения оповещений в соответствии с распределением векторов внимания целевой клиентской аудитории.

В сочетании с другими мерами повышения информационной безопасности это позволит качественно снизить количество мошеннических инцидентов, связанных с хищением денег со счетов физических лиц.

«С КЕМ МЫ ИМЕЕМ ДЕЛО?»

ФОРМИРОВАНИЕ ГРУПП РИСКА СОТРУДНИКОВ КАК ИНСТРУМЕНТ ДЛЯ ИБ-СПЕЦИАЛИСТОВ



**Ольга
ЛИМОНОВА**
психолог
ООО «Антифишинг»



**Андрей
ЖАРКЕВИЧ**
редактор
ООО «Антифишинг»

Разделение по группам риска — понятный способ категоризации сотрудников компании в интересах ИБ, однако на практике его мало кто использует, поскольку для этого требуется ответить на множество вопросов:

- ◆ по каким критериям формировать группы,
- ◆ как определять значимость того или иного фактора,
- ◆ где брать необходимую информацию о сотрудниках,
- ◆ как накапливать сведения и в каком виде их хранить.

В результате руководители понимают, в чём состоит ценность для бизнес-процессов разных должностей и подразделений, ИБ-специалисты уверенно ранжируют опасность уязвимостей в системах, но остаётся невосребованным огромный пласт важнейшей социально-психологической информации, которую не только можно, но и нужно использовать в интересах ИБ. Чтобы восполнить этот пробел, поговорим о том, как работа с группами риска помогает повысить информационную безопасность компании.

ГРУППЫ РИСКА И ИХ ФУНКЦИИ

Термин «группа риска» чаще всего используют в медицине и социологии для выявления людей, наиболее уязвимых к определённым обстоятельствам или воздействиям окружающей среды. К примеру, в социологии к группам риска относят многодетные, неполные семьи и семьи, имеющие детей-инвалидов, в медицине — группы риска развития диабета, сердечно-сосудистых заболеваний, в криминалистике в группе риска находятся бездомные, нарко- и алкозависимые, а также лица, имеющие раннее и повторное антиобщественное поведение.

ISO 27005 определяет в качестве информационного риска «возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации». И хотя стандарт не выделяет группы риска для категоризации человеческого фактора в качестве критерия уязвимости компании, с большой долей вероятности их официальное появление лишь вопрос времени. Опытные безопасники уже используют этот инструмент в повседневной работе, понимая, что

информационная безопасность требует учитывать наравне с техническим фактором человеческий.

В качестве инструмента работы с человеческим фактором группы риска могут выполнять следующие функции:

- ◆ *систематизирующую* — сбор и упорядочивание потенциальных уязвимостей;
- ◆ *аналитическую* — выявление актуальных для компании уязвимостей;
- ◆ *прогностическую* — предсказание последствий найденных уязвимостей, а также перспектив проведения предупредительной работы;
- ◆ *защитную* — выбор мер по устранению уязвимостей, например, дополнительного информирования групп риска или более частого обучения и тренировки, сопоставление установленной категории риска с разработанным перечнем профилактических мероприятий и выдача рекомендаций по предупреждению небезопасного поведения у конкретных работников.
- ◆ *инновационную* — подбор методов устранения уязвимостей компании через работу с выявленными группами риска.

ОСОБЕННОСТИ ФОРМИРОВАНИЯ

Формирование групп риска в компании состоит из четырёх этапов.

1. *Выбор актуальных факторов для категоризации* — наиболее релевантных компании качеств сотрудников, позволяющих определить их уязвимость и принадлежность к той или иной группе риска.

2. *Определение компонентов данных факторов*, которые потенциально можно собрать в имеющихся условиях. Здесь важно максимально точно понять, какие сведения о сотрудниках необходимы и как их можно получить.

3. *Задание веса выбранным компонентам факторов*. Чтобы понять, какой из факторов важнее, ему присваивается некая условная значимость, которую затем проверяют на практике.

4. *Распределение факторов по группам риска*. Когда вес компонентов факторов определён, производится их категоризация по группам риска: какой фактор из-за низкого веса следует отнести к низкому риску, какой к среднему и какой к высокому.

Схематично данный процесс можно изобразить следующим образом — рис. 1.

ФАКТОРЫ И КОМПОНЕНТЫ

Основными факторами формирования групп риска являются:

- ◆ поведение;
- ◆ демографические характеристики;
- ◆ психологические особенности;
- ◆ специализированные критерии, определяемые особенностями компании и бизнес-задачами.

Компонентами *поведенческого фактора* могут быть зафиксированные небезопасные действия сотрудников, неоднократное нарушение установленных правил ИБ, инциденты ИБ, результаты обучения и имитированных атак, а также отсутствие взаимодействия сотрудника с отделом ИБ. Например, необычным выглядит поведение человека, который работает в компании больше года, но ни разу не пересылал на проверку подозрительные письма, особенно если его коллеги делают это регулярно.

Определение значимых компонентов поведенческого фактора сильно зависит от внутриорганизационных особенностей, политики ИБ и корпоративной культуры. Если в компании нет регулярного обучения основам ИБ и нет налаженного канала взаимодействия с отделом безопасности, данные факторы бессмысленно учитывать в системе групп риска, поскольку они будут присутствовать у всех.

К *демографическому фактору* относятся: пол, возраст, место жительства и социально-экономическая принадлежность, опыт работы с ПК, интернетом и почтой. Исследовательские данные подтверждают, что к более высокой группе риска можно относить женщин (по половому признаку), людей в возрасте до 25 и старше 50 лет (по возрастному признаку), жителей дальних регионов (по территориальному признаку), с низкой заработной платой (по социально-экономическому признаку), с низким и непрофильным по должности опытом работы с ПК, интернетом и почтой (по признаку опыта).

Психологический фактор включает личностные черты, психологические расстройства, актуальные потребности, ведущий тип мотивации и эмоциональные состояния (если в компании есть средства мониторинга и лингвистического анализа исходящих писем) сотрудников.

Самые опасные из личностных черт: эмоциональная неустойчивость (нейротизм), доброжелательность, импульсивность, открытость опыту, невнимательность, общительность, подчинённость, доверчивость, безответственность, любопытство.

Наиболее опасные расстройства личности — нарциссическое и антисоциальное.



Рисунок 1. Четыре этапа при формировании групп риска в компании

К *специализированным факторам* относятся:

- ◆ должность / отдел / филиал;
- ◆ статус (новый или увольняющийся сотрудник);
- ◆ бизнес-значение, значение сотрудника с точки зрения результатов деятельности компании или определяемая руководством важность;
- ◆ известные технические уязвимости на рабочем месте сотрудника, которые невозможно устранить.

ГРУППА РИСКА ИНСАЙДЕРСКОЙ УГРОЗЫ

В рамках работы по формированию групп риска можно выделить группы для инсайдерской угрозы либо совместить их в рамках общей категоризации сотрудников по уязвимости.

В отчёте INSA¹ перечислены виды негативного инсайдерского поведения и психологических состояний, по которым можно выявить угрозу. Они систематизированы относительно актуальных стрессоров.

1. *Эмоциональных*, которые связывают внешние стрессоры с проявляющимися негативными эмоциями и агрессивным поведением.

2. *Организационных*, которые фиксируют неадекватное поведение сотрудников по отношению к организации и её процессам.

3. *Ситуационных* триггеров, которые могут усугублять поведение, увеличивая индивидуальный стресс.

Используя диагностическую методологию, аналогичную DSM-5, авторы отчёта предлагают соотнести эти специфические формы поведения на индивидуальном и групповом уровне с уровнем угрозы и типом нарушения, исходя из предположения, что большое количество случаев такого поведения может указывать на рост вероятности более серьёзных злонамеренных действий, особенно если стрессовые события накапливаются.

¹ Assessing the mind of the malicious insider: using a behavioral model and data analytics to improve continuous evaluation, INSA, 2017.

Стрессор	Эмоция			
Уровень проявления	Индивидуальный	Индивидуальный	Индивидуальный	Индивидуальный
Уровень угрозы	Незначительный	Серьёзный	Незначительный	Серьёзный
Тип нарушения	Негрубое	Негрубое	Грубое	Грубое
Компоненты факторов	Опоздания Низкая производительность Некачественная работа Злоупотребление рабочим временем Нецелевое использование ресурсов компании Непринятие обратной связи Постоянное недовольство Несогласованная история работы Несообщаемые изменения в личной истории/жизни	Фальсификация данных о занятости Чрезмерные прогулы Кража информации/ имущества компании Мошенничество с фиксацией отработанного времени Фальсификация данных, связанных с работой Проявление параноидальных установок Пренебрежение авторитетом Чрезмерная секретность Недоверие к другим людям	Небезопасное поведение (принятие рисков) Употребление алкоголя / наркотиков Издавательство над коллегами Словесные оскорбления / ненормативная лексика Невыраженный гнев Агрессия по отношению к другим людям Демонизация	Открытая агрессия/гнев Уничтожение имущества Нападение Кража Растущая паранойя Действия, опасные для себя и других Пренебрежение авторитетом Аресты

Стрессор	Организационный вопрос			
Уровень проявления	Индивидуальный	Индивидуальный	Группа	Группа
Уровень угрозы	Незначительный	Серьёзный	Незначительный	Серьёзный
Тип нарушения	Негрубое	Негрубое	Грубое	Грубое
Компоненты факторов	Опоздания Некачественная работа Злоупотребление рабочим временем Нецелевое использование ресурсов компании Недоверие вне группы Сдвиг лояльности от корпорации к группе Секретность внутри группы	Невыход на работу / частые больничные Сомнительная групповая активность Прогресс работы замедлен Организованное воровство Фальсификация данных Недоверие к посторонним людям Демонизация негрупповых членов / организаций	Частые больничные Издаательства вне группы Несанкционированные митинги Нецелевое использование ресурсов Недоверие вне группы Сдвиг лояльности от корпорации к группе Злоупотребление рабочим временем	Фальсификация данных Необычные схемы работы Массовые беспорядки Нападения Саботаж Организованное воровство Открытая агрессия к «чужакам»

Стрессор	Ситуационные триггеры			
Уровень проявления	Окружающая среда	Окружающая среда	Корпоративный	Корпоративный
Уровень угрозы	Незначительный	Серьёзный	Незначительный	Серьёзный
Тип нарушения	Требует наблюдения	Требует наблюдения	Требует наблюдения	Требует наблюдения
Компоненты факторов	Проблемы со здоровьем (своим или члена семьи) Депрессия Наличие издевательств на работе Столкновение с несправедливостью (по отношению к себе или окружающим) Финансовые потери Снижение удовлетворённости работой Самоубийство в семье	Потеря контроля (реального или мнимого) Плохие рабочие отношения Супружеские / семейные трудности Плохая оценка работы Отказано в продвижении по службе Ожидание расторжения трудового договора	Расхождение практики и принятой в компании политики Несогласованность рабочих процессов Отсутствие профессиональной подготовки Недоверие к сотрудникам Изменения в системе вознаграждения Игнорирование правил безопасности Непоследовательный процесс вознаграждения сотрудников Смена авторитета в коллективе	Изменение полномочий сотрудников Сокращение персонала Увольнение Отсутствие коммуникаций Потеря выгоды Отношение к сотрудникам (лояльность) Нарушение этики

Рисунок 2. Виды негативного инсайдерского поведения и психологические состояния, по которым можно выявить угрозу, систематизированные относительно актуальных стрессоров

Модель отлично отражает возможность использования подобных данных в формировании инсайдерских групп риска с целью помощи в разработке стратегий исправления ситуации на местах (рис. 2).

ЗНАЧИМОСТЬ ФАКТОРОВ РИСКА

Значимость факторов для формирования групп риска назначается через оценку путём распределения веса среди компонентов факторов вручную в зависимости от особенностей компании, существующих актуальных процессов и бизнес-приоритетов.

В качестве системы оценки для определения значимости компонентов факторов обычно используют десятичную (0–10), дробно-десятичную (0–1,0) или бинарную (0–1).

Бинарная оценка наиболее простая, так как вес распределяется равномерно в рамках двух категорий: значим фактор или нет. Минус такой оценки в том, что невозможно отдать предпочтение какому-либо фактору, то есть выделить более или менее важные факторы. Поэтому в более сложных моделях лучше использовать оценку, которая позволит точнее распределить приоритеты внутри факторов.

Критериями эффективности распределения веса между факторами в сформированных группах риска являются:

♦ Ограниченное количество выбранных отслеживаемых факторов — от 5 до 10. Если факторов слишком много, на выходе получится ни о чём не говорящий усреднённый результат. Недостаточное количество не покажет реальную угрозу, которую создают психологические особенности людей.

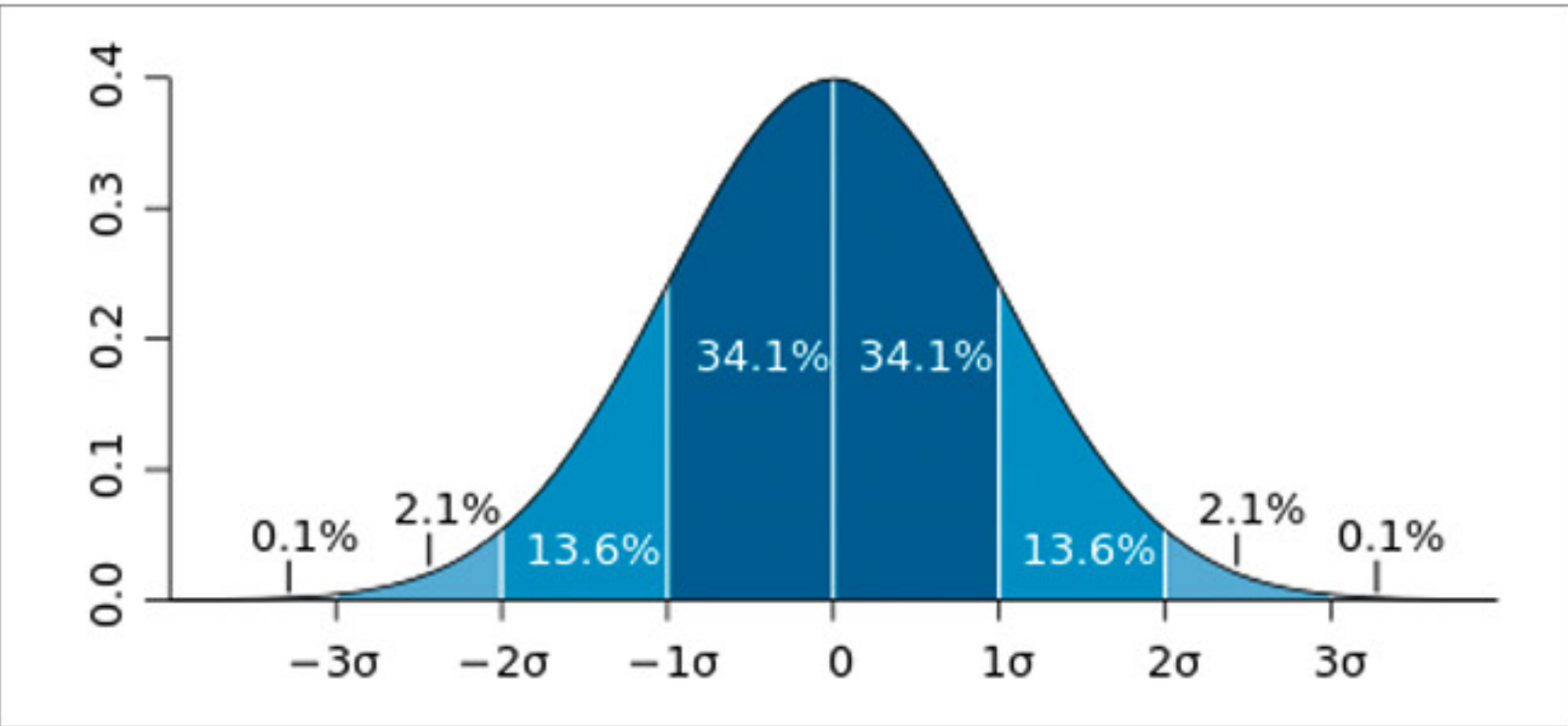


Рисунок 3. Нормальное распределение по группам риска соответствует теории вероятности: в самой массовой средней группе оказывается большинство, а в немногочисленных крайних — убеждённые нарушители и устойчивые к угрозам сотрудники

♦ Нормальное распределение по группам риска соответствует теории вероятности: в самой массовой средней группе оказывается большинство, а в немногочисленных крайних — убеждённые нарушители и устойчивые к угрозам сотрудники (рис. 3).

РАСПРЕДЕЛЕНИЕ ФАКТОРОВ И СОТРУДНИКОВ

Распределение факторов по группам риска будет зависеть от выбранной системы классификации. Наиболее простым и понятным является деление на низкий, средний и высокий риск. Категоризация только на низкий и высокий уровень риска, как правило, оказывается неэффективной.

Пример распределения поведенческих факторов по группам риска — на рис. 4.

Группа риска	Условия попадания или перехода в группу риска
Высокая	• систематически нарушает правила ИБ; • успешно реализованы две и более имитированные атаки, либо атаки не проводились; • по результатам проведения интегрального тестирования показал низкий уровень знаний (пробелы в знаниях более чем по одной теме) и/или не проходил интегральное тестирование; • изучено менее 50% курсов повышения осведомлённости;
Средняя	• нарушения правил ИБ происходят редко и нерегулярно; • в ходе имитированной атаки совершает не более одного небезопасного действия при условии использования шаблонов сложности «нормально»; • по результатам проведения интегрального тестирования показал средний уровень знаний (пробелы в знаниях не более чем по 1-й теме); • пройдена большая часть курсов повышения осведомлённости;
Низкая	• нарушения правил ИБ носят нерегулярный характер и имеют очень низкую частоту; • в ходе цифровой атаки совершает не более одного небезопасного действия при условии использования шаблонов сложности «сложно»; • по результатам проведения интегрального тестирования показал средний уровень знаний: пробелы в знаниях присутствуют не более чем в одной теме; • пройдены все / почти все курсы повышения осведомлённости (более 90% курсов).

Рисунок 4. Пример распределения поведенческих факторов по группам риска



Распределение сотрудников по группам риска желательно автоматизировать. Если сделать это по каким-то причинам невозможно, необходимо не реже, чем раз в три месяца, проводить ручной пересмотр групп риска, при необходимости добавляя или удаляя сотрудников.

При неполном соответствии работника группе с более низким риском его следует переместить в группу с более высоким риском.

СБОР И СИСТЕМАТИЗАЦИЯ ИНФОРМАЦИИ

Если вопросы с регистрацией поведенческого фактора помогают решить системы мониторинга и контроля защищённости, с психологическими параметрами ситуация сложнее.

Представляется оптимальным вариант получения психологической информации о сотрудниках через взаимодействие с HR-отделом, который может предоставлять данные тестирования, проведённого в процессе собеседования претендентов на вакансию. В качестве возможных затруднений по этому сценарию отметим следующие:

1. Психологическое тестирование может вообще не проводиться в компании, а значит, эта процедура потребует внедрения в деловую практику.

2. Как правило, результаты психологического тестирования не систематизируются и не сохраняются, а значит, придётся убедить HR-отдел потратить дополнительные усилия на процесс, который не обладает для него ценностью.

3. Необходимо будет решить вопрос конфиденциальности собираемых данных и получить письменное согласие кандидата на использование результатов тестирования отделом ИБ.

Альтернативный способ работы с психологическим фактором — использование психопрофилей должности. При отсутствии индивидуальных данных о сотрудниках это позволяет разрабатывать групповые характеристики, в соответствии с которыми отбираются кандидаты. Именно такой подход порождает стереотипы о типичных бухгалтерях и айтишниках.

Групповые психологические профили можно позаимствовать у HR-отдела, если он ими располагает, либо воспользоваться открытыми источниками. Уровень риска при этом будет формироваться в соответствии с должностью. Главный минус такого подхода — высокая вероятность ошибки, в результате которой сотрудник распределяется не в ту группу риска.

Для хранения собранных сведений целесообразно использовать электронную базу данных, которая:

- ◆ содержит информацию о степени риска по каждому работнику и каждому фактору, который может стать причиной небезопасного поведения;
- ◆ позволяет формировать группы в зависимости от степени риска и действующего фактора для проведения групповых и индивидуальных мероприятий по профилактике небезопасного поведения;
- ◆ может регулярно дополняться новыми сведениями о работниках, условиях труда и результатами обучения по ИБ.

ЗАКЛЮЧЕНИЕ

Быстро меняющийся ландшафт угроз информационной безопасности компании требует от ИБ-сотрудников учитывать при построении моделей угроз не только технические, но и психологические факторы. И если для технического анализа риска уже имеется богатый набор методик и программных инструментов, психологическая составляющая этим похвастаться не может.

В этих условиях группы риска могут стать важной частью арсенала эффективного ИБ-специалиста и вывести результативность защиты безопасности компании на принципиально новый уровень.

«ВЫБРОСЬ ЭТО СТАРЬЁ!»

Анна
КАТАНКИНА
корреспондент
BIS Journal

ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА НИЗШЕЙ СТУПЕНИ ГОССТРУКТУР

В профессиональной среде много говорят о программно-аппаратных средствах защиты, утечках, мониторинге и прочих финансово затратных мероприятиях по предотвращению несанкционированного доступа к информации предприятий и персональным данным граждан.

А как обстоят дела в обыденной реальности? Не будем далеко ходить, остановимся на уровне московского района. Своими впечатлениями с нашим корреспондентом Анной Катанкиной поделился мелкий московский чиновник, по понятным причинам попросивший сохранить его имя в тайне.

— По образованию я инженер-программист, работал системным администратором, знаком с методами защиты информации. Некоторое время назад устроился в одну из государственных структур Москвы на рядовую должность.

Сеть нашей организации — десять рабочих мест, включая два места руководителей и два — бухгалтерии. Весь документооборот идёт по открытым каналам данных, в какой-то момент мы попытались подключиться к системе московского электронного документооборота (ЭДО), но сначала упёрлись в технические и финансовые проблемы, а потом случился переезд...

Вот при переезде и выяснилось, как в реальности обстоят дела с информационной безопасностью на низшей ступени наших госструктур.

Переезжали мы перед карантинном, одновременно с дружественной государственной организацией, своими силами. Понятно, что все вещи складывали сами: упаковали содержимое своих столов и шкафов в коробки, промаркировали компьютеры и оргтехнику...

Перед тем как покинуть здание, мы прошлись по пустым и открытым помещениям нашей и соседней организаций. Следом за нами уже шли рабочие, начинавшие ремонт, а также неизвестные граждане, явно желающие поживиться тем, что плохо лежит, — здание никто не охранял. В одном из кабинетов мы набрали на залежи брошенных вещей. Среди всякого хлама валялись и старые жёсткие диски, и огромное количество флешек. Я их собрал в большую коробку, отнёс к себе на новое место и благополучно

забыл — переезд был сложным и многодневным, новое помещение требовало ремонта...

Вспомнил я о своей находке через несколько месяцев, когда начал разбирать вещи, обустраниваясь на новом месте. Оказалось, жёсткие диски были сняты с рабочих компьютеров и помимо операционной системы и офисных программ содержали много служебной документации. Устаревшей на данный момент, но при необходимости в чьих-то руках она может найти достойное применение.

Ещё более интересную информацию хранили usb-накопители. Опять же, все сведения на них были старыми, но актуальности они явно не потеряли. Фактически государственная организация выбросила при переезде сотни записей, содержащих персональную информацию о гражданах, их адреса, телефоны и даже политические взгляды — видимо, сведения учитывались в ходе выборов разных уровней.

Служебная информация файлов указывала на одного из руководителей соседней организации как на автора документов. Коллегу-сисадмина,

Фактически государственная организация выбросила при переезде сотни записей, содержащих персональную информацию о гражданах, их адреса, телефоны и даже политические взгляды

к которому я обратился, угроза утечки этой информации не взволновала. Он просто махнул рукой: «Выбрось это старье...»

Подчеркну, что компьютерная сеть у дружественной организации находится в ведении Департамента информационных технологий города, защищена всеми возможными способами и доступ к сторонним информационным ресурсам и сайтам в учреждении сильно ограничен, а вся система документооборота бюрократизирована с помощью ЭДО. Спрашивается: ну зачем такая секретность при такой безалаберности?

Если вернуться к состоянию сети уже в моей организации, то вход в неё «открыт» для всех умеющих. Разговоры о необходимости установки межсетевого экрана мы ведём несколько месяцев. Сначала были отговорки типа «у нас нечего красть, а бухгалтерия работает с ключами», потом пошли разговоры, что закупим всё разом, в порядке обновления техники. Но тут случился карантин и удалённая работа...

Как я понимаю, тратить несколько десятков тысяч рублей на самую примитивную систему ИБ моё руководство так и не планирует. Экономит оно и на антивирусной защите — это лишние расходы. Впрочем, мой непосредственный начальник уже пострадал от собственной жадности — его жёсткий диск с программами доступа к торговым площадкам оказался забит вирусами и троянами. Восстановить винчестер удалось лишь частично... Но это его ничему не научило.

Отдельно упомяну о любителях доступа к открытым сетям Wi-Fi. В задачи нашей организации входит регулярное проведение собраний с участием ответственных за разные направления чиновников. Вспомогательный материал мы заливаем на планшеты до заседаний. Большинство коллег относится к этому спокойно, при необходимости доступа в интернет им хватает своих мобильных устройств. Но есть группа лиц, требующих доступа в глобальную сеть через Wi-Fi, в том числе и с планшетов. При этом им абсолютно всё равно, чья это сеть и как она организована, есть ли у неё пароль или подключиться может кто угодно. Регулярно звучат претензии (ко мне, в частности), что мы запрещаем доступ в интернет с планшетов с материалами ДСП, когда «всем так хочется». Попытки провести краткий ликбез по информационной безопасности натываются на стену непонимания — «всё вы врётё, нет никакой угрозы утечки». Самое печальное, что эти люди наделены правом принятия решений и желают двигаться дальше по карьерной лестнице, в том числе на федеральный уровень, мечтают принимать законы...

* * *

Несмотря на все наши просьбы по минимальной ИБ-защите организации, руководство не считает нужным тратить на то ПО и оборудование, без которого и так всё работает. До первого серьёзного инцидента.

КОРОТКО ПО ТЕМЕ

♦ За 2019 год в мире утекли 13,7 млрд записей персональных данных, сообщают исследователи проекта Kaspersky ICS CERT. Там же говорится и о целевых атаках киберпреступников на промышленные организации в Японии и странах Европы.

♦ Совет Федерации РФ одобрил закон о создании единого федерального регистра, содержащего информацию о населении страны. В нём будут отслеживаться все важные этапы жизни граждан: от рождения до смерти. Оператором регистра будет Федеральная налоговая служба. Эта информационная база должна заработать в России с 1 января 2023 года.

♦ Максимальные штрафы за утечку персональных данных в новой редакции Кодекса об административных правонарушениях (КоАП) планируется увеличить с 50 тыс. до 500 тыс. руб. для юридических лиц, сообщил «Коммерсант», в начале июля 2020 г. Для индивидуальных предпринимателей штрафы вырастут с 20 тыс. до 300 тыс. руб., для должностных лиц — с 10 тыс. до 100 тыс. руб., остальных граждан — с 2 тыс. до 20 тыс. руб.

♦ Поправки об увеличении штрафов разрабатывает и комитет Госдумы по информационной политике, информационным технологиям и связи.

♦ По данным InfoWatch, в 2019 г. количество утечек персональных данных в России выросло на 40 % по сравнению с предыдущим годом. В 2020 г. ситуация ухудшится на фоне самоизоляции из-за коронавируса: в результате массового перехода на удалённую работу число попыток неправомерного доступа к данным увеличилось примерно наполовину, причём около 30 % инцидентов составляют явно противоправные попытки скопировать клиентские базы данных и передать их вовне, в том числе через мессенджеры, а 10 % инцидентов приходится на действия хакеров.



Денис БАТРАНКОВ
эксперт BIS Journal,
консультант по информационной
безопасности Palo Alto Networks

СОГЛАСНО ЗАКОНОДАТЕЛЬСТВУ РФ...

Существуют мировые практики по анализу рисков, которым следуют единицы компаний. С точки зрения методологии рекомендуется провести Business Impact Analysis, где оценивается влияние различных рисков на бизнес-процессы компании и на этой основе строится дальнейшая защита. В большинстве же компаний руководство оценивает риск обывательски: смотрят, как сделано у других, реализуют какую-то одну методику защиты и успокаиваются или вообще принимают вероятность риска только на основе своего жизненного опыта, а не на основе мнения профессионалов. И соответственно, подготовка к угрозам обычно отсутствует, пока эти угрозы не осуществляются: произойдёт утечка, пройдёт DDoS-атака, выйдет из строя какая-то важная бизнес-система.

Существует такой метод реагирования, как принятие риска, что означает, что ты согласен, что риск есть, но тебе проще его проигнорировать, чем разбираться и защищаться от него. Если утечка не приносит никакого вреда самой компании, то компания её игнорирует. Но в государственных компаниях утечка может нанести существенный вред гражданам. Поэтому надзорные органы должны вводить требования по защите, а мотивацией становятся штрафы и выговоры.

Я однажды познакомился на свадьбе с владельцем фармацевтической компании, естественно, речь пошла про безопасность. И он мне сказал, что у него в офисе за все ИТ отвечает студент. Когда у него студент становится профессионалом, то увольняется и появляется новый студент. Так вот на вопрос с утечками мне ответили, что ему ничего не жалко: список дистрибьюторов, список лекарств? Всё это доступно и так. Криптолокеры? Переустанавливает

Windows и продолжает работать. И он прав в своих размышлениях — ему не приносит боли никакая атака. Он легко перезапустит бизнес, даже если все ИТ-ресурсы умрут. Про угрозы на производстве и дистанционное банковское обслуживание мы не говорили.

В итоге если безопасник рассказывает про немыслимые ранее ущербы, то он должен оценивать ущерб в первую очередь для каждого бизнес-процесса на основе параметра MTD — Maximum Tolerable Downtime. То есть время простоя бизнес-процесса, после которого процесс уже не восстановить. Сколько организация проживёт без электронной почты? Сколько бизнес проживёт без электронной системы учёта товаров? Задавая подобные вопросы руководству, понимаешь, что часть рисков можно принять, поскольку часть сервисов проще переустановить с нуля, чем ставить сложную систему защиты, которая удержит систему в стабильном состоянии.

* * *

В случае с государственными органами контроль за утечками возлагается на каждого служащего, согласно законодательству РФ. И такие формы утечек, как забытые флешки и жёсткие диски, на самом деле оговорены регулируемыми органами и приводят к персональной ответственности. Такие риски нельзя «принять». Да, нерадивые сотрудники встречаются в каждой компании. Поэтому рекомендуется выполнять шифрование внешних и внутренних носителей, и это ответственность ИТ- и ИБ-службы. И если в какой-то организации найдены незашифрованные флешки и жёсткие диски, то вопросы нужно адресовать к ответственному за защиту персональных данных и руководителю организации.



Марина БРОДСКАЯ
обозреватель BIS Journal



ТРИГГЕР СРАБОТАЛ

COVID-19 ДАЛ СТАРТ ПЕРЕХОДУ В ОНЛАЙН И ОСВОЕНИЮ ПРОФЕССИЙ В СФЕРЕ ИБ

Благодаря эпидемии коронавируса в мире произошёл массовый переход школьников и студентов на онлайн-обучение. Подавляющее большинство учащихся и учителей были вынуждены остаться дома и подстраивать свою жизнь под новые для многих технологические решения учебного процесса. Вместе с массовым переходом в онлайн в сетях оживились хакеры, и соответственно вырос спрос на специалистов в области информационной безопасности.

Если первое время учителя выбирали удобную для работы онлайн-платформу, то спустя короткое время обеспокоились вопросами безопасности. Например, у ставшего популярным

благодаря своим возможностям американского сервиса видеоконференций Zoom были найдены многочисленные уязвимости. Уроки нередко прерывались хакерами, а сам сервис непреднамеренно похищал пароли пользователей платформы из учётной записи Windows. Технические проблемы Zoom, подорожавший благодаря COVID-19 за год вдвое, безусловно, решит. Но проблем в онлайн-образовании оказалось больше, чем можно было представить.

Как показала практика мирового карантина, необходимо срочное внедрение современных IT-технологий в образование, которое осталось в стороне от технического прогресса — традиционное обучение в классах считается

лучшей формой передачи информации. Но в период эпидемии такой формат становится опасным для всех участников процесса. Одна из выявленных проблем — отсутствие поддержки преподавателей в обучении новым технологиям и необходимость финансирования программ для переобучения учителей.

ВЕЛИКОБРИТАНИЯ

Столкнувшись с проблемой онлайн-обучения, правительство Великобритании планирует выделить 10 млн фунтов на поддержку Стратегии развития образовательных технологий (Education Technology Strategy) — плана, появившегося в начале апреля для поддержки и улучшения цифрового обучения. Конечная цель стратегии —

стимулировать изменения в образовании с помощью технологических инноваций. Например, предлагается исключить из обязанностей педагогов решение трудоёмких административных задач, но разрешить учителям проводить индивидуальные курсы при обучении онлайн.

«Преподаватели и студенты могут легко общаться с помощью существующих приложений, таких как Zoom, Facetime или Skype. Виртуальная реальность может изменить то, как преподаются предметы, а специальное программное обеспечение должно поддержать процесс обучения и оценку знаний студентов», — считают авторы ресурса FEnews — The Future in Education News Channel.

Онлайн-платформы позволяют совместно использовать и по мере необходимости обновлять ресурсы, а также предоставляют полезные инструменты типа преобразования речи в текст и обмена мгновенными сообщениями. Возможность подключиться к занятиям с разных гаджетов обеспечит большую доступность знаний для студентов.

Администрации школ смогут просматривать данные занятий, собранные с помощью программного обеспечения, чтобы лучше распределять финансовые ресурсы, выставлять оценки и собирать информацию, которая может быть записана автоматически для дальнейшего использования.

Однако Стратегия развития образовательных технологий не освобождает участников учебного процесса от проблем с кибербезопасностью. Ещё осенью 2019 г. 83 % британских школ столкнулись с проблемами в области ИБ. Самыми распространёнными типами угроз стали фишинговые атаки и заражение вредоносным ПО, 21 % атак пришлись на спуфинг.

Несмотря на это, большинство опрошенных школ заявили, что у них есть средства защиты в виде антивирусных программ и брандмауэров. Но политика BYOD (использование персональных устройств в рабочих целях) стала причиной многочисленных заражений корпоративных сетей школ и университетов. Учебные заведения не могут контролировать использование личных гаджетов студентов и сотрудников,

частоту обновления программного и антивирусного обеспечения на них.

Ещё одной потенциальной угрозой и точкой проникновения вирусов во внутреннюю сеть университетов и кампусов является эксплуатационная технология университетских городков, которая объединяет системы отопления, вентиляции и кондиционирования воздуха. Кажется, что эти системы далеки от интересов хакеров, однако теоретически их можно использовать для проникновения и атаки. А поскольку всё больше школ собирают, хранят информацию и обмениваются ею в интернете, вопросы безопасности персональных данных, финансовой информации требуют разработки новой стратегии защиты данных.

Что советуют использовать школам британские эксперты в области ИБ учебных заведений? Отслеживать типы и количество подключённых к сети устройств, ограничивать доступ к сети или её сегментам, использовать VPN. И повышать грамотность пользователей, в т.ч. в части кибербезопасности, защиты персональных компьютеров и гаджетов и в части распознавания фишинга и спуфинга. Онлайн-обучение и цифровые образовательные сообщества позволят учащимся, преподавателям и администраторам школ работать в любых условиях. Но все участники процесса должны помнить,

что кибербезопасность должна стать приоритетом — риск кибератак высок там, где есть онлайн-активности любого рода.

ИССЛЕДОВАНИЯ JISC

Впрочем, вопросами кибербезопасности заведений высшего и дополнительного (для лиц от 16 и старше) образования в Великобритании занимается Jisc (ранее the Joint Information Systems Committee, в настоящее время — Комиссия по цифровым технологиям и ресурсам в сфере высшего образования, дополнительного образования, навыкам и научным исследованиям). Эта некоммерческая организация поддерживает учреждения образования, предоставляет IT и сетевые услуги, цифровые ресурсы, разрабатывает новые информационные технологии и способы работы учебных заведений. Jisc финансируется благотворительными фондами, фондами университетов и отдельными высшими учебными заведениями.

С 2017 г. Комиссия проводит исследования состояния кибербезопасности в учреждениях высшего и дополнительного образования (ДО). Последний отчёт был подготовлен осенью 2019 г. Конечно, с тех пор прошёл почти год, за который мир претерпел некоторые изменения, однако само исследование наглядно показывает, как мало внимания





уделяют вопросам ИБ учебные заведения даже в такой продвинутой с точки зрения подхода к вопросам обучения кибербезопасности стране, как Великобритания.

При подготовке исследования Jisc поставил несколько задач, среди которых были понимание текущего кадрового обеспечения кибербезопасности организаций и понимание текущего положения организаций в области ИБ, изучение представлений организаций о текущих уровнях защиты, рисках и возможности улучшения ситуации, а также вопросы сертификации и обучения с учётом представления о будущих угрозах кибербезопасности.

В опросе 2019 г. приняли участие руководители и специалисты в области ИБ 122 учебных заведений, примерно столько же (118) организаций было опрошено годом ранее. Основные выводы, которые сделали специалисты Комиссии:

- ♦ кибербезопасность становится всё более актуальной задачей стратегического планирования;
- ♦ растёт доля организаций, имеющих в штате руководителей в области ИБ;
- ♦ всё больше заведений проходит сертификацию и подключается к центрам реагирования на киберугрозы;

♦ некоторые университеты создали группы реагирования на киберугрозы в режиме 24/7, однако то, как организации реагируют на инциденты кибербезопасности, свидетельствуют об отсутствии единого подхода и формальной процедуры реагирования.

По сравнению с более ранними исследованиями представления о киберзащите организаций оставались на довольно низком уровне и даже понизились. И это на фоне роста числа кибератак, их эволюционирующей природы и повышения сложности угроз, роста числа мошеннических действий и новых требований к защите персональных данных (GDPR). С другой стороны, отмечают авторы исследования, снижение оценки уровня киберзащиты учебных заведений может быть связано с приходом в них специалистов по ИБ, которые объективно оценивают уровень киберзащиты организаций. Таким образом, представители Jisc получили более реалистичную оценку ситуации.

Из исследований также следует, что с 2017 г. учебные заведения проводят работу по улучшению ситуации в области информационной безопасности, а для упреждения кибератак многие организации привлекают

специализированные компании для получения информации о настоящих и возникающих угрозах.

Среди основных угроз и приоритетов кибербезопасности ответившие на анкету отметили фишинг и социальную инженерию. Недостаточная осведомлённость, плохая профессиональная подготовка в области ИБ и часто человеческий фактор оставались серьёзными проблемами и рисками как в 2018, так и в 2019 г.

Для организаций высшего образования в пятёрку самых распространённых инцидентов также входят случаи утечки персональных данных, атаки с использованием вредоносных программ и управления исправлениями, а в учреждениях дополнительного образования лидирует вредоносное ПО и вирусы-вымогатели (они на третьем месте), далее следуют DDoS-атаки, вредоносные атаки изнутри системы. Утечки данных актуальны для всех перечисленных угроз.

И если 2/3 организаций высшего образования осознали опасность киберугроз и утвердили руководителя подразделения ИБ или выделили его обязанности в отдельную должность, то в учреждениях ДО дела обстоят намного хуже — руководители направления

ИБ есть всего в 38 % случаев. С 2017 г. рост в организациях высшего и дополнительного образования составил 10 %.

16 % организаций высшего образования имеют собственный штат для круглосуточного реагирования на инциденты кибербезопасности, ещё 17 % организовали поддержку режима 24/7 в ином формате. Для учреждений дополнительного образования цифры ниже — своё подразделение имеют всего 9 % заведений и работают с третьими лицами ещё 9 % организаций.

Треть организаций высшего образования утверждает, что имеет собственную команду CSIRT или SOC, ещё 6 % отдали его на аутсорсинг. Доля организаций дополнительного образования с собственной группой CSIRT или SOC — 11 %. Ещё 8 % работают со сторонними организациями. 56 % организаций высшего образования и 80 % дополнительного не имеют SOC вовсе.

Почти все ответившие на вопросы исследований организации (95 и 98 %) не возражают, если Jisc возьмёт на себя координацию действий и оповещение при DDoS-атаках на научно-исследовательский и образовательный сектор.

СЕРТИФИКАЦИЯ

Число университетов, прошедших сертификацию Cyber Essentials, разработанную при участии правительства Великобритании в 2014 г., выросло за год на 30 %: в 2018 г. таких учебных заведений было 14 %, в 2019 г. уже 44 %. Для организаций дополнительного образования доля ниже — сертификацию прошли всего 31 %, в 2017 г. таких учреждений было 7 %. Дальше — до Cyber Essentials Plus продвинулись 17 % университетов и 9 % учреждений ДО (в прошлые годы таких не было), а 11 % организаций высшего образования соответствуют требованиям стандарта ISO 27001 (Системы менеджмента информационной безопасности). О планах получить сертификацию ISO 27001 рассказали представители 19 % университетов и 34 % учреждений ДО.

Обязательное обучение персонала остаётся более распространённым, чем обучение студентов для 69 % университетов и 45 % организаций ДО. При этом учебные заведения дополнительного

образования чаще (20 %) проводят подготовку и студентов, чем университеты (всего 2 %).

И напоследок, 72 % университетов и 59 % организаций ДО готовы работать с SOC центром Jisc и развернуть хангпоты (honeypots) в своей сети, 14 % университетов и всего одно учреждение ДО уже сделали это. И лишь одна организация из всех опрошенных готова платить вознаграждения за поиск уязвимостей в своей сети.

СТРАТЕГИЧЕСКИЕ ВЫВОДЫ

По мнению одного из авторов исследования, главы SOC Jisc Джона Чапмена, университеты привлекательны для киберпреступников, и потому борьба с постоянно меняющимся ландшафтом угроз должна планироваться с нуля, а информационная безопасность должна быть частью цифровой стратегии университета.

Как показал массовый переход на дистанционное обучение, внедрение ИБ на всех уровнях образовательного

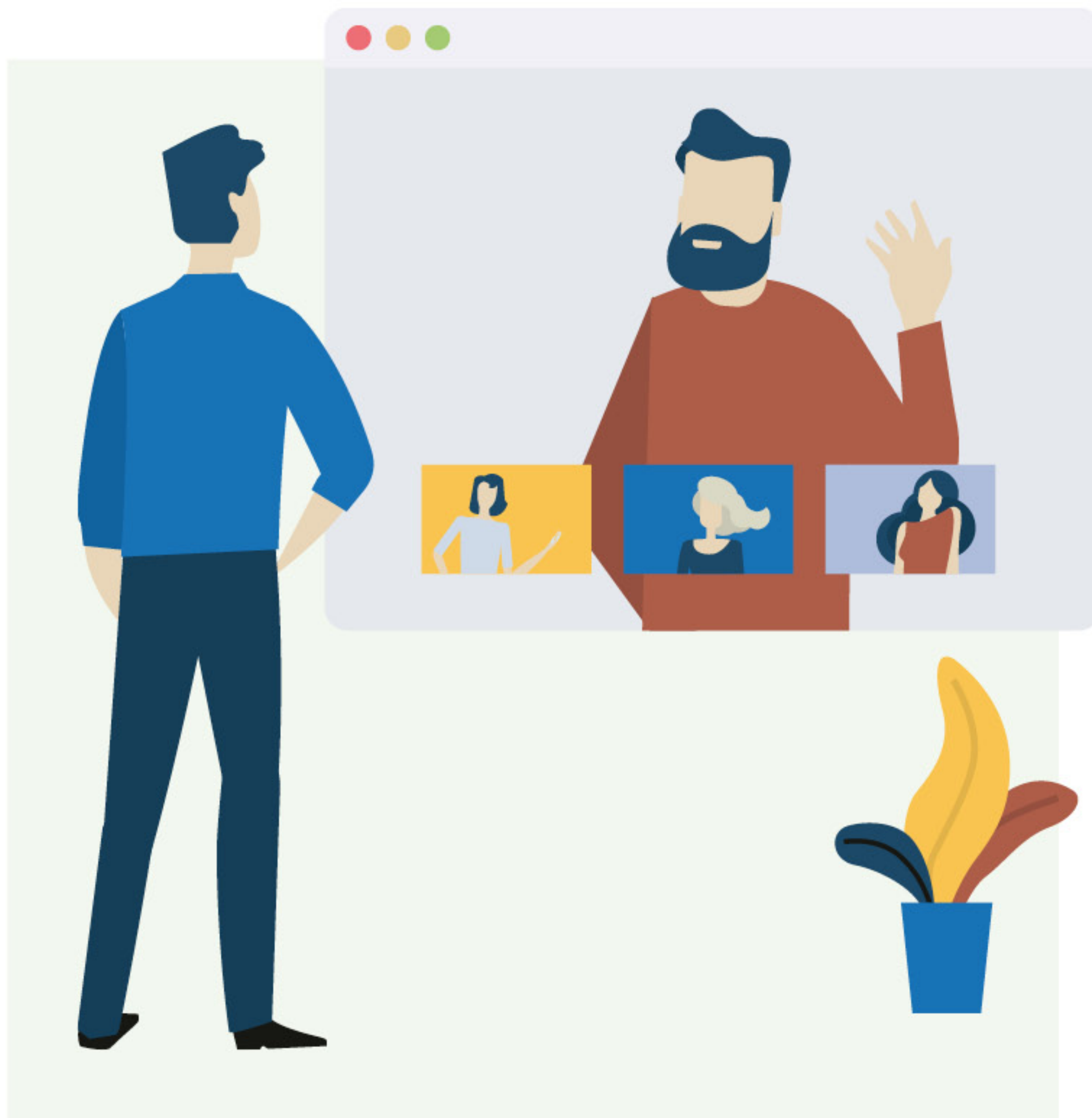
процесса должен стать массовым и обязательным не только в Великобритании или США, но и в России.

США. КОРОТКО О ГЛАВНОМ

Министр образования США Бетси DeVos назвала первых лауреатов Президентской премии образования в области кибербезопасности, учреждённой Президентом США Д. Трампом в мае 2019 г.

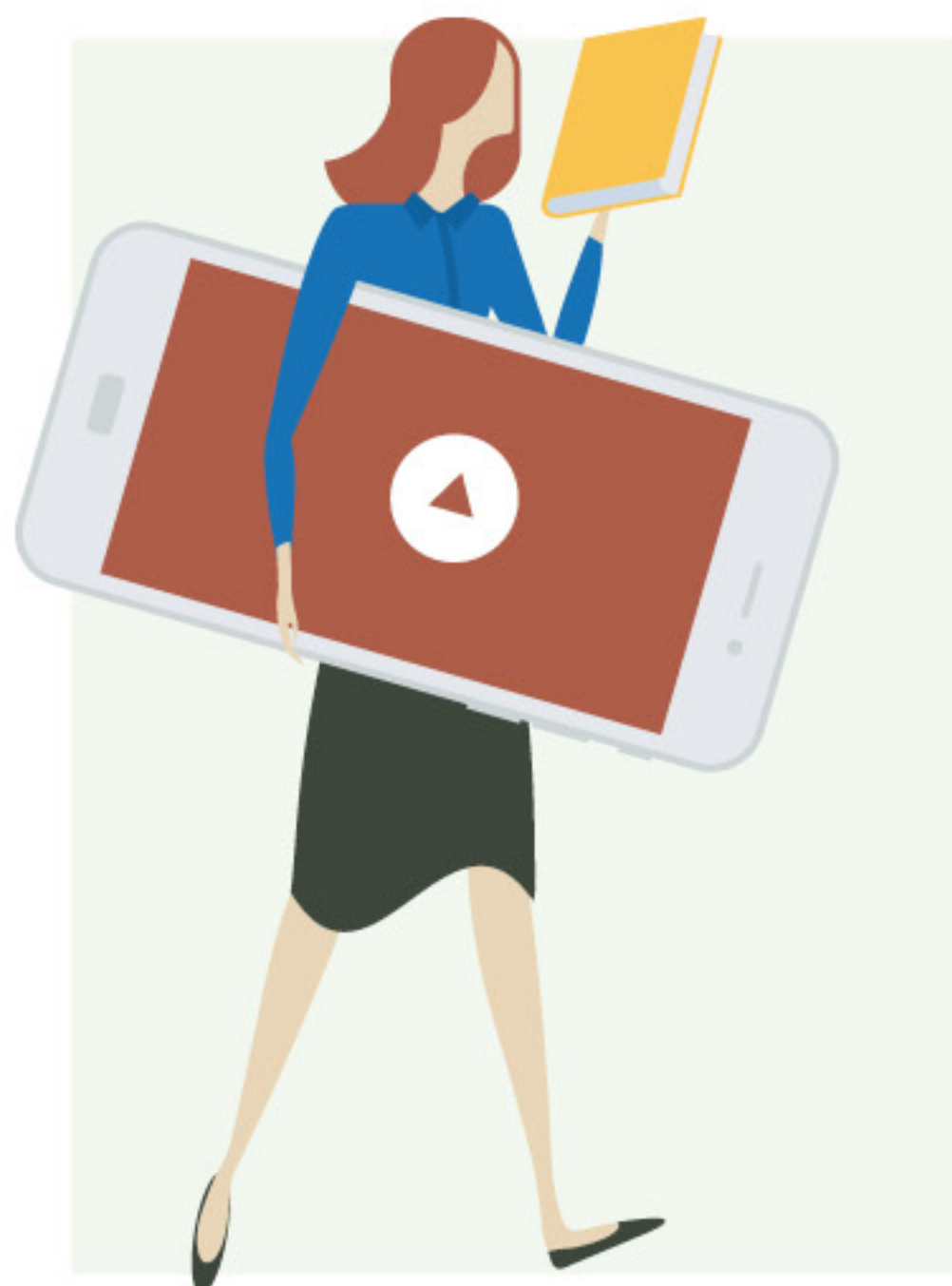
Две учительницы — Донна Вудс из средней школы Каньон-Спрингс в Морено-Вэлли, штат Калифорния, и Кара Форбеа из средней школы Нью-Тауна, Северная Дакота, получили эту награду за то, что привили своим ученикам навыки, знания и страсть к кибербезопасности.

Департамент образования получил 43 кандидатуры из 23 штатов. Первые лауреаты были отобраны по итогам демонстрации своих достижений, показателей академической успеваемости учеников и лидерских качеств, способствующих повышению уровня образования.



Директор средней школы в Нью-Тауне Кара Форбеа стала инициатором принятия образовательных инициатив в области ИБ, направленных на обучение навыкам цифровой грамотности и безопасности учащихся всех возрастов. Под её руководством учителя средней школы Нью-Тауна вели уроки кибербезопасности в классе, учащиеся школы в рамках первой ступени обучения узнали о базовых принципах ИБ и о карьерных перспективах в области ИБ. Директор стала инициатором сотрудничества школы с Летней академией государственного университета Вэлли-Сити. Также школьники смогли принять участие в проекте NASA «Ближний космос» Университета Северной Дакоты.

Донна Вудс стала создателем и руководителем программ профессионального и технического образования с упором на ИБ, которые включают в себя практическое обучение — стажировки и ученичество наряду с обучением в классе. За пять лет работы по программе ИБ в Cyber Academic Path в объединённом школьном округе Морено-Вэлли 97,4% учащихся получили отраслевые сертификаты. Ученики Вудс смогли применить полученные навыки на практике при работе сетевыми аналитиками, системными инженерами, специалистами в области IT и пр. Учительница также возглавляла команды школы на соревнованиях CyberPatriot, её ученики становились



победителями при решении сложных задач по защите виртуальных сетей.

Как лауреаты Премии Президента эти женщины получают помимо премии общественное признание как лидеры образования в области кибербезопасности и возможность профессионального развития.

ОТДЕЛЬНЫЕ ИНИЦИАТИВЫ

С осени 2020 года Александрийский технический и общественный колледж предлагает новую программу подготовки специалистов в области кибербезопасности по сертификатам. Сертификат на обучение может быть заполнен онлайн в течение одного года.

В ходе обучения по 30-дневной программе студенты получают навыки, необходимые для оценки, защиты и исправления подверженных риску компьютерных и сетевых систем, смогут работать в сфере компьютерной безопасности, включая кибербезопасность, сетевую безопасность, информационное обеспечение и расследование инцидентов, которые все считаются областями высокого спроса. Обучение будет проходить по новой системе, максимально приближенной к реальным условиям работы.

В связи с ростом безработицы по всей стране на фоне пандемии коронавируса многие ищут новые возможности в стабильных областях. По мнению руководителей колледжа, кибербезопасность является идеальным вариантом.

Единственное требование программы к поступающим — базовые знания

о компьютерах, которые могут быть изучены с помощью дополнительных курсовых работ, если это необходимо. Такой вариант повышения квалификации — отличный вариант для работающих или частично занятых взрослых, стремящихся вырастить свои навыки или перейти в новую сферу.

СМЕНА ПРОФЕССИИ

По оценкам Бюро статистики труда США, за время пандемии коронавируса более 21 млн американцев, или 16,3% трудоспособного населения страны, остались без работы. Кто-то надеется вернуться на старое место, но многим придется переучиваться и выйти на новую работу.

Среди наиболее востребованных профессий специалисты по кадрам называют программистов и специалистов по работе с данными, знатоков в области искусственного интеллекта и специалистов в области информационной безопасности.

Как отмечают эксперты, тенденция перевода работы в онлайн уже привела к тому, что уровень киберугроз вырос, повысился и спрос на специалистов по кибербезопасности. Специальность будет востребована в ближайшие годы.

Согласно исследованию компании (ISC)², крупнейшей ассоциации сертифицированных специалистов по кибербезопасности, в 2019 г. в мире работали порядка 2,8 млн профессионалов в сфере ИБ, однако для ликвидации дефицита кадров потребуется ещё 4 млн обученных работников.



Валерий КУЛИКОВ
обозреватель BIS Journal

«...ПОКА НЕ ПОТЕРЯНО ВСЁ»

О СОЦИАЛЬНОЙ ИНЖЕНЕРИИ ДЕФИЦИТА КАДРОВ

Символы современного «послешкольного» образования — ФГОСы и дистанционное («онлайн») обучение. Есть мнение, что «в эпоху стратегической неопределённости» эти механизмы позволят излечить одну из болевых точек трансформируемой экономики — кадровый «голод», нехватку «квалифицированных» специалистов. В том числе и нехватку специалистов в сфере ИТ и кибербезопасности.

Слова «голод» и «квалифицированных» взяты в кавычки в связи с тем, что обычно не слишком внятно раскрывается содержание этих понятий.

ТЕОРИЯ ХАОСА

«Голод» — это сколько и кого не хватает? В многочисленных выступлениях и публикациях ИТ&ИБ-«экспертов» наблюдается существенный разбой как в оценках потребных количеств специалистов (величины «сколько» отличаются в разы), так и в понимании содержания компетенций, что приводит к стремительному «размножению» ФГОСов. Наименования проектов этих документов, как правило, — незатейливый «копипаст» терминов, облепивших подобно тле кривую «жизненного цикла инновационных технологий» от аналитиков Gartner. Аналитики не несут никакой ответственности за свои прогнозы и неопределённость терминологии, которая тем не менее старательно воспроизводится «экспертами». Что совсем не удивительно.

Ведь костяк нынешних «экспертов» в сфере образования — это две категории людей. Первая — встроившиеся в реформы 90-х бизнесмены от

образования, предвосхитившие рекомендации премьера о том, что в бизнесе можно заработать гораздо больше, чем на ниве образования, и слившиеся с аналитиками Gartner в маркетинговом экстазе. Вторая — выпускники 90-х, продукты учебного процесса, трансформированного на основе принципа «они делают вид, что платят нам за работу, мы делаем вид, что работаем».

При этом первоочередной задачей системы высшего образования новой России стало не образование, а демпфирование катастрофических социальных потрясений, к которым неизбежно привела бы ожидаемая безработица в 40 млн человек после «реформ» 90-х.

Автоматизированная система планирования Госплана честно предсказала реформаторам эту «цифру», но принцип «Через ЕГЭ — в вуз!» позволил отложить выход на улицы молодёжи, собрав её в неопрятных аудиториях «университетов» новой России. Качество образовательного процесса отошло на второй план, но социальные потрясения оказались не катастрофическими, а всего лишь ужасными.

Но в результате базовым принципом образования стал «все мы учились понемногу, чему-нибудь и как-нибудь».

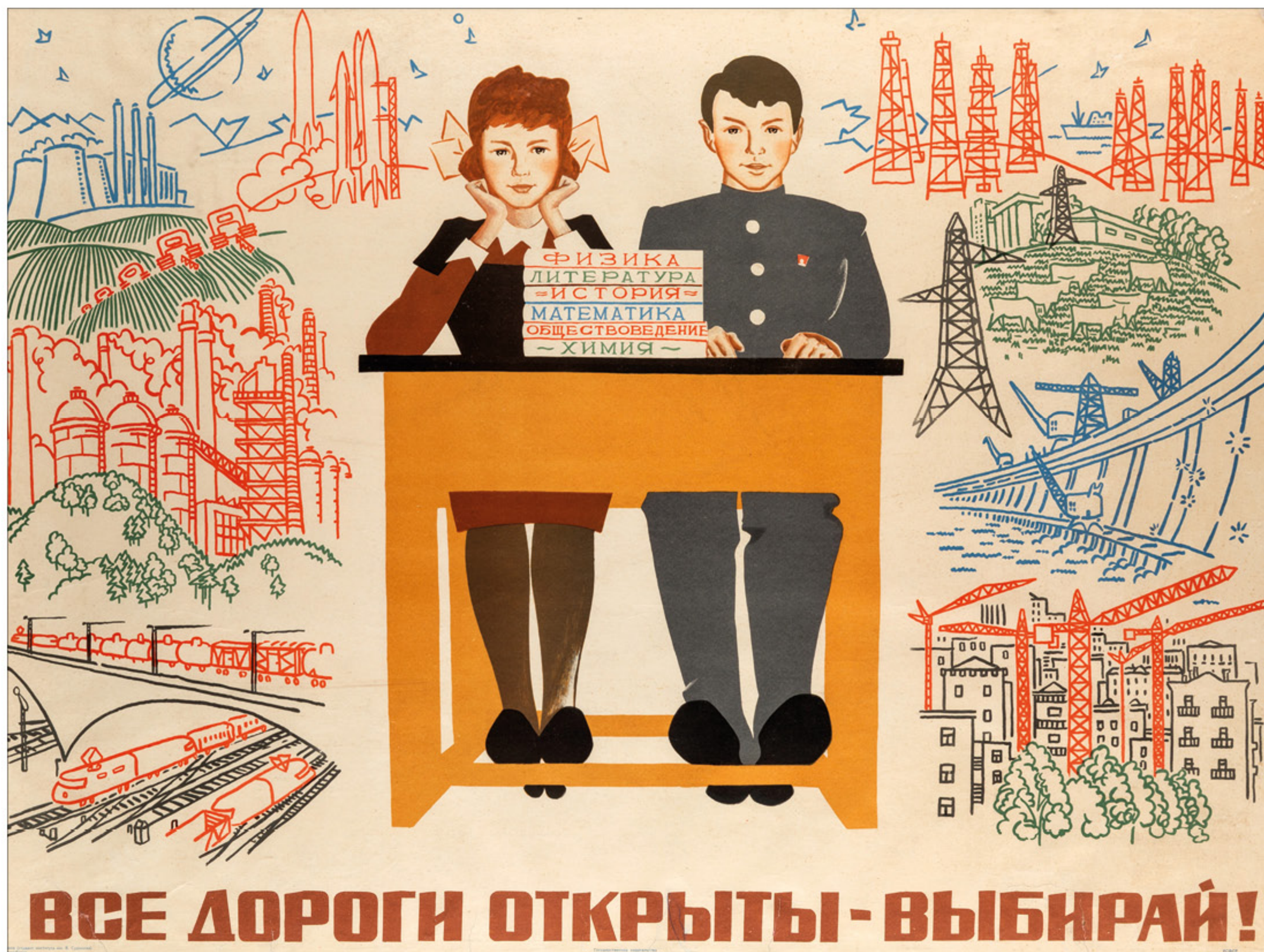
ИТ&ИБэшные студенты в этих условиях занимались текучкой реверс-инжиниринга (самостийно или по заданию преподавателей-бизнесменов) и администрированием компов, выходя в жизнь, по сути, лишь с этими «слесарными» навыками. Лишь немногие оставались в бизнесе своих «университетских» наставников и получали возможность приобрести знания, трансформировать часть этих знаний в квалификацию и научиться приобретать новые квалификации.

Те, для кого ИТ-образование было непрофильной частью образовательного процесса, изучали МС Офис и Эксель под маркой курсов «Информационные технологии в таможенном деле» и подобных со слегка варьирующимися названиями, но с одинаковым содержанием секретарского уровня.

ХОРОШУЮ РЕЛИГИЮ ПРИДУМАЛИ ИНДУСЫ?

Трансформация советских бюджетных вузов в коммерциализированные университеты новой России позволила расчистить авгиевы конюшни разрухи туалетов и общежитий. Теперь она же успешно превращает единую в прошлом систему высшего образования

В многочисленных выступлениях ИТ&ИБ-«экспертов» наблюдается существенный разбой как в оценках потребных количеств специалистов, так и в понимании содержания компетенций, что приводит к стремительному «размножению» ФГОСов



Плакат «Все дороги открыты — выбирай!», художник В. Рыбаков, 1963

в сожителство систем «специально-го» образования и высшего образования, а вузы намерена ранжировать по «кастам» — базовая, продвинутая и ведущая.

Реализовав таким образом планы, «бюджетненько» и дистанционно «клепать» специалистов по «завёртыванию гайки № 44», обеспеченных работой под заказ такого образования. А для части студентов предлагать миссионерскую функцию по получению высшего образования классической закваски без гарантий трудоустройства.

Уместно заметить, что неочевидна готовность потенциально безработных носителей «элитарного» высшего образования «выпастись» подобно конькам-горбункам на подножных кормах, с готовностью ожидая призывного посвиста поучаствовать в чём-нибудь прорывном.

Уместно заметить также, что «завёртывание гайки № 44», которое в сфере ИТ может именоваться, например, как «аналитик Siebel» или «программист на Go», отнюдь не вечно под Луной! И смогут ли в этом случае специализированные «аналитики Siebel» заняться чем-то другим высокотехнологичным — только подлежит проверке.

В своё время инженерные кадры, подготовленные штатной системой высшего образования СССР (которую по нынешним меркам можно было бы назвать «элитарной»), успешно запустили цифровизацию телекома страны и её банковской системы, не попавших в проскрипционные списки реформ 90-х. А также, к слову сказать, освоили экономику капитализма и пропаганду антисоветизма, существенно поддержав гайдаровские реформы.

НОВЫЙ ПОВОРОТ, ЧТО ОН НАМ НЕСЁТ?

Естественная убыль по разным каналам кадров старой закваски и болонская система привели к тому, что «...у нас работают люди после Бауманки, МИФИ, МГУ, но их знания вообще не нужны, по сути, ... им приходится на практике потом всё заново изучать...»

Эту проблему пытаются решить многообразием ФГОСов.

Но если говорить об ИТ&ИБ сфере, то нарастающий вал киберугроз заставляет вспомнить фразу Альберта Эйнштейна: «Вы никогда не сумеете решить возникшую проблему, если сохраните то же мышление и тот же подход, который привёл вас к этой проблеме».

А надежды на появление нового мышления хотя и не умерли, но минимальны. Ибо «мэтры» (60+), похоже, растеряли свои интеллектуальные ресурсы, встав

на путь встраивания в систему на основе субординации к начальствам. Покидать командные высоты и высотки и закрывать свой бизнес они, конечно, не собираются, но всё чаще на публичных обсуждениях киберпроблем VUCA-мира устало ссылаются на возраст и предлагают засучить рукава тем, кто помоложе.

Встроенная же в систему «молодёжь», достигшая молочно-восковой спелости (40+), также не готова переламываться: «не каждый сможет всю жизнь бегать, чтобы стоять на месте, так как часто на работе учиться некогда, а после работы не всегда есть возможность, потому что у человека есть друзья, хобби, а со временем появляется и семья...»

К тому же у неё свой взгляд на собственную жизненную миссию и на возраст, в котором от процессов созидания следует переходить в категорию рантье: «...„старички“, которым уже под 50, своё большое дело *[имеется в виду первый миллиард — прим. автора]* в жизни сделали».

И взгляды на профессию, где можно сделать упомянутое «большое дело», у них весьма упрощённые: «...как поётся в одной песне, „ещё мы делаем ракеты“, но кто из нас их видит? ...хороший компьютер стоит всего тысячу долларов. Сотня кнопок на клавиатуре — и пожалуйста: хочешь написать программу лучше, чем Microsoft или даже 1С, — пробуй!»

ЗЕМЛЯ В ИЛЛЮМИНАТОРЕ

Цитата про ракеты и 1С, кроме своего очевидного упрощенства, сводящего ИТ-квалификации к инвестициям в ПК и навыкам обращения с клавиатурой, содержит и пару скрытых смыслов, ускользнувших, по-видимому, от автора.

И не будем разбирать тот из них, что связан с бесспорной возможностью создания чего-то лучшего, чем «Microsoft или даже 1С» (напомним, при обязательном условии изменения мышления и подходов, которые и привели к созданию этих, взятых за образец, программных продуктов).

Лучше обратимся к опыту в сферах, близких к невидимым нынешнему обывательскому взгляду ракетам, а именно к космическим полётам.

Крайний раз, как принято говорить в этой отрасли, с темой космоса автору пришлось столкнуться в декабре

2019 года: слушал лекцию лётчика-космонавта Сергея Рязанского. Одна из раскрытых им тогда сторон жизни отряда космонавтов — система их подготовки, финальный этап которой — предполётное «слаживание» экипажей.

Но первый из трёх этапов подготовки — это фундаментальный общий для всех двухгодичный курс высшего «космического образования», который проходят все лётчики, бортинженеры и даже учёные.

И о пользе для борьбы с кадровым «голодом» сохранённой многоэтапной системы «космического образования», пусть сложной и дорогой, говорят не только десятилетия успехов в эксплуатации космической техники, но и тот конкретный факт, что биолог по первому образованию (МГУ им. М. В. Ломоносова), Сергей Рязанский смог подниматься в космос и в качестве бортинженера, и в качестве командира экипажа.

На этом фоне бледно выглядит по достигнутым результатам внедряемая в гражданской авиации инновационная «скороспелая» система переучивания людей в операторов для «дежурства» в кабинах «киберфизически» автопилотируемых «Боингов».

Из этого нового авиационного опыта откровенно торчат уши идеологии, скрытой в квинтэссенции уже упомянутой фразы «...всего тысячу долларов. ...сотня кнопок на клавиатуре — и пожалуйста... — пробуй!»

Кстати, недавно некоторые СМИ опубликовали внутрикорпоративные комментарии о подходах к разработке автоматических систем управления последним поколением «Боингов»: «спроектировано клоунами под руководством обезьян».

ВСЁ ЗНАТЬ НЕЛЬЗЯ, НАДО УМЕТЬ УЗНАВАТЬ

Возвращаясь к сохранённым принципам системы обучения в отряде космонавтов, уместно заметить, что это не только многие годы обучения и сотни экзаменов и зачётов, но и предварительный отбор. В числе его инструментов есть тест, когда кандидату предлагается изучить менее чем за пару дней несколько сот страниц и сдать экзамен по этому фолианту.

Те, кто выходит на такой экзамен, — это люди, способные за короткое время вычленив суть проблемы из вороха информации и приступить к её решению, опираясь на умение задавать вопросы. Когда-то этому учила система Физтеха.

Предлагая её государству и получив под её проект хорошие, как бы теперь сказали, инвестиции, отцы-основатели обещали готовить инженеров, которым нужна неделя для того, чтобы разобраться в сути проблемы и начать её решать.

Отцы-основатели не обманули государство, и страна получила ракеты разного назначения, атомный флот, включая ледоколы для Севморпути, вычислительную технику и АСУ для Госплана.

В связи с этим уместно заметить, что в упомянутой ранее фразе с упреком в сторону Бауманки, МИФИ, МГУ, возможно, также скрыто непонимание автором принципов работы на острие прогресса. Возможно, там, где сегодня бизнес пытается применить микроскоп для забивания гвоздей, никакого прогресса нет, а есть лишь попытка делать бизнес, сохраняя то же мышление и тот же подход, который привёл к проблемам.

Исправление ситуации с подготовкой ИТ&ИБ кадров в высшей школе — это дорога с двусторонним движением.

Высшая школа должна быть избавлена от превращающейся в самоцель административно направляемой волатильности принципов и вернуться к демократичной подготовке инженерной элиты; подготовке тех, кто способен и готов творчески решать проблемы, если те вдруг начинают выбиваться из регламентов, умея уверенно разбираться в самих регламентах и создавать новые.

Нынешний же работодатель должен понять, что интеллект нельзя заменить только ремеслом. А также признать то, что лафа кончилась и кадровый ресурс СССР исчерпан.

* * *

Для подготовки новых инженеров придётся и искать отцов-основателей, и отбирать абитуриентов, и тратить большие деньги на образование. Возможно, шанс ещё есть. По крайней мере, «ничего не потеряно, пока не потеряно всё» (Гёте).



Офицеры разведывательного отдела штаба 10-й воздушной армии за работой, июль-август 1945

КРИПТОГРАФЫ СССР ПРОТИВ САМУРАЕВ

К 75-ЛЕТИЮ ПОБЕДЫ НАД ЯПОНИЕЙ



Дмитрий ЛАРИН
кандидат
технических наук,
АО «Лаборатория
СКАТ»

75 лет назад советские войска, заставив капитулировать Японию, поставили точку во Второй мировой войне. В ходе советско-японской войны, длившейся с 9 августа по 2 сентября 1945 года, важную роль сыграли наши связисты и криптографы.

БОЛЬШАЯ НЕВИДИМКА

К началу боевых действий на Дальнем Востоке была организована стационарная сеть правительственной связи, которая послужила основой для развёртывания сетей связи на театре боевых действий (ТБД). Подготовка велась несколько лет.

С началом войны с Германией Отдел правительственной связи (ОПС) НКВД СССР, помимо обеспечения связи с частями действующей армии, обеспечивал функционирование сети правительственной связи в тылу, в том числе и на

Дальнем Востоке. В 1941–1942 гг. были построены станции засекреченной связи (ВЧ-станции) в Чите, Хабаровске, Владивостоке и ещё десяти городах.

В течение 1943–1945 гг. там было протянуто 2 тыс. км проводов, построено 37 узлов связи и других объектов. Но в целом пропускная способность каналов связи к началу 1945 г., их техническое состояние и протяжённость не могли обеспечить эффективный обмен информацией. Для исправления ситуации ОПС направил на Дальний Восток свои резервы.

Как и во всех войсках, перебрасываемых на Дальний Восток, в частях правительственной связи соблюдался режим секретности. Главной тайной была цель передислокации. Личному составу передовых частей, отправленных на Дальний Восток в марте-апреле 1945 г., сообщалось, что они направляются для строительства новых

и ремонта существующих линий связи. И только командиры в общих чертах знали истинную цель переброски войск.

Объяснить передислокацию было трудно: война с немцами ещё не закончилась, и солдаты и офицеры не понимали, почему они должны уезжать за тысячи километров от фронта. Однако приказ есть приказ, и эшелоны войск правительственной связи (ВПС) полным ходом шли на Дальний Восток.

После окончания войны с Германией стало легче, переброску войск теперь маскировали под эшелоны с демобилизованными, на вагонах вывешивались лозунги «Домой с Победой!» и т.д.

Разумеется, всё, что касалось переброски войск на Дальний Восток и планов предстоящих боевых действий, обсуждалось советским руководством исключительно по каналам шифрованной связи, наиболее важные сообщения передавались с курьерами. В результате

колоссальную по масштабам переброску войск удалось провести скрытно. При том, что на советском Дальнем Востоке работало множество японских агентов. Но используемые японской агентурой шифры были вскрыты нашими специалистами, благодаря чему практически всех шпионов взяли под контроль или нейтрализовали.

В ТРУДНЫХ УСЛОВИЯХ

Одной из главных задач при создании сетей правительственной связи на Дальнем Востоке стало обеспечение частей ВПС стройматериалами и необходимым имуществом. Руководство ВПС понимало, что ввиду удалённости поступление материалов потребует времени. Чтобы исключить задержку, началась переброска самого необходимого с германского фронта ещё до окончания боевых действий. В результате уже к 10 мая 1945 г. были созданы необходимые запасы. Начался ремонт существующих и прокладка новых линий связи. Работы велись интенсивно, и к началу боевых действий удалось создать эффективную сеть связи.

Поставленные задачи выполнялись в крайне сложных условиях. Значительная часть линий связи проходила далеко от железных и автомобильных, даже грунтовых, дорог. Приходилось работать в пустынях Монголии, горах и тайге Маньчжурии. Часть линий проходила через болота. Погода тоже не помогала: частые ливневые дожди, сопровождавшиеся сильными грозами и разливами рек, множество вредных насекомых... В некоторых местах отсутствовали не то что дороги, даже тропы! Материалы, имущество и продовольствие к месту работ доставлялось в лучшем случае на лошадях, ослухах или верблюдах, а в худшем — связисты несли всё на себе.

Несмотря на трудности, все работы были выполнены в срок.

БОЕВЫЕ ДЕЙСТВИЯ НА ОГРОМНОЙ ТЕРРИТОРИИ

9 августа 1945 года советские войска начали наступление. Основной была Маньчжурская операция, в ходе которой проводились локальные: Хинганско-Мукденская, Харбино-Гиринская и Сунгарийская, проводимые войсками



Погрузка торпеды с надписью «Смерть самураям!» на советскую подводную лодку Тихоокеанского флота типа «Щука», август 1945 года

Забайкальского, 1-го и 2-го Дальневосточных фронтов. Главная цель — расчленив Квантунскую армию, насчитывающую более 2 млн солдат и офицеров, и разгромить её по частям.

С точки зрения связи проблемой стала огромная площадь театра боевых действий. Только на границе СССР с Маньчжоу-го она составляла около 1,5 млн кв. км, длина фронта была более 3 тыс. км. Для захвата важных японских объектов наши войска очень быстро продвигались вглубь Маньчжурии — на отдельных направлениях на 700–800 км. И связисты не отставали.

Также проблемой было и то, что пункты управления ВПС находились на большом расстоянии между собой. Штабы фронтов удалялись от штаба Главнокомандующего на расстояние до 3 тыс. км, что объяснялось очень высокими темпами продвижения войск. Такое развитие событий было предусмотрено, в связи с чем проводилась тщательная разведка по возможной организации линий шифрованной связи.

Советские линии связи подвергались постоянному обстрелу. Например, в районе города Иман была разрушена основная проводная линия. Но во всех случаях связь оперативно восстанавливалась.

Приняли участие в организации шифрованной связи и моряки. Связь подразделений, частей и соединений Тихоокеанского флота была

организована по отработанным в ходе ВОВ схемам. Также моряки наладили надёжную шифрованную связь со штабами частей РККА для взаимодействия в ходе освобождения Южного Сахалина и Курильских островов.

В целом во время Советско-японской войны было протянуто только линий ВЧ-связи — 36 854 км.

РАДИОРАЗВЕДЧИКИ И КРИПТОГРАФЫ НКВД

В 1927 г. Спецотделом ОГПУ началось «чтение» японской шифрпереписки, в 1930-е гг. были достигнуты значительные результаты. Главным результатом этой работы стало получение информации о невступлении Японии в войну против СССР в 1941 году.

Наряду с дешифрованием японской военной переписки (этим занимались в основном армейские и флотские криптографы), важнейшее значение имело систематическое чтение дипломатических шифрматериалов. Раскрытие дипломатических шифров было возложено на дешифровальную службу НКВД.

Если военная переписка освещала ход военных действий на определённых участках фронта и позволяла делать выводы о тактических действиях противника, то чтение дипломатической шифрпереписки было призвано раскрывать стратегические замыслы и планы. В шифрпереписке между Токио



Моряки Тихоокеанского флота
водружают флаг военно-морского флота
над Порт-Артуром, август 1945 года.
Фото: Е. Халдей, источник: tass.ru

и его посольствами не раз обсуждались военные и политические планы нашего основного противника — Германии. Во многих шифртелеграммах содержалась весьма подробная информация о состоянии немецкой армии и оборонной промышленности, а также политическая информация.

Полезную информацию дешифровальная служба давала о разведывательной деятельности японских дипломатов и военных атташе. Например, их телеграммы содержали план создания японцами информационной сети в Европе. И конечно же, важнейшую роль играла информация о намерениях Японии в отношении СССР.

В период Второй мировой войны Япония имела весьма разветвлённые сети шифрованной связи в большинстве стран мира. Связь велась очень активно, применялось наибольшее количество шифрсистем, различных по своему построению и стойкости. Использовались шифры замены и перестановки, коды, а также шифрмашин. Для зашифрования текста телеграмм широко практиковалось одновременное применение нескольких кодов. Так, в 1941 г. японская дипломатия использовала 19 кодов, в 1942 г. — 20, в 1943 г. — 19, в 1944 г. — 10, в 1945 — 9. Сроки действия шифров исчислялись годами, месяцами и даже днями.

Информацию о планах Японии советское руководство получало не только из японской шифрпереписки, но и из дешифрованных немецких и итальянских телеграмм. Немцы и итальянцы активно обсуждали позицию японского руководства по разным вопросам — эта информация и становилась достоянием наших криптоаналитиков.

Анализ дешифрованных радиogramм Японии и её союзников свидетельствует, что нашим криптоаналитикам удавалось их прочитывать и своевременно докладывать эту информацию советскому руководству. По всем системам шифров за годы войны было перехвачено 132 113 телеграмм, из них дешифровано — 97 446. То есть японская переписка почти полностью контролировалась.

АРМЕЙСКАЯ РАДИОРАЗВЕДКА

Армейские радиоразведчики и криптографы действовали непосредственно на Дальнем Востоке. Первое подразделение радиоразведки было сформировано там в 1931 г. (в Хабаровске). Накануне Великой Отечественной войны было развёрнуто пять отдельных радиодивизионов, а сразу после её начала — ещё шесть.

Удара от японцев ожидали в любой момент, и потому данные радиоразведки особенно ценились. Даже в такое трудное время, как зима 1942 г., управление войсковой разведки Генштаба приняло директиву «О задачах радиоразведки на Дальнем Востоке». Вот её содержание: «За прошедший период Великой Отечественной войны отдельные радиодивизионы ОСНАЗ Дальневосточного и Забайкальского фронтов добились значительных успехов в разведке радиосетей японской армии. Улучшилось качество разведывательных сводок, увеличилось количество разведывательных сведений по данным пеленгации».

На Дальнем Востоке активно использовался опыт радиоразведчиков, работавших против Германии. В течение всего 1943 г. наши специалисты работали по выявлению группировки японских войск. Командованию нужны были не только данные по штабам округов и армий, но и по дислокации полков, батальонов, отрядов, гарнизонов, арсеналов.

Новый 1944 г. прошёл в напряжённой подготовительной работе. В ноябре отдел радиоразведки Разведуправления РККА доложил, что части ОСНАЗ Дальневосточного и Забайкальского фронтов к выполнению разведывательных задач в военное время готовы.

До начала наступления 9 августа 1945 г. радиоразведчики и дешифровальщики постоянно уточняли состав и направление движения подразделений Квантунской армии. Удалось отследить секретную информацию о срочном призыве резервов в японскую армию. Японцы ускоренными темпами проводили подготовку новых солдат и командиров. По сути наши специалисты полностью вскрыли состав и районы боевых действий войск противника.

НАСТУПЛЕНИЕ

9 августа 1945 г. на всех фронтах началось наступление наших войск. Удар был столь мощным, что управление в соединениях Квантунской армии во многом было потеряно. Некоторые радиосети вышли из строя. «Стремительное наступление Красной армии, — писал в своём отчёте начальник разведотдела 2-го Дальневосточного фронта, — вынудило японцев сразу же начать массовое отступление... В результате такого характера военных действий с первого же дня начали одна за другой прекращать работу радиостанции действующих радиосетей в приграничной полосе. Появление новых радиосетей почти не наблюдалось. Радиостанции, прекратившие работу в новых пунктах, как правило, не обнаруживались».

Начальник отделения радиоразведки разведотдела штаба 1-го Дальневосточного фронта В. Плошай описал ситуацию ещё более конкретно. «В период военных действий, — сказал он, — радиосвязь частей Квантунской армии развернуться полностью не смогла, так как стремительное наступление наших войск лишило командование Квантунской армии возможности использовать радиосвязь».

БЫСТРОТА И НАТИСК. В МАНЬЧЖУРИИ

Первоочередная задача командования во время наступления — понимать, куда отступает противник. Наши специалисты

успешно справились с этой задачей к исходу 11 августа. Наблюдая работу радиостанций штабов Квантунской армии, они установили направление отступления японцев. Те уходили в центральные районы Маньчжурии. К 19 августа советские войска расчленили силы противника в центральной Маньчжурии и завершили их окружение. Штаб Квантунской армии заявил о своей готовности капитулировать.

Однако оставались отдельные группировки, продолжавшие сопротивление. И тут наши специалисты не подкачали — определили их дислокацию в районах западнее и юго-западнее Калгана, севернее Цзямусы, Гайхуа, Датун, южнее Мукдена. Туда были направлены советские войска, сопротивление прекратилось, и 30 августа разоружение Квантунской армии было закончено.

НА МОРЕ

Наши радиоразведчики и криптоаналитики действовали не только на суше. Советский Тихоокеанский флот (ТОФ) был создан весной 1932 года, тогда же там появилось первое подразделение радиоразведки. Поначалу это были радиоразведчики и криптоаналитики поневоле, хороших специалистов не было не только на ТОФ, но и вообще в ВМФ. Тем не менее отделение проделало полезную работу по выработке подходов к использованию шифров и кодов, доля которых в радиообмене ВМС Японии непрерывно возрастала.

Задача эта была непростая, переведённые с Балтики и Чёрного моря специалисты, хоть и были уже достаточно опытными, но совершенно не знали японского языка. Язык пришлось освоить, и не только его. Сам язык, письменность, азбука катакана, её телеграфный код Морзе — всё это было так необычно, что принять текст на слух было просто невозможно. Но справились, и довольно быстро! Криптографы ТОФ совершенствовались своё мастерство и добились больших успехов в чтении японской шифрпереписки.

Основным источником информации являлись сообщения, зашифрованные вскрытым нашими специалистами кодом Главного штаба ВМС Японии для связи с портами и транспортом



Переговоры советского командования с представителями штаба Квантунской армии об условиях капитуляции, 1 сентября 1945 года. Фото: Г. Хомзор, источник: visualrian.ru

для организации морских перевозок. В разработке находились и другие коды ВМС Японии, но по большинству из них было слишком мало радиоперехватов в пределах возможностей, имеющихся у Дешифровально-разведывательной службы (ДРС). Накануне и во время боевых действий советские специалисты читали все сообщения японских военных транспортов и судов обеспечения, а также портовых радиостанций. Руководству ТОФ передавались сведения о маршрутах следования, характере и объёме перевозимого груза, гидрографической и метеорологической обстановке, встреченных плавающих минах, действующих фарватерах, навигационном обеспечении, занятости причальных сооружений, местах обнаружения американских подводных лодок и другая полезная информация.

Эти сведения оказались крайне важны при подготовке и проведении Южно-Сахалинской наступательной и Курильской десантной операций, при этом часть информации руководство ТОФ передавало командирам частей РККА, участвующих в этих операциях.

После объявления капитуляции японские капитаны в массовом порядке стали открывать кингстоны на своих судах, чтобы их затопить. Координаты мест затопления, отсылаемые в порты приписки, стали последними дешифрованными сообщениями для ДРС ТОФ.

НА АМУРЕ

Дешифровальщики ТОФ тесно взаимодействовали с дешифровальным отделением штаба Краснознамённой Амурской флотилии (КАФ). Отделение было создано в 1934 г. в Хабаровске и считается старейшим чисто криптографическим подразделением ВМФ СССР. Специалисты ДРС КАФ читали практически все японские шифры во время подготовки и проведения Маньчжурской операции. Объектами наблюдения были Сунгарийская флотилия, Северо-Маньчжурское пароходство, погранполицейские войска японцев и некоторые другие сухопутные сети. Информация, добытая ДРС КАФ, весьма пригодилась советскому командованию при подготовке наступления. Кстати, уже на третий день операции 90% японских радиосетей, контролируемых ДРС КАФ, прекратили свою работу.

В целом специалисты дальневосточных подразделений Дешифровально-разведывательных служб НКВД, РККА и ВМФ добывали информацию, необходимую для подготовки ударов, предопределивших сокрушительный разгром японских вооружённых сил. 2 сентября 1945 г. Япония подписала акт о безоговорочной капитуляции. В достижении этого результата есть немалая заслуга наших связистов и криптографов.



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

«ОН БЫЛ ОБРАЗЦОВЫЙ НАЧАЛЬНИК...»

О ВРЕМЕНИ И ШИФРОВАЛЬНОМ ХОЗЯЙСТВЕ
ИМПЕРАТОРА АЛЕКСАНДРА III



Картина Ильи Репина
«Приём волостных старшин
Александром III во дворе
Петровского дворца в Москве»

175 лет назад, 10 марта 1845 г., родился Великий князь Александр Александрович Романов, будущий Император Александр III. Ныне он едва ли не единственный из высших руководителей нашего Отечества XIX–XX столетий, солидарно поминаемый в целом положительно. Он вступил на престол после гибели отца Императора Александра II от рук террористов 1 марта 1881 г.

СНИЖЕНИЕ СОЦИАЛЬНОГО НАПРЯЖЕНИЯ

Как известно, корректировка реформ прежнего царствования позволила разрядить социальную обстановку и начать восстановление финансовой системы, расстроенной войной 1877–1878 гг. с Турцией. Состояние страны осветила 15-я Всероссийская промышленно-художественная выставка, состоявшаяся в Москве в 1882 г. В ней участвовали 5318 экспонентов, а количество посетителей превысило 1 млн человек. По числу участников лидировали сельское хозяйство, кустарная и лёгкая промышленность; значительным было представительство и в научно-учебном отделе.

СВОБОДНЫЙ ВЫХОД В ОКЕАНЫ

Рост экономики России в 1880-е годы позволил восстановить Черноморский флот и увеличить морские возможности в других бассейнах. Большую роль в восстановлении флота и в организации морских внешнеторговых сообщений сыграло Российское Общество Промышленности и Торговли (РОПиТ). Суда этого акционерного пароходства вышли во все океаны. Плавали и в Персидский залив, и по Индийскому океану, беспокоя Великобританию приближением к её индийским владениям, главному сокровищу британцев.

Повсеместное развитие морских сообщений настоятельно указывало на необходимость свободных выходов в океаны. Нужны были и незамерзающие порты. Такую роль должны были сыграть новые порты на Мурманском побережье и Дальнем Востоке. Император Александр III хотел, чтобы основной военный порт был устроен на Кольском Севере в обширной незамерзающей Екатерининской гавани, при этом сама гавань должна была соединиться железной дорогой с Петербургом.

«ПУТЬ ДАЛЁК — ДАЛЬНИЙ ВОСТОК»

Конечно, каждая новая задача тянула за собой множество других. Предстояло трудоёмкое и дорогостоящее освоение Севера, Сибири и Дальнего Востока. Надо было, прежде всего, заселить перспективные районы, обеспечить транспортную и телеграфную связь с ними. Но ещё

раньше надо было изучить эти места. Разведка северных и восточных морей и подходов к устьям рек Сибири активно велась ещё в 1733–1743 гг. Тогда, как известно, отрядам Великой Северной экспедиции удалось исследовать арктическое побережье Сибири, а также добраться до берегов Северной Америки и Японии.

В конце XIX столетия для организации регулярного судоходства требовалось уже детальное представление об особенностях северных и восточных морей и их берегов. На этих берегах предстояло закрепиться. Так в 1860 г., сразу же после присоединения Уссурийского края к России, в удобном заливе Японского моря был основан Владивосток.

Когда Цесаревич Николай достиг совершеннолетия, то Император Александр III отправил его в путешествие именно на Дальний Восток. Да и замысел великого транссибирского пути глубоко занимал Александра III. Цесаревича он назначил председателем комитета по созданию Транссиба, и тот очень увлёкся своим назначением. Он и заложил 19 мая 1891 г. основание Уссурийской железной дороги, соединившей Владивосток и Хабаровск. Став Императором, Николай II сохранил за собой звание председателя комитета и всё время интересовался его делами.

Но для подлинного закрепления и освоения новых территорий нужны были массы переселенцев. Активная государственная переселенческая политика XIX столетия тоже началась с 1891 г., совпав по времени с широким разворотом работ по прокладке Транссибирской магистрали.

ИМПЕРАТОРСКИЕ КАДРОВЫЕ НАЗНАЧЕНИЯ

Надо отметить, что при Александре III крупные государственные свершения вполне сочетались с оригинальными кадровыми назначениями. Так, его выдвиженцы, министры финансов И. А. Вышнеградский и С. Ю. Витте, известные своей энергичной деятельностью, пришли из железнодорожного транспорта, причём оба по образованию были математиками. Вышнеградский учился в Петербурге и стал знаменит своими трудами по теоретической и прикладной механике, теории автоматического управления. Витте блестяще



Закладка великой сибирской дороги. Его Императорское Высочество Государь Наследник Цесаревич Николай Александрович собственноручно отвозит тачку земли на полотно дороги во Владивостоке 19 мая 1891 г.

окончил физико-математический факультет Новороссийского университета в Одессе, тоже мечтал об учёной карьере, но стал железнодорожным предпринимателем.

Много позже Витте вспоминал о начале своей чиновной карьеры так. Однажды, занимая пост управляющего одной из частных дорог на юго-западе России, он в своём рапорте министру путей сообщения написал о необходимости снижения скорости движения царского поезда ввиду его чрезмерной тяжести. При личной встрече в царском поезде министр заметил ему, что на других дорогах никто не осмелился требовать, чтобы Государя везли с меньшей скоростью. На это Витте ответил: «Пускай делают другие, как хотят, а я Государю голову ломать не хочу, потому что кончится тем, что Вы таким образом Государю голову сломаете». Спустя два месяца произошла известная катастрофа с царским поездом в Борках. Прошло ещё немного времени, и Александр III уполномочил министра финансов Вышнеградского передать Витте предложение возглавить новый департамент железнодорожных дел в его министерстве, «так как Витте оказался прав».

ЗАМЫСЛЫ ОСУЩЕСТВИЛИСЬ

Инерция, заданная в правление Александра III росту экономики, действовала до самой мировой войны, определяя поступательное развитие России.

Первый поезд пришёл из Петербурга во Владивосток в июле 1903 г., всего через 12 лет после начала строительства дороги, полностью профинансированной государством. Правда, этот первоначальный путь проходил через спрямляющий трассу участок, расположенный на китайской территории в Манчжурии. С этого участка, из нового города Харбина, тогда же железная дорога прошла в новую базу Тихоокеанского флота Порт-Артур.

Транссиб стал особенно активно использоваться переселенцами из европейской части России после завершения военных перевозок, связанных с Русско-японской войной. Конечно, сильно повезло в заселении районам, расположенным неподалёку от магистрали. Уже к 1896 году там осело более 1 млн переселенцев. В 1897–1914 гг. Сибирь и Дальний Восток освоили ещё 2,5 млн новосёлов, тогда же нынешняя территория Казахстана приняла 1,3 млн переселенцев. При том, что в европейской части России в тот период активно развивалась промышленность и росло городское население.

Безусловно, здесь существенно влияние высокого естественного прироста населения Российской империи, в 1894–1914 годах, он составил 40%. Но не менее важны те льготы, которые получали переселенцы в Сибирь и на Дальний Восток.

Осуществился и замысел Александра III о железнодорожной магистрали на Мурманское побережье Баренцева моря. Но она вступила в строй лишь в 1916 г., одновременно с основанием города Романов-на-Мурмане (ныне Мурманск).

«ТАМОЖЕННЫЙ ТАРИФ» — ЭТО ДА!

Ускорение развития России в царствование Александра III исследователи связывают с переменой экономической политики: прежняя либеральная политика свободной торговли сменилась протекционизмом, поддержкой собственных производителей. Большую роль здесь сыграли новые таможенные тарифы. Свой заметный вклад в их составление внёс Д. И. Менделеев. Помимо прочего, Дмитрий Иванович показал себя успешным предпринимателем, и министр финансов И. А. Вышнеградский привлёк своего товарища по учёбе на физико-математическом факультете к разработке тарифов на нефтехимические продукты и оборудование. Конечно, мы знаем Д. И. Менделеева прежде всего как великого химика. В 2019 году исполнилось 150 лет «Периодической системе элементов», носящей его имя. Но сам Дмитрий Иванович о главных своих достижениях отзывался так: «Что «Общая химия», вот «Таможенный тариф» — это да!»

С. Ю. Витте, министр финансов в правительствах Александра III и Николая II, указал в своих мемуарах: «Император Александр III не был ни либералом, ни реакционером, а был — честный, благороднейший, прямой человек... он был образцовый начальник, образцовый хозяин... Если что-нибудь он сказал, то на его слово можно было рассчитывать, как на каменную гору. Он твёрдо настаивал на введении протекционной системы, благодаря которой... недалеко уже то время, когда Россия будет одной из величайших промышленных стран».

«ЦАРЬ-МИРОТВОРЕЦ»

Всё же главным достижением правления Александра III обычно признают обеспечение мирного развития России, сопровождавшегося заметным ростом

её международного авторитета. Все 13 лет его правления Россия прожила без терактов и ни разу не участвовала в войнах. Хотя межгосударственные отношения складывались порой для неё весьма напряжённо. Так, в 1887 г. началась «таможенная война» с Германией, которая завершилась в итоге справедливым и выгодным для России торговым договором 1894 г.

Александр III вошёл в историю как «Царь-миротворец». Такая оценка впервые прозвучала осенью 1894 г., когда Император уже был близок к своей неожиданной и безвременной кончине. В европейских столицах тогда признавали: «Мы теряем арбитра, который всегда руководствовался идеей справедливости». Даже негативно отзывавшийся о политике России британский маркиз Солсбери заявил: «Александр III много раз спасал Европу от ужасов войны». Так, энергичные действия русского Царя предотвратили войну Германии с Францией в 1887 г. Современник Александра III, немецкий историк О. Егер написал для «Всемирной истории»: «Подобно всем государям, сознающим свою силу, он никогда, нигде и никому не угрожал ею и ни разу не воспользовался в ущерб чьих бы то ни было интересов... Постоянно имея в виду только интересы и достоинство России, Александр III вёл свою политику открыто, не прибегая ни к каким ухищрениям, держась в отношении к другим державам безукоризненной прямооты и неуклонной справедливости... Россия, возведённая Императором Александром III на высшую степень могущества, получила решающий голос в делах европейских и азиатских».

ХОДЯЧИЙ АРХИВ МИДА

По свидетельству современников, Александр III был подлинным организатором своей дипломатии и, вероятно, справедливо его высказывание: «Я сам себе министр иностранных дел». Но и МИД во главе с Н. К. Гирсом обеспечивал ему квалифицированную помощь.

Особенный авторитет у Императора имел благодаря своей работоспособности и компетентности Владимир Николаевич Ламздорф. В 1882 г. он возглавил канцелярию МИДа, с 1886 г. стал

первым советником министра и по совместительству вошёл в Комитет шифров. Позже, при Николае II, он получил назначения вначале товарищем министра, а затем и министром иностранных дел. При всём противоречии отзывов о нём, по мнению многих современников, Ламздорф был «ходячим архивом министерства иностранных дел по всем его секретным делам», деловым и скромным человеком. В. Н. Ламздорф оставил для истории свой дневник 1886–1896 гг., ныне он опубликован. Это 26 больших тетрадей с подробным описанием на французском языке событий и документов. В дневнике более пятидесяти раз упоминается о доложенных Александру III и Николаю II материалах дешифрования дипломатических телеграмм и резолюциях государей на них. Это переписка послов в России со своими правительствами, обмен телеграммами английского посла в Персии с министром иностранных дел Великобритании, немецкого посла в Турции с Берлином, между Берлином и Парижем и т.д.

«ШИФРЫ ВСЕХ ВЕЛИКИХ ДЕРЖАВ ВСКРЫТЫ»

Вот запись от 14 апреля 1890 г.: «Вчера министр послал [государю] перлюстрированную телеграмму германского Генерального штаба к [военному атташе] Йорку фон Вартенбургу от 11 апреля следующего содержания: «Важный документ № ... будет отправлен вам сегодня вечером с курьером. Генеральный штаб». Около номера Его Величество поставил красным карандашом «13» и написал: «Нельзя ли постараться разобрать, какой №. Я думаю, что должно быть № 13». После

того как шифровальный отдел подтвердил это предположение, государь приписал на том же документе: «Если это № 13, то нет сомнения, что Йорк выкрал из главного штаба расписание № 13» (то есть самое последнее, самое новое мобилизационное расписание). Его Величество сказал министру, что в это дело, требующее особой осторожности, не должен быть посвящён никто, кроме [петербургского градоначальника] Грессера, и что последнему, не сообщая об источнике нашей информации, необходимо поручить следить за приезжающим сегодня германским курьером и за Йорком, для того чтобы знать, кому будет передан полученный им пакет».

2 декабря 1895 г.: «Вчера в 2 часа собирався Комитет по шифрам. Послушать наших перлюстраторов, так они делают в самом деле просто чудеса, однако количество чиновников, занимающихся этим благородным ремеслом, недостаточно, и целую массу телеграмм подвергнуть дешифрованию не удаётся. Шифры всех великих держав и большей части других стран вскрыты; один лишь австрийский шифр не поддаётся усилиям наших перлюстраторов, и поэтому никогда не удавалось читать секретную переписку венского кабинета».

Показатели дешифровального отделения по работе с телеграммами за 1883–1892 гг. приведены в таблице 1, также указаны данные за предыдущее десятилетие.

По результатам дешифрования дипломатической переписки руководство России имело достаточно ясное представление о реальных сообщениях иностранных представителей в Петербурге своим правительствам. Например,

	1883–1892 гг.	1873–1882 гг.
Количество входящих телеграмм	39524	21107
Количество разобранных телеграмм	12431	8062
Процент разобранных телеграмм	31	38
Среднее число служащих	4	3,3
Среднее число разобранных телеграмм на одного служащего	3107	2442

Таблица 1. Показатели дешифровального отделения по работе с телеграммами



Портрет императора Александра III, 1896 год, художник Н. Дмитриев-Оренбургский

Ламздорф 25 ноября 1890 г. отметил, что «перлюстрации телеграмм турецкого посла [Гусни-паша] убедили нас в том, что он имеет несчастную привычку представлять своему правительству всё происходящее в совершенно ложном свете».

«МЕНЯ ПРЕДУПРЕДИЛИ...»

Перлюстрация позволяла проследить, насколько точно иностранные дипломаты информируют своё руководство о собственных официальных беседах в Петербурге, и даже узнать о содержании разговоров российских послов с иностранными министрами. Так, 28 февраля и 5 марта 1891 г. в дневнике отмечено, что из перлюстрации телеграмм министра иностранных дел Франции А. Рибо его послу в России А. Лабулэ стало ясно — посол России во Франции А. П. Моренгейм прочёл французскому министру не только официальное письмо министра Н. К. Гирса, но и «личную собственноручную записку, которую г. Гирс послал ему 19 февраля. Моренгейм отнюдь не был на это уполномочен». Со своей стороны Гирс на тексте перлюстрированной французской телеграммы сделал помету для императора: «Хотя и не поручал барону Моренгейму прочесть моё письмо г. Рибо, но, может быть, он недурно сделал, решившись на такое сообщение». Рядом помета Александра III «Да», подтверждающая одобрение рискованного шага российского посла.

6 июня 1895 г. В. Н. Ламздорф привёл фрагмент дешифрованной телеграммы германского посла, отправленной в Берлин: «Использую этот шифр из осторожности, так как предыдущий употреблялся слишком часто и у меня появились основания для недоверия. Меня предупредили, прошу о новом шифре». Это было уже при новом министре А. Б. Лобанове. Далее В. Н. Ламздорф добавил свой комментарий: «Сабанин, старший чиновник нашей экспедиции по перлюстрациям, прилагает к данному документу письмо на имя князя Лобанова; в нём он привлекает внимание министра к вредности тех «предупреждений», наличие которых выясняется из телеграммы. Совершенно очевидно, что проболтаться в данном случае могли Лобанов или Шишкин (товарищ, т. е. заместитель

министра — Б.С.) при их разговорах с дипломатами или же с министром финансов и его агентами».

ГЛУБОКОЙ НОЧЬЮ

По записям в дневнике можно составить представление и о трудоёмкости применения собственных дипломатических шифров. Вот что Ламздорф сообщил о расшифровании телеграммы, доставленной вечером 9 марта 1890 г.: «Из Берлина только что получена длинная телеграмма; дежурный чиновник Столыпин приносит её мне; она начинается словами: «Строго личная». Это шесть листов шифра, к которым вскоре добавляется шесть листов продолжения. Сажусь тотчас за работу. Вернувшийся около 11 часов Оболенский немного мне помогает. Когда министр возвращается из театра, я решаю ввиду важности известий прочесть ему расшифрованную первую половину. Заканчиваем расшифровку около половины третьего. Оболенский уходит, и я проверяю и переписываю текст, чтобы иметь возможность послать его рано утром министру». В телеграмме, отправленной послом Шуваловым, тогда сообщалось о его встрече с германским императором Вильгельмом II и об отставке канцлера Бисмарка. Положение с расшифрованием «строго личных» телеграмм несколько облегчалось тем, что квартиры руководителей МИД находились в его здании.

МЕРИЛО ВОЗНАГРАЖДЕНИЯ

1 ноября 1886 г. Александр III утвердил новое Положение о Цифирной части, занимавшейся шифрами, и ввёл его в действие «негласно с целью неразглашения мер по улучшению деятельности шифровальной части».

Сохранилось разделение Цифирной части на две экспедиции (отделения). Первая обеспечивала разработку собственных шифров, вторая занималась дешифровкой дипломатической корреспонденции. Были расширены штаты дешифровальщиков: к прежним трём чиновным должностям добавили ещё две — младших чиновников. Увеличено было и поощрение «с целью удержания их как можно долее при их специальных занятиях и вознаграждения за малую подвижность их служебной карьеры».

Содержание нового Положения о Цифирной части предварительно обсуждалось в Комитете по шифрам. Старший чиновник Л. П. Иессен предлагал установить для младших чиновников прибавку за каждые пять лет службы в 20 % от жалования, мотивируя это тем, что «через 15 или 20 лет деньги ещё удешевятся, а жизнь неминуемо настолько же вздорожает». Он также критиковал предложение решать вопрос о размере вознаграждения за разбор иностранного шифра, исходя из его важности в данный момент. Иессен напомнил, что ранее такой вопрос уже поднимался. Но, «несмотря на скупость покойного канцлера Горчакова на трату казённых денег», пришли к выводу, что «не полезность шифра, а трудность разбора его должна служить мерилом вознаграждения», ибо «на этой системе постоянных поощрений зиждется успех сего многотрудного дела». В результате в новом Положении о Цифирной части МИД предусматривалась доплата старшему, младшим чиновникам и помощникам младших чиновников за каждые пять лет в размере 15 % штатного оклада, «присвоенного должности, которую они занимают в день выслуги этой надбавки». Прежние премии за вскрытие нового шифра (до 800 рублей) были сохранены.

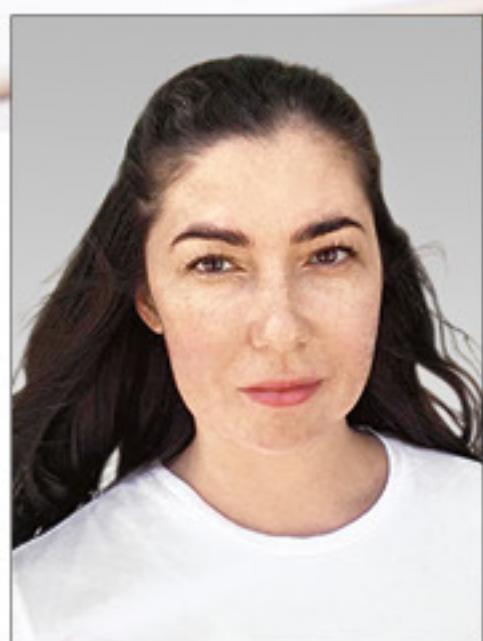
Каким мог быть единовременный годовой оклад с пятилетними прибавками, видно на примере старшего чиновника тайного советника Л. П. Иессена. Он прослужил к 23 августа 1888 г. двадцать пять лет, и ему начислили в качестве вознаграждения 4400 руб. Сколько получали криптографы в начале своей карьеры, можно узнать из послужного списка К. В. Циглера. Он был допущен к секретным занятиям с 16 ноября 1895 г., испытательный срок закончился через месяц. С января 1896 г. ему было установлено жалование 50 руб. в месяц как помощнику младшего чиновника, но 22 августа его назначили младшим чиновником и с 31 июля установили жалование 125 руб. в месяц.

Надо также отметить, что для чиновников цифирных экспедиций должности не имели классности. Поэтому младший чиновник мог дослужиться до статского советника — гражданско-го чина уже генеральского ранга! Это были весьма доверенные работники.

ПО ТРУДАМ И ЧЕСТЬ

Когда в 1890 г. Германия воздержалась от продления договора с Россией, летом 1891 г. министр Н. К. Гирс и В. Н. Ламздорф стали готовить соглашение уже между Россией и Францией. Это означало резкий поворот во внешней политике России от многолетней ориентации на союз с Германией. В связи с высокой секретностью данного манёвра Александр III просил Н. К. Гирса скрыть информацию о будущем соглашении даже от его единственного заместителя Н. П. Шишкина. Государь тогда приказал, чтобы «только один старший чиновник г. Битепаж (начальник дешифровального отделения — Б.С.) был допущен к расшифровке французских телеграмм, касающихся этих переговоров». Между прочим, после завершения переговоров К. А. Битепаж стал действительным статским советником, что соответствовало званию генерал-майора, согласно Табели о рангах.

28 августа 1892 г. этот чиновник представил Комитету по шифрам семь работ своего отделения: генеральный шифр правительства Великобритании для связи с посольствами в Санкт-Петербурге, Тегеране и Константинополе, действовавший с декабря 1890 г.; сербский шифр для связи правительства в Белграде с сербской миссией в Санкт-Петербурге, действовавший с июня 1889 г.; французский генеральный шифр, которым с мая 1883 г. четыре года пользовались Военное и Морское министерства в сообщениях с экспедицией адмирала Курбе в Китай; три немецких генеральных шифра для переписки правительства Германии с посольствами в Санкт-Петербурге и Константинополе, а также с консулами в России, бывшие в употреблении с апреля 1889 г.; французский специальный шифр, использовавшийся с декабря 1890 г. правительством Греции для связи с греческой миссией в Петербурге. В основном эти работы были коллективными. Все исполнители за каждую из разработок получили от 300 до 800 руб. Их трудами постоянно пополнялись важными документами министерские папки для докладов Императору Александру III.



**Валерия
ЧАПЧАЕВА**
руководитель спец-
проектов Медиа
Группы «Авангард»

«НАША ИГРА» НА УДАЛЁНКЕ

КАК ЭЛИТАРНОЕ ШОУ ВО ВРЕМЯ КАРАНТИНА
ВЫШЛО В ОНЛАЙН И СТАЛО МАССОВЫМ

Недавно всех нас накрыло волной самоизоляции. Началась Великая удалёнка... Но вместе с осознанием неизбежности и необходимости #stayhome пришло понимание, что дома можно и нужно заниматься не только работой...

Мы искали «наш» формат для наших людей — людей, которые любят и

ценят мероприятия «Авангарда», с удовольствием их посещают и участвуют в активностях. После серии мозговых штурмов решение пришло: общая для всех онлайн-игра по информационной безопасности.

В прошлом году с большим успехом мы провели первый сезон интеллектуального шоу в закрытом клубе «Наша

игра». Этакий симпатичный междусобойчик, великосветская туса с любимым развлечением. Собрались семь лихих команд ИБ-эрудитов. Они азартно отвечали на каверзные вопросы «великого и ужасного» ведущего Алексея Лукацкого, часами общались после игры, вместе с гостями праздновали победы и не расстраивались из-за

поражений. Этот живой формат покорила не только активных участников и зрителей, но и тех, кто не был вполне уверен в своих ИБ-знаниях. Все с удовольствием обсуждали вопросы, темы очередных туров игры, и мы понимали, что такой опыт пришёлся специалистам по вкусу.

ВЫХОДИМ В ОНЛАЙН

Именно отсюда — из этого закрытого и элитарного, в общем-то, развлечения и родился массовый онлайн-формат «Нашей игры», который пришёлся как никогда ко времени. Ведь специалисты ИБ оказались лишены привычных мероприятий, по сути, остались без живого как профессионального, так и личного общения.

При запуске таких проектов всегда возникают сомнения, переживания, но мы загорелись, мы постарались, и у нас получилось!

КАК ЭТО БЫЛО

Раз в неделю у экранов собирались для общения люди, самые разные люди, которых было бы невозможно объединить, если бы они сами не чувствовали тягу к «умному» отдыху в компании

«своих». В игре встречались и банковские безопасники, и специалисты по ИБ из небольших учреждений — медицинских центров, администраций небольших городов и региональных компаний. Вся ИБ-Россия! Мы и не рассчитывали на такое разнообразие и географию и, конечно, очень быстро ощутили масштаб ответственности.

Темы игр соответствовали происходящим в те дни событиям: «Криптографический фронт» (ко Дню Победы), «Российская ИБ», «Безопасность в эпоху самоизоляции» и т.д.

Немного о технической составляющей. В игре могли участвовать все желающие, достаточно было иметь под рукой два компьютера, но кто-то ухитрялся играть и с одного. За правильные ответы начислялись очки. После каждого ответа на экране появлялся рейтинг из самых успешных игроков.

НАМ ПОМОГАЛИ

Кажется, нашим участникам нравилось получать наши подарки, так же, как и нам их дарить. Нам нравилось делиться поддержкой, нравилось активное, живое участие людей. Конечно, у нас были единомышленники, которые помогали

В ПОРЫВЕ ТВОРЧЕСТВА

Чтобы зрителям — всем, а не только профессиональным безопасникам, — было интересно наблюдать, а игроки не переживали по поводу постоянных изменений в рейтинге, мы периодически проводили творческие конкурсы на самые разные темы.

О, этот творческий конкурс совершенно точно заслуживает отдельного внимания! Люди в разных концах страны в едином порыве сочиняли стихи о безопасности, яркие слоганы и захватывающие сценарии... И даже придумывали инновационные ИБ-продукты (не удивлюсь, если некоторые из них уже взяты в конкретную разработку). Вы только вчитайтесь в эти строки — шедевры словесности!

Тавтограммы

Шмеркалось! Шестой шифровальщик шифровал шепелявя шифром широкий шрифт. Шок!

Сломал сеть самурай, сломал совсем, слёзы, стенания в серверной...

Сценарии фильмов

Звёздные безопасники: призрачная угроза. Давным-давно в одной далекой-далекой серверной...

ФСБ слезам не верит. А не надо было хакать...

Великолепный стек. История одной долгой разработки

ИБ-продукты

«ДУБ» — ИБ-стажер пришёл в вашу компанию

VPN-шлюз «Ручеёк». И ваша информация всегда защищена кристально чистым извилистым шифрованием!

Кибероружие «Выпускник». Наш энтузиазм и любопытство положат любую систему!

Ну вот, вы уже улыбаетесь.

Это создавало отличную творческую и дружескую атмосферу общения. Этакий глоток свежего воздуха после трудного дня в душной домашней серверной.

BIS-СПРАВКА

Телешоу «Наша игра» — проект Медиа Группы «Авангард»

Формат: интеллектуальное состязание 3–5 команд из 5 человек на закрытом заседании клуба «НАША ИГРА».

Условия: игра на выбывание. Команды отвечают на вопросы по ИБ и зарабатывают баллы. Серия игр завершается грандиозным финалом.

Популярность: в 2019 г. первый сезон шоу из пяти игр посмотрели в записи более 10 тыс. человек. В апреле-мае 2020 г. игра проводилась в онлайн-режиме. Играли 700 человек, были зрителями и участниками активностей — 3 тыс. человек.

Сайт: ib-bank.ru/igra





Фотографии победителей «Нашей игры home edition» с призами от Медиа Группы «Авангард»

подготовить это сногшибательное действо. Вопросы готовили и Алексей Лукацкий, и сообщество RUSCADASEC, и специалисты Банка России. Кстати, последние дали участникам шанс взглянуть на себя как на рядовых клиентов банка, а не как специалистов ИБ. И это тоже был очень интересный опыт.

Знаем, что многие любят цифры и бренды. Нашу игру посмотрели в онлайн-режиме 3000 человек, а играли почти 700. Впечатляет, верно? Среди игроков были сотрудники компаний Сбербанк-Технологии, Ассоциации ФинТех, КриптоПро, ИнфоТеКС, R-Vision, Positive Technologies, PwC, Softline... Участвовало и подрастающее поколение безопасников — из колледжа связи № 54. И это только те, кого удалось опознать. География одних только

победителей впечатляет — Москва, Челябинск, Петрозаводск, Рыбинск, Екатеринбург.

ЧТО ДАЛЬШЕ?

Сейчас даже немного жаль, что всё это понемногу уходит в прошлое. Начинает не хватать уютных вечеров перед экраном — шуток ведущего, комментариев коллег, ведь все потихоньку возвращаются к привычной занятости.

Но зато теперь есть понимание, что «Наша игра» нужна, что её ждут. И мы снова не подведём! Для нас «Наша игра» — это большая и важная часть жизни «Авангарда» и всех наших друзей, это наша история, которая не должна закончиться. Сообщество специалистов по ИБ активно существует, и ему интересны интеллектуальные

развлечения, а значит, всегда найдётся и пространство для комфортного общения.

Уже есть предложения использовать этот отличный опыт и дальше, например, проводить такие игры внутри крупных ИБ-компаний. Игровая форма способствует лёгкости: даже выбрав не тот ответ, улыбаешься, понимая, что это всего лишь игра. Так что будем укреплять игрой корпоративный дух!

ДО СКОРЫХ ВСТРЕЧ!

Мы прошли вместе трудное время самоизоляции и движемся вперёд. А вот что ещё мы предложим в скором будущем, мы вам обязательно расскажем. Ждите наших новостей и готовьтесь к новым интеллектуальным свершениям!

АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Образование
и карьера

ib-bank.ru

BIS Journal



ЛЕТ



За

**информационную
безопасность**