

BIS

JOURNAL

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ
БИЗНЕСА

№4 (51) 2023

**Борис
МИРОШНИКОВ**
ГК «Гарда»
«ИБ – давно
самостоятельная
отрасль» → 52



Андрей ЕФРЕМОВ
«Лаборатория
Касперского»
Вместе
можно сделать
больше → 56



Защита данных: сохранить всё

Дмитрий ДУБЫНИН
Минцифры
Пять
вопросов → 76

Марина БРОДСКАЯ
BIS Journal
Под названием
NGFW... → 88

Олег ХНЫКОВ
Positive Technologies
Как SOC и NOC
спасают бизнес → 91





SOC Tech: Практическая конференция
для руководителей ИБ-подразделений
и специалистов в области мониторинга

Основные темы

- ◆ Технологии обнаружения
- ◆ Реагирование, автоматизация и отчетность (BI)
- ◆ Treat Intelligence и Treat Hunting
- ◆ Практика расследования киберинцидентов
- ◆ Автоматизация Pentest, BAD
- ◆ Риск-ориентированный мониторинг



ib-bank.ru/soctech

30 ноября 2023, Москва
кибербез-хаб КИБЕРДОМ



Артём ЗУБКОВ
генеральный директор
Медиа Группы «Авангард»

Дорогие читатели, представляем вам «BIS Journal – Информационная безопасность бизнеса»! Обновлённое название означает, что тематика журнала отныне охватывает кибербезопасность всех российских компаний, независимо от сферы деятельности и формы собственности. Наша цель – расширить аудиторию и предоставить возможность новым авторам выразить свой взгляд на вопросы информационной безопасности в различных отраслях. Уже скоро вы найдёте печатные экземпляры BIS Journal на ключевых деловых мероприятиях, посвящённых темам информационной безопасности и информационных технологий.

Меняя концепцию, мы сохраняем то, что всегда выделяло BIS Journal: глубину проработки вопросов, внимание к нюансам и взвешенную позицию, рассказ доступным языком о сложных вопросах. Журнал по-прежнему будет служить площадкой для дискуссий, расширять кругозор читателей и предлагать им полезные советы, привлекать к сотрудничеству практиков защиты информации и регуляторов отрасли. А веб-портал и электронная версия продолжат развитие в качестве оперативного источника новостей, справочной и аналитической информации в области информационной безопасности.

Мы планируем сохранить активную поддержку социально значимых проектов, связанных с воспитанием кадров для отрасли, включая ежегодные церемонии награждения победителей олимпиад для школьников по криптографии и по компьютерной безопасности (с 2011 года), а также информационное сопровождение деятельности НКО «Фонд содействия развитию безопасных информационных технологий», направленной на укрепление исторической памяти о подвигах отечественных криптографов и служб радио-разведки в годы Великой Отечественной войны.

Уделяя внимание всем аспектам информационной безопасности, мы поможем нашим читателям лучше ориентироваться в современном ландшафте технологий, в актуальных подходах, законодательных актах и киберугрозах. Рассказывая в деталях об обеспечении информационной безопасности бизнеса, BIS Journal сможет делать больше для укрепления информационной безопасности России.

Благодарим вас за интерес и представляем новый BIS Journal – Информационная безопасность бизнеса!



ИЗДАЁТСЯ С 2010 ГОДА

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Батранков Д. В. — руководитель направления сетевой безопасности Positive Technologies
Былевский П. Г. — шеф-редактор, доцент департамента ИБ Финансового университета при Правительстве РФ, доцент кафедры международной ИБ МГЛУ, 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. — старший научный сотрудник ФГУП «ЦНИИХМ»
Вихорев С. В. — советник генерального директора по информационной безопасности IT Expertise
Дзержинский Ф. Я. — независимый эксперт
Зубков А. Н. — генеральный директор ООО «Медиа Группа „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Калашников А. И. — управляющий директор Центра информационной безопасности дочерних и зависимых обществ Газпромбанка (АО)
Курило А. П. — советник по вопросам ИБ ФБК и FBK CyberSecurity, кандидат технических наук
Левиев Д. О. — председатель Совета НП «Партнёрство специалистов по информационной безопасности»
Мельников С. Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», доктор физико-математических наук
Некрасов И. В. — главный редактор журнала
Одувалов М. В. — директор службы Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО)
Окулесский В. А. — вице-президент по информационной безопасности ЦМРБанка, кандидат технических наук
Пазизин С. В. — заместитель начальника Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО), кандидат физико-математических наук
Филипчук А. А. — технический директор ГК ЦРТ
Хайретдинов Р. Н. — заместитель генерального директора ГК «Гарда»
Шумский Л. С. — руководитель службы информационной безопасности Яндекс Банка
Янсон И. А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И. В.**
 Директор по развитию: **Минаков А. В.**
 Арт-директор: **Мельников Н. С.**
 Руководитель интернет-проектов: **Воробьева А. А.**
 Обозреватели: **Бродская М. А., Покатаева Е. Н.**
 Иллюстрация на обложке: **Виктор Миллер Гаусса**
 Фото в номере: **Depositphotos**
 Цветокорректор: **Науменко М. В.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»
 Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д. 21
 Тел.: +7 495 921 42 44
 Интернет-версия: ib-bank.ru/bisjournal
 E-mail: bis@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как «BIS Journal – Информационная безопасность банков».

Зарегистрирован 11 июля 2023 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как «BIS Journal – Информационная безопасность бизнеса». Свидетельство ПИ № ФС77–85487 от 11.07.2023 г.

Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal – Информационная безопасность бизнеса». 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. Возрастная категория 16+.

Подписан в печать 10.10.2023. Тираж 5000 экз. Заказ № 2932023.
 Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS JOURNAL, 2023



BIS JOURNAL

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА

ВПЕРЕД К НОВЫМ ГОРИЗОНТАМ!

Двенадцать лет и 50 номеров назад, когда создавалась концепция журнала «BIS Journal – Информационная безопасность банков», российский финансовый сектор был безусловным лидером цифровизации и находился на передовой борьбы с киберпреступностью практически в одиночестве. На страницах журнала велись дискуссии с участием регуляторов отрасли, банков, разработчиков и поставщиков решений, специалисты по защите информации делились с читателями опытом по обеспечению информационной безопасности. Вместе с журналом развивался Уральский форум «Информационная безопасность банков», ставший основной площадкой общения по теме информационной безопасности финансовой сферы.

Полсотни номеров журнала отражают эволюцию информационной безопасности за последние годы: возникновение новых угроз, их распространение на финансовую сферу и смежные отрасли; появление новых подходов к обеспечению

кибербезопасности; становление и формирование нормативной базы по защите информации финансовых организаций. BIS Journal неизменно освещал самые актуальные и важные темы, сохраняя фокус на обеспечении информационной безопасности в банках.

Дальнейшее развитие информационных технологий, их проникновение во все виды экономической деятельности, а также расширение спектра угроз привели к тому, что тема защиты информации стала критически актуальной в ретейле, промышленности, добывающих отраслях, медицине, электронных средствах массовой информации и др. Кибератаки, проведенные в последние годы против компаний в самых различных сферах бизнеса, подтверждают этот тезис. Многие наработки финансовой сферы в области применения средств защиты, нормативного регулирования, управления информационной безопасностью, защиты данных, мониторинга и обработки инцидентов успешно внедряются в других отраслях.

Разработаны и вступили в силу нормативные требования по обе-

спечению безопасности субъектов критической информационной инфраструктуры в сфере государственного управления, здравоохранения, науки, транспорта, связи, энергетики, финансов, топливно-энергетического комплекса, атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Изданы указы Президента России «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Ужесточаются требования в части защиты персональных данных, включая введение оборотных штрафов за их утечку. Созданы Государственная система обнаружения, противодействия и ликвидации последствий компьютерных атак (ГосСОПКА) и Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

В 2023 году на Урале, на месте проведения ежегодного Уральского форума по информационной безопасности

банков, с участием издателя журнала Медиа Группы «Авангард» состоялась конференция «Цифровая устойчивость и информационная безопасность России» под патронажем Министерства цифрового развития. Планируется запуск ежегодных конференций по защите данных («Защита данных: сохранить всё») и по мониторингу инцидентов информационной безопасности и противодействию кибератакам («Технологии SOC»).

В этих условиях редакционная коллегия приняла решение о расширении задач журнала.

Представляем вам «BIS Journal — Информационная безопасность бизнеса»! Обновлённое название означает, что тематика журнала отныне охватывает кибербезопасность всех российских компаний, независимо от сферы деятельности и формы собственности. Наша цель — расширить аудиторию и предоставить возможность новым авторам выразить свой

взгляд на вопросы информационной безопасности в различных отраслях. Уже скоро вы найдёте печатные экземпляры BIS Journal на ключевых деловых мероприятиях, посвящённых темам информационной безопасности и информационных технологий.

Меняя концепцию, мы сохраняем то, что всегда выделяло BIS Journal: глубину проработки вопросов, внимание к нюансам и взвешенную позицию, рассказ доступным языком о сложных вопросах. Журнал по-прежнему будет служить площадкой для дискуссий, расширять кругозор читателей и предлагать им полезные советы, привлекать к сотрудничеству практиков защиты информации и регуляторов отрасли. А веб-портал и электронная версия продолжат развитие в качестве оперативного источника новостной, справочной и аналитической информации в области информационной безопасности.

Мы планируем сохранить активную поддержку социально значимых

проектов, связанных с воспитанием кадров для отрасли, включая ежегодные церемонии награждения победителей олимпиад для школьников по криптографии и по компьютерной безопасности (с 2011 года), а также информационное сопровождение деятельности НКО «Фонд содействия развитию безопасных информационных технологий», направленной на укрепление исторической памяти о подвигах отечественных криптографов и служб радиоразведки в годы Великой Отечественной войны.

Уделяя внимание всем аспектам информационной безопасности, мы поможем нашим читателям лучше ориентироваться в современном ландшафте технологий, в актуальных подходах, законодательных актах и киберугрозах. Рассказывая в деталях об обеспечении информационной безопасности бизнеса, BIS Journal сможет делать больше для укрепления информационной безопасности России.

ТЫ ПОМНИШЬ, КАК ВСЁ НАЧИНАЛОСЬ?



Василий ОКУЛЕСКИЙ

вице-президент по информационной безопасности ЦМРБанка, член редколлегии BIS Journal

Давным-давно, ещё в конце прошлого века, началась новая история защиты информации в России. Первой ве- хой можно считать Федеральный закон от 20 февраля 1995 г. №24-ФЗ «Об информации, информатизации и защите информации»,

когда на государственном уровне были сформулированы цели деятельности.

Появилась ЗАДАЧА, и чтобы её решить, нужны были понятные инструменты и инструкции по применению. Так появились на свет наши первые стандарты, рекомендации по

стандартизации — ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа. Общие технические требования», ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».

Можно по-разному оценивать роль банковского сектора в становлении ИБ.

В конце 90-х — начале 2000-х многие отрасли пошли своей дорогой, вплоть до разработки собственных стандартов ЭЦП и системы сертификации на соответствие отраслевым стандартам. Банк России не стал исключением и создал собственную ЭЦП «Mag-МЦИ». Но очень скоро пришло осознание, что для такого огромного сообщества, как банки России

«ВЫ ОЧЕНЬ НУЖНЫ!»



Борис МИРОШНИКОВ
вице-президент группы компаний «Гарда»

— **Какое место в становлении и развитии ИБ в России, на ваш взгляд, должны занимать отраслевые СМИ, в том числе BIS Journal? Нам важно понимать свою роль в общем процессе, а поняв, играть её достойно, ощущать себя полезными своей отрасли, профессии безопасника.**

— Наверное, в силу возраста я всегда предпочитаю «читать бумагу». Пробовал по-другому, но не нравился. «Невкусно!» Очень ценю ваш журнал, изучаю регулярно, по мере появления. Он в лучшую сторону отличается от других таких же — отраслевых. У вас нет раздражающей комплиментарности, помпезности.

Вы интересны деловитостью и демократичностью — у вас много интересных и разнообразных авторов. Что нужно? Нужен спор, дискуссия. Показ альтернативы, другого мнения.

Важно и то, о чём мы говорили: какие специалисты нужны? Каких перебор? Разбор ошибок! Это всегда важнее, чем убогие «лучшие практики». Маловато обзоров зарубежного опыта. Объективного. Тем более что опыт там средний, рассчитанный на среднего западного обывателя, а не на нашего бунтаря. Но это не беда, опыт — это всегда интересно. Только в умном исполнении.

Вы очень нужны! Прислушивайтесь к людям, и они это оценят. Успехов!

того времени, нужны единые требования, единые подходы к оценке их выполнения, обобщение передового опыта, методическая помощь новичкам... И как ответ на этот вызов появилась первая редакция знаменитой серии Стандартов Банка России СТО БР ИББС-1.0–2004 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». С появлением этого семейства стандартов финансовая отрасль стала практически законодателем мод в развитии ИБ.

Дальнейший путь от ISO/IEC 27001:2005 до ГОСТ Р ИСО/МЭК 27001–2021 банковская система России прошла довольно ровно, сформировав понимание универсальности базовых основ построения цельной системы обеспечения ИБ.

Активная деятельность банковского сообщества по развитию и совершенствованию ИБ потребовала создания информационной,

дискуссионной площадки, где специалисты могли бы обменяться своими мнениями и сомнениями, поделиться опытом — успешным и не очень, создать, наконец, целую, как сейчас модно говорить, экосистему. И такой отраслевой информационной экосистемой стал «BIS Journal — информационная безопасность банков».

За 12 лет активной работы журнал опубликовал сотни статей корифеев ИБ, регуляторов, представителей властных структур, разработчиков и интеграторов, преподавателей и студентов. Список авторов и читателей давно вышел за рамки банковской отрасли. Сейчас BIS Journal — это не просто журнал, это место, где сталкиваются разные мнения, рождаются решения, открываются новые имена, талантливые специалисты... Место, где история отечественной криптографии пересекается с новейшими достижениями квантовых технологий, где люди, ставшие

историей профессии, встречаются с молодыми, самыми продвинутыми ИБэшниками....

Сегодня специалисты по ИБ, получившие опыт работы в банках, трудятся в самых разных отраслях — телекомах, нефтянке, транспорте, на добыче алмазов, в энергетике и медицине, торговле и правительственных структурах, вузах и школах. Всего не перечислить. Журнал стал популярен везде, где возникают проблемы с защитой информации и где необходимо эти проблемы решать на самом высоком профессиональном уровне. И мы не заметили, как вместе со всей отраслью ИБ наше любимое издание выросло из тесных штанишек банковской тематики и вышло на широкие просторы безопасности бизнеса. Пожелаем же ему удачи!

НОВОСТИ

- 8 **Законодательство, промышленность, технологии**

ТЕМА НОМЕРА ЗАЩИТА ДАННЫХ: СОХРАНИТЬ ВСЁ!

- 10 Рустэм Хайретдинов (ГК «Гарда») «Я за персональную ответственность»
- 15 Елена Покатаева (BIS Journal) Перед прочтением... обезличить
- 27 Илья Шаленков, Анна Чеботарёва (Kerpt) Строже закона
- 30 Артём Калихов (Web3 Tech) «Исключить риск утечек можно»
- 34 Денис Суржко (ВТБ) Защитить ИИ, чтобы он защитил нас
- 36 Никита Назаров (HFLabs) «Бизнес заинтересован в решениях, обеспечивающих „умное“ обезличивание и сохраняющих смысл данных»
- 39 Сергей Вельц (Кибертоника) Искать компромисс!
- 41 Дмитрий Семёнов (ТехЛАБ) Цифровая медицина
- 44 Евгений Царёв (RTM Group) Помогут оборотные штрафы и другие меры

РЕГУЛЯТОРЫ

- 48 **Государственная Дума**
Василий Пискарев (Государственная Дума)
Чем сильнее будут на нас давить, тем жёстче будет ответная реакция

ИБ В ОТРАСЛИ

- 52 **Собеседник**
Борис Мирошников (ГК «Гарда») «ИБ – давно самостоятельная отрасль»
- 56 **Собеседник**
Андрей Ефремов (Лаборатория Касперского) «Один плюс один – намного больше, чем два»
- 60 **Ассоциация ФинТех**
Олег Моргун (Ассоциация ФинТех) Репозиторий АФТ как объединяющая сила



УГРОЗЫ И РЕШЕНИЯ

- 64 **Передача данных**
Вячеслав Половинко (АМТ-ГРУП) Междоменные решения
- 66 **Домены**
Денис Полушин (Аладдин), Евгений Паутов (ГК «Астра») Доверенная доменная инфраструктура
- 68 **Доверенная среда**
Вячеслав Савлюк (ИТ-Экспертиза), Артём Туренок (ДиалогНаука) ZTNA vs VPN: антиподы или друзья?
- 70 **Рынок ИБ**
Максим Степченков (RuSIEM) Скупой платит дважды
- 72 **Межсетевые экраны**
Дмитрий Хомутов (Ideco) Открытая перспектива
- 74 **РАМ-системы**
Филипп Ружковский, Лев Семёнов (АТК «Ямал») Переход на РАМ



ИНФРАСТРУКТУРА

- 76 Деловые мероприятия**
Дмитрий Дубынин (Минцифра)
Пять вопросов
- 82 Деловые мероприятия**
Анна Катанкина (BIS Journal)
XX Международный банковский Форум
- 85 Безопасность API**
Сергей Борисов (VK)
Топ-10 API Security Risks 2023
- 88 Продукт года**
Марина Бродская (BIS Journal)
Под названием NGFW...
- 91 ИТ + ИБ**
Олег Хныков (Positive Technologies)
О теории относительности в сети

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 96 Человеческий фактор**
Андрей Жаркевич (Антифишинг)
People As Code

НИ-НУМЕ

- 100 ChatGPT**
Павел Былевский (BIS Journal)
Угрозы ChatGPT мнимые и реальные: не сверхразум, а лживый иноагент

ЗА РУБЕЖОМ

- 104 Дайджест ИноСМИ**
Марина Бродская (BIS Journal)
Вплоть до дальнего космоса
- 108 Законодательство**
Александр Виноградов (ФГУП «ЦНИИХМ»), Сергей Меньшиков (Belarusian InfoSecurity Community), Андрей Ситнов (независимый эксперт)
ОДКБ. Республика Беларусь



СУБЪЕКТЫ

- 112 История**
Борис Столпаков
(историк криптографии)
«Кто в море не бывал...»
- 119 История**
Борис Столпаков
(историк криптографии)
Как наше слово отзовется?
- 124 Заметки безопасника**
Александр Игонин (BIS Journal)
Замки на песке

НЕ ВСЕГДА ВИНОВАТЫ ХАКЕРЫ...

Сбой в ИТ-инфраструктуре концерна Volkswagen парализовал работу ряда его подразделений (в том числе Porsche и Audi): остановилось движение конвейерных лент, пострадала корпоративная связь.

Встали заводы в Германии, а также в США и Китае. Причина сбоя всё ещё неизвестна, хотя кризисная группа, работавшая над восстановлением систем, так и не нашла признаков хакерской атаки.

Месяцем раньше аналогично остановились 14 заводов автоконцерна Toyota в Японии. Там тоже сначала винили хакеров, но реальной причиной оказалась... нехватка места на диске базы данных. Поскольку серверы работали в одной системе, сбой произошел в функции резервного копирования, переключение не удалось выполнить, что и привело к остановке заводов.

ПИРАТОВ — НА РЕЮ!

Минюст опубликовал поправки к статье УК РФ о нарушении авторских прав. Предлагается изменить порог преступлений, совершённых в крупном и особо крупном размере: с 100 тыс. рублей до 500 тыс. и с 1 млн рублей до 2 млн соответственно.

Национальная федерация музыкальной индустрии (НФМИ) выступила резко против. Она настаивает на повышении тюремных сроков для цифровых пиратов: с 2 до 3 лет при крупном ущербе и с 3 до 8 в особо крупном. Эксперты пояснили: в существующем виде статья «недоступна правообладателям для борьбы с интернет-пиратством».

Против поправок также АРПП «Отечественный софт» и Некоммерческое партнёрство поставщиков программных продуктов. Там заявили: если такие нормы будут приняты, под защитой останется только «3–5% дорогостоящего ПО».

«ТЛЕН, МРАК И БЕЗЫСХОДНОСТЬ»

На IX Федеральном форуме по ИТ и цифровым технологиям нефтегазовой отрасли РФ представители производств рассказали, что предприятия испытывают нехватку российских контроллеров Wi-Fi и ядер Private LTE для промышленной связи.

Гендиректор ООО «Сибур Коннект» Р. Абдрахманов заявил, что у проводных решений ядра сети, маршрутизации, межсетевого экранирования — «пока тлен, мрак и безысходность». Он надеется, что альтернативы появятся в ближайшие три года. По его словам, в беспроводном сегменте есть «хорошие аналоги по Wi-Fi, однако, большие проблемы с софтом», при этом в сегменте 5G, 3G и LTE «есть достойные ядра», но нет базовых станций.

М. Кулешов, ОАО «Северсталь-информ», отметил проблему с контроллерами Wi-Fi и мощным хардом для

ЦОДов, а также призвал российских вендоров «не повторять маркетинговых приколов», связанных с подпиской на лицензии. Особенно для ИБ-решений.

П. Мартынов, ООО «Газпромнефть ИТО», также заявил, что российских ядер сети «нет и пока не из чего даже пытаться выбрать».

Наконец, И. Черкасец, ООО «Протей технологии» (разработчик ядра сети Private LTE), заключил, что компания не успевает дорабатывать продукт под требования всех заказчиков из-за нехватки кадров и «наличия коммерческих обязательств».



ИДЁТ ПРИТИРКА С СИЛОВИКАМИ

Ассоциация больших данных (АБД, включает «Яндекс», VK, «Ростелеком», «МегаФон» и др.) не поддержала правительственный законопроект о контроле силовиков за базами ПДн. В АБД уверены: прямой доступ к информационным системам нарушит их целостность, а также создаст риски передачи информации третьим лицам.

Обсуждаемые поправки к федеральным законам внесли в Госдуму в начале августа. Они предусматривают то, что правоохранители получают возможность удалять и модифицировать записи, связанные с лицами из ряда категорий. В том числе посредством удалённого доступа к базам ПДн.

А это, как отмечают в АБД, может повлечь преследование лиц, ответственных за базы из-за несоответствия с другими законами, в частности, теми, которым должны следовать финорганизации и субъекты КИИ. Помимо этого, ав-

торы отзыва раскритиковали пункт, обязывающий уведомлять органы власти о появлении в БД «сведений о ведомственной принадлежности» людей.

В ассоциации заключили, что любые манипуляции с данными должны осуществляться не напрямую, а через отправку официальных запросов, «в том числе через выделенных работников операторов ПДн, имеющих допуск к гостайне».



КАБМИН ГОТОВИТ НОВУЮ СТРАТЕГИЮ

Выступая в Координационном центре правительства на сессии по развитию ИИ, глава правительства РФ М. Мишустин рассказал об обновлении Национальной стратегии в сфере инновационных технологий в соответствии с общемировыми тенденциями.

Новая Стратегия должна обеспечить рост вычислительных мощностей, запустить венчурное финансирование, снять регуляторные барьеры и укрепить международное сотрудничество. Большое внимание уделено развитию ИИ, т.к. по прогнозам к 2025 г. объем рынка ИИ превысит 1 трлн рублей.

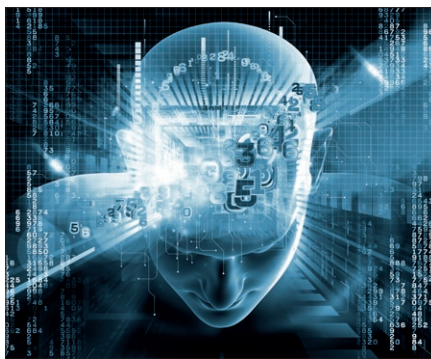
Предполагается, что реализация стратегии к 2030 году позволит:

- пяти тысячам организаций получить поддержку и льготный доступ к вычислительным мощностям для разработки ИИ;

- 95% компаний интегрируют новые технологии в свою работу благодаря господдержке;

- 85% всех субъектов экономики будут знакомы с принципами использования ИИ для решения рабочих задач.

Планируется запуск более 300 научных прикладных проектов, в том числе с международным участием. За пять лет дополнительный прирост ВВП в результате массового внедрения ИИ составит 11 трлн руб.



РОБОТЫ ПРОТИВ МОШЕННИКОВ

«Тинькофф Банк» анонсировал «Фабрику человекоподобных роботов», которые будут работать со скамерами. Звонок от мошенника перенаправляется на виртуального помощника – «Защитника Олега», который в свою очередь запускает сценарии, имитирующие разговор с реальным человеком.

В банке пояснили: чем дольше злоумышленник «висит» на линии, тем меньше потенциальных жертв он успеет обзвонить за день. Плюс роботы собирают информацию о новых мошеннических схемах.

«В рамках пилота мы делали некоторых персонажей намеренно грубоватыми для достижения реалистичного эффекта. Интересно, что в таких сценариях меняются роли, теперь добычей становятся сами мошенники», — рассказали в «Тинькофф».

24-25 октября 2023 года
"Рэдиссон Славянская"
Москва



X МЕЖДУНАРОДНЫЙ ФОРУМ
ВБА-2023
ВСЯ БАНКОВСКАЯ АВТОМАТИЗАЦИЯ

ОРГАНИЗАТОРЫ
iFIN
media
АРБ Ассоциация
Российских
Банков

СПОНСОРЫ



ПАРТНЕРЫ



24-25 октября 2023 года в Москве пройдет X Юбилейный международный форум ВБА-2023 «Вся банковская автоматизация» – <https://vbaforum.ru/>, организованный компанией «АйФин Медиа» при поддержке Ассоциации российских банков (АРБ). Форум пройдет исключительно в онлайн-формате в гостинице «Рэдиссон Славянская» (Москва, Площадь Европы, 2).

Участниками Форума ВБА-2023 стали уже более 20 компаний. Спонсорами ВБА-2023 традиционно выступают iCAM Group и Компания BSS. Партнеры Форума: ПрограмБанк, SimbirSoft, ИНВЕРСИЯ, Фродекс, РЕД СОФТ, Комита, Финансовые Информационные Системы (FIS), Лаборатория модульной автоматизации (ЛМА), Abanking. Экспоненты и участники деловой программы: Орбсофт, RapidSoft, Адваланж, RNDISOFT, iSpring, Dynamika, ВЦ Инлайн, Cybertonica, Перула, АРТ-Банк, ХотКом.

Количество мест на выставке и тайм-слотов в деловой программе ограничено.

ВБА-2023 – это главное мероприятие в России по банковской автоматизации. На Форуме более 40 ведущих разработчиков решений для финансовых организаций, поставщиков оборудования и интеграторов продемонстрируют свои новейшие продукты и услуги, а банки и финансовые компании поделятся опытом и расскажут о том, как современные инструменты автоматизации помогают эффективно решать новые задачи, увеличивать доходы, снижать издержки, привлекать новых и повышать лояльность существующих клиентов.

В деловой программе ВБА-2023 будут представлены лучшие кейсы и экспертные доклады от ведущих специалистов и руководителей из банков и ИТ-компаний.

Форум ВБА-2023 проводится для руководителей ИТ и бизнес-подразделений, топ-менеджеров, ответственных за эффективное использование современных технологий, оптимизацию бизнес-процессов, развитие финансовых услуг и обслуживание клиентов.

Делегаты от банков и финансовых организаций (страховых и инвестиционных компаний, МФО, НПФ) могут принять участие в мероприятии бесплатно.

Оргкомитет форума ВБА-2023: Тел.: +7 (495) 229-8502, E-mail: 2023@vbaforum.ru, <https://vbaforum.ru>

«Я ЗА ПЕРСОНАЛЬНУЮ ОТВЕТСТВЕННОСТЬ»

В ПРЕДДВЕРИИ КОНФЕРЕНЦИИ «ЗАЩИТА ДАННЫХ: СОХРАНИТЬ ВСЁ» НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ ОДИН ИЗ ЕЁ ОРГАНИЗАТОРОВ



Рустэм ХАЙРЕТДИНОВ
заместитель
генерального директора
ГК «Гарда»

КРИЗИС НЕДОПРОИЗВОДСТВА

— Рустэм Нилович, вы известный эксперт в области информационных технологий и кибербезопасности. В марте 2023 года вы стали заместителем генерального директора группы компаний «Гарда», где отвечаете за реализацию стратегии роста бизнеса компании, а до этого работали в крупных отечественных и западных компаниях, добились там заметных успехов. Что вам больше помогает в работе: опыт, творчество или принципиально новые стратегии и подходы?

— Начнём с того, что если я в чём-то и эксперт, то скорее в выводе технологических компаний на корпоративный рынок, но никак не в кибербезопасности. Я никогда не делал руками ничего, связанного с кибербезопасностью: не отражал атаки, не искал уязвимости, не анализировал код, не изучал логи и т.п., а последнюю компьютерную программу написал в 1990 году. Поэтому, когда меня спрашивают о технике, я обычно отвечаю, что экспертного мнения на этот счёт не имею. Что, в общем-то, не особо мешает принимать решения о запуске и позиционировании продуктов и довольно успешно их продавать.

До прихода в «Лабораторию Касперского» в 2001 году я активно занимался ИТ, работал в российском вендоре и нескольких интеграторах, у меня был свой бизнес, проданный потом АФК-системе, так что в ИБ я попал сразу на директорскую позицию.

— Значит, опыт?

— Не совсем. Я считаю, что при выводе продукта или компании на рынок прошлый успех нельзя повторить, ведь новые задачи возникают в конкретный момент в уникальных условиях: экономическая ситуация, зрелость заказчиков, конкурентное окружение, рост или стагнация конкретного рынка, бренд компании или её акционеров — всё это определяет стратегию и тактику вывода продукта или компании.

Сегодня ситуация в стране вообще и в ИТ в частности недоизученная экономистами. У нас в России сейчас кризис избыточного спроса, в то время как все известные кризисы последних столетий — кризисы недостаточного спроса, говоря словами учебников, кризисы перепроизводства. Рецепты успеха на таком рынке негде подсмотреть и не у кого скопировать, все российские игроки идут на ощупь. Так что сегодня все маркетологи, продуктологи и продавцы находятся в уникальной ситуации, во многом импровизируя.

МЫ БЫСТРО ДОГОНЯЕМ

— В линейке продуктов группы компаний «Гарда» есть несколько решений по защите корпоративных баз данных и неструктурированных данных в сети заказчика. Отметили ли вы увеличение спроса на такие продукты в связи с ростом числа утечек данных в России и по всему миру?

— Спрос последний год рос в основном на фоне ухода иностранных конкурентов. То есть те, кто пользовался иностранными решениями, замещают их на отечественные. Ёмкость этого рынка — миллиардов десять рублей, но быстро забрать их все не получится. Клиенты привыкли к определённому набору функций, а наши продукты, как и большинство российских разработок, не уступают иностранным решениям в базовых функциях, но пока проигрывают в удобстве, управляемости и интеграции с другими решениями. Мы их быстро

догоняем, но за один год все желания заказчиков исполнить не удастся.

Рынок же первичных покупок пока только формируется, компании должны достигнуть определённой зрелости своей системы ИБ, закрыть первоочередные дыры на периметре и только потом сосредоточиться на том, как используются данные внутри баз данных и приложений. Прошлый год у крупных клиентов ушёл на работу над ошибками, совершёнными в защите периметра заказчиков, поэтому хорошо продавались наши решения по защите от DDoS и сетевой безопасности, а первые покупатели защиты баз данных, у которых никогда не было решений такого класса, уже составляют значимую долю в продажах.

ПРО КОНФЕРЕНЦИЮ

– **23 октября в Москве пройдёт конференция «Защита данных: сохранить всё», где впервые планируется обсудить вопросы только защиты данных. Кто стал идейным вдохновителем мероприятия?**

– Это коллегиальное решение, можно сказать, идея витала в воздухе. В России много хороших конференций по информационной безопасности, но все они посвящены защите инфраструктуры, потому что их организаторы и спонсоры – наши уважаемые братья по оружию и одновременно конкуренты – специализируются на этом сегменте рынка. Тема защиты данных на этих конференциях проходит на круглых столах и мастер-классах, но как бы на периферии, на полях этих конференций и представлена небольшими DLP-или DCAP-вендорами. Соответственно, эти не очень массовые секции на этих конференциях, как и отдельные конференции DLP-вендоров, посвящены продвижению конкретных продуктов, что не раскрывает всей широты задачи и вариантов её решений. Поэтому, когда мы пришли с идеей такой конференции к регуляторам и игрокам рынка, все её поддержали, никто не сказал «и так полно конференций, зачем нам ещё одна».

ДАННЫЕ И ОТРАСЛЕВАЯ СПЕЦИФИКА

– **Как вы, эксперт в области ИБ, оцениваете ситуацию на рынке защиты данных? Есть ли у вас какие-то предложения и готовые решения, которые вы готовы предложить участникам для обсуждения?**

– Данные, в отличие от инфраструктуры, защищать сложнее – защита данных носит контекстный характер в зависимости от

С защитой данных в каждой отрасли есть специфика – разные бизнес-процессы, разные приложения, разные типы данных, разное отраслевое регулирование их использования

индустрии. В банке и в розничной сети инфраструктура может быть похожей, поэтому без особых изменений можно продавать антивирус, анти-DDoS или сканер уязвимостей в обе отрасли. А вот с защитой данных в каждой отрасли есть специфика – разные бизнес-процессы, разные приложения, разные типы данных, разное отраслевое регулирование их использования и т.п. Поэтому систему, успешно защищающую, скажем, данные в банке, просто так перенести на сеть розничной торговли вряд ли удастся. Очевидно, что компании, успешно защищающие цифровые инфраструктуры, не спешат заниматься защитой данных, это удел нишевых компаний, экспертиза сосредоточена именно в них.

ДЛЯ КОГО?

– **Как вы полагаете, кого больше должна заинтересовать конференция – представителей ИТ и ИБ или операторов данных из разных отраслей экономики, представителей ФОИВ и юристов?**

– Мы формируем программу конференции таким образом, чтобы участие в ней было интересным для всех упомянутых категорий участников. Защита данных – задача комплексная, она задействует многие подразделения компаний:

- ◆ ИТ-службу, обеспечивающую сбор и обработку данных в бизнес-целях;
- ◆ функциональных руководителей, которые пользуются результатами обработки этих данных;
- ◆ юристов, формализующих в конкретных регламентах требования регуляторов и собирающих доказательства для суда;
- ◆ кадровиков, которые должны доводить эти регламенты до сотрудников и требовать их выполнения;
- ◆ экономистов, которые оценивают стоимость данных и ущерб от их утечек;

♦ rg-службы, которые должны активно включаться в информирование клиентов в случае утечек данных;

♦ и конечно, специалистов в области информационной безопасности, чья работа — защищать корпоративные данные.

БЕЗОПАСНАЯ РАЗРАБОТКА — ЭТО БИЗНЕС-РЕШЕНИЕ

— Многие утечки после марта 2022 года связаны с попытками ретейлеров создать новые приложения взамен иностранных. И первое, что происходит после попытки перехода на новое решение, — массовая утечка данных клиентов компаний. Примеров масса. В связи с этим возникает вопрос, как внедрить подход Secure-by-Design в разработку ПО, связанного со сбором, обработкой и хранением персональных данных любого объёма?

— Ретейлерам можно только посочувствовать: до февраля прошлого года почти все они в своих программах лояльности пользовались облачным сервисом польского разработчика и потеряли в одночасье доступ и к функциям, и к данным. Чтобы сохранить в действии программы лояльности, все спешно занялись собственной разработкой, и приоритет тут, очевидно, отдавался скорости разработки, а не безопасности. Результаты этого мы сейчас, к сожалению, и пожинаем.

Если же говорить о безопасной разработке, то это сегодня одна из самых горячих тем, спрос на неё гораздо выше, чем могут предложить игроки российского ИТ-рынка. Собственной разработкой сегодня занимаются практически все крупные не ИТ-компании, в них работают сотни тысяч программистов, создающих десятки тысяч приложений. Поэтому не хватает не только инструментов, но и специалистов, умеющих обслуживать эти инструменты и организовывать процессы.

Безопасная разработка — довольно затратное занятие. Сами разработчики жалуются, что она в полтора раза замедляет разработку процесс создания продукта, то есть он выходит на рынок позже. Кроме того, позже выходит на рынок и на 30 % увеличивается стоимость разработки за счёт дополнительных специалистов, инструментов анализа приложения, тестов и инфраструктуры. То есть делать разработку безопасной или нет — это бизнес-решение, которое должны принимать руководители компаний, а не разработчики или безопасники.

КНУТ УДАРИТ ПО ГОРДОСТИ СТРАНЫ

— Как вы полагаете, нужны ли для реализации таких подходов законодательные нормы или требования регуляторов? Может ли отрасль ИТ саморегулироваться или в любом случае необходим кнут?

— Область ИТ в России с самого начала саморегулировалась, потому что государству просто не было до неё дела. Так что традиции саморегулирования у нас очень сильны. Сейчас маятник качнулся в другую сторону: государство вдруг активно стало участвовать в ИТ-индустрии как многочисленными льготами и другими формами поддержки, так и запретами и штрафами, даже уголовным преследованием провинившихся. Совсем без кнута, то есть ответа на вопрос «а что нам будет, если мы не подчинимся требованиям», обойтись не удастся, но налегать на это с рыночной точки зрения неправильно. Это просто остановит цифровизацию и отразится на удобстве цифровых сервисов как коммерческих, так и государственных, а сегодня такие сервисы — гордость страны, мы одни из лидеров цифровизации в мире.

— Необходимо ли, по вашему мнению, ввести некие этические нормы и правила информирования об утечках данных не только регуляторов, но и клиентов?

— Лучший регулятор этики — конкуренция. В таких высококонкурентных отраслях, как банки, телеком, розничная онлайн- и офлайн-торговля, клиент быстро голосует ногами. Я сам как пользователь очень чувствителен к отношению сервиса ко мне и быстро нахожу альтернативу.

В мало- и неконкурентных отраслях с этим сложнее: нам некуда уйти от государственных сервисов и от монополистов типа железнодорожных перевозок, энергокомпаний и агрегатора такси. Их надо, на мой взгляд, в соглашениях с пользователями заставлять брать на себя обязательство в случае утечки информации обрабатывать заранее определённый процесс информирования клиентов по заранее определённым каналам.

ЕСТЬ ОПЫТ ДРУГИХ ОТРАСЛЕЙ

— Массовых утечек данных из-за незакрытых уязвимостей в инструментах и сервисах можно избежать, если вовремя закрыть уязвимости и обновить ПО. Как бороться с нерадивостью ИТ- и ИБ-служб на местах, в конкретных организациях?

— Нерадивость — слово, которого не должно быть там, где автоматизируются важные



процессы. Чёткие, не допускающие неоднозначных толкований требования, постоянный контроль за их исполнением, чувствительные санкции за неисполнение — человечество придумало, как избежать «нерадивости» за сотни лет до изобретения ИТ. Противопожарная безопасность, требования к охране труда на производстве, обращение с опасными материалами, медицинские регламенты — люди руководствуются этой методикой много лет. Это не помогает полностью избежать инцидентов даже в таких регулируемых областях, как атомная энергетика, но делает их существенно более редкими, а ущерб от них — минимально возможным.

Надо понимать, что такие меры делают цифровизацию медленнее и дороже, но

таково требование времени. Раньше автомобили тоже продавались без встроенных средств безопасности и потому были дешевле, но количество погибших в авариях вызвало к увеличению расходов на безопасность, и сегодня купить автомобиль без подушки безопасности, антиблокировочной системы, специальных стёкол невозможно.

СИТУАЦИЯ ИЗМЕНИЛАСЬ

— **Утечки — это не только уязвимости в ПО или хакерские атаки, но и человеческий фактор. Есть ли у вас предложения, как быть с этим явлением?**

— Отрасль давно имеет лучшие практики противодействия утечкам, просто их применение должно быть осознанным и

комплексным. Недостаточно просто купить какое-то наложенное средство и думать, что проблема будет решена. Противодействие утечкам — проблема больше организационная, чем техническая: процессы сбора и обработки данных должны быть автоматизированы так, чтобы никто и никак не смог получить доступ к большому массиву данных. Все нужные технологии для этого есть: управление доступом, мониторинг и блокирование транзакций в базе данных, обезличивание данных, проверка ПО и инфраструктуры на уязвимости, защита привилегированных учётных записей, контроль трафика и операций на рабочих станциях и т.п. Их нужно бесшовно встроить в цифровые системы, наложить на это регламенты их использования и постоянно обучать пользователей.

Нынешние цифровые системы проектировались лет десять назад, во время бума цифровой трансформации бизнеса, когда эффект от внедрения «цифры» — экономия, охват, масштабирование, ускорение транзакций — был важнее защищённости этих систем. Поэтому действующие системы часто не готовы быть защищёнными архитектурно.

Новые системы строятся уже с пониманием масштабности проблем информационной безопасности, и, думаю, по мере перехода с нынешних цифровых систем на новые проблемы с массовой утечкой данных уйдут в прошлое, хотя полностью проблема не решится, как она не решилась с пожарами и инцидентами на опасном производстве.

И КРИПТОГРАФИЯ, И АРХИТЕКТУРА

— **Специалисты всё больше говорят о внедрении в ПО отечественной криптографии. Для этого создана АНО «Национальный технологический центр цифровой криптографии». Поможет ли массовое внедрение криптографических методов предотвращать массовые утечки?**

— Шифрование — одно из самых старых и эффективных средств безопасности, но оно решает только часть проблем — с хранением и передачей данных. Для обработки данные должны быть расшифрованы, поэтому дело не столько в самом шифровании, сколько в такой организации процесса обработки, при которой пользователь получает только те данные, которые ему нужны в конкретный момент, да и то максимально обезличенные. Администратор вообще не имеет доступа к расшифрованному содержимому СУБД,

аналитик получает не сырые данные, а подготовленные и обезличенные. Разработчики для тестирования ПО получают данные «испорченными», замаскированными, поскольку им нужны данные конкретного типа структуры, а не сами данные. Это дело вовсе не криптографов, а архитекторов цифровых систем.

ОБ ОБОРОТНЫХ ШТРАФАХ

— **Закон об оборотных штрафах. Нужен или нет и с какими нормами? Не получится ли, что отрасль ИБ предлагает один вариант законопроекта, а на выходе депутаты примут абсолютно другой документ, идущий вразрез с первоначальными идеями, как это уже не раз случалось?**

— Оборотные штрафы — одна из самых обсуждаемых сегодня мер регуляторов. У меня к ней противоречивое отношение. С одной стороны, требования, не подтверждённые карательными мерами за невыполнение, выполняться не будут, а нынешние штрафы в 50 тысяч рублей за утечку миллионов записей не мотивируют заниматься их защитой. С другой стороны, в экономике с большой долей государства штрафы на госпредприятия — это просто перекладывание денег из кармана в карман. Ну хорошо, оштрафуют энергетическую, скажем, компанию за утечку данных из биллинга. Денег на штраф у неё нет. Если она заплатит из текущих операций, у неё не будет денег на поддержку непрерывности подачи энергии, и государство деньги ей обязательно выделит — либо через повышение тарифов, либо просто из госбюджета. Получается, что штраф заплатим мы с вами.

А полностью частная компания после начисления такого оборотного штрафа подаст на банкротство. Пострадают и клиенты, и сотрудники — мы точно хотим этого?

На мой взгляд, персональная ответственность гораздо эффективнее. Начислить ответственному за утечку руководителю персональный штраф в несколько годовых окладов с принудительным отчислением половины в доход пострадавших от утечки — действенная мера. Или запретить человеку занимать должности, связанные с проектированием или обслуживанием цифровых систем, как это происходит, например, с аннулированием медицинских лицензий. Но при таком подходе должен быть обязательно прозрачный механизм независимых расследований инцидентов, чтобы можно было выяснить и доказать в суде халатность сотрудника, ответственного за утечку.

ПЕРЕД ПРОЧТЕНИЕМ... ОБЕЗЛИЧИТЬ

КАК ДАННЫЕ ТЕРЯЮТ ЛИЦО И КАК УПРАВЛЯТЬ ЭТИМ ПРОЦЕССОМ



Елена ПОКАТАЕВА
обозреватель
BIS Journal

Почему нынешнее состояние дел в области защиты персональных данных, несмотря на неуклонный рост угроз, напоминает разногласный бесконечный хоровод, и как данная отрасль пытается выйти на путь поступательного системного развития?

ТЕКУЩАЯ СИТУАЦИЯ

«Тёмная сторона» цифровизации не собирается сдаваться, несмотря на активные усилия структур информационной безопасности по противодействию киберкриминалу. Злоумышленники продолжают совершенствовать методы социальной инженерии,

Darknet пополняется новыми порциями похищенных персональных данных (ПД). Согласно данным аналитического отчёта «Значимые утечки данных в 2022 году», подготовленного «Лабораторией Касперского», в прошлом году в результате 168 значимых утечек было опубликовано более 2 млрд записей с пользовательскими данными. Причём в подавляющем большинстве это довольно свежие утечки: 74% данных были выгружены в 2022 г. и 16% — в 2021 г.

Лидером стал ритейл — он взял «золото» и «серебро» сразу в двух номинациях: количество фактов утечек и количество скомпрометированных пользовательских данных (рис. 1, 2).

Интересно, что лидером по объёмам похищенных данных стал сегмент доставки, который по параметру количества утечек не вошёл в первую пятёрку отраслей. Ещё интереснее ситуация с сегментом здравоохранения: четвертое место по объёмам данных при единственной зафиксированной утечке. В «Лаборатории Касперского» объясняют: 64% пользовательских данных были скомпрометированы в результате атак на крупный

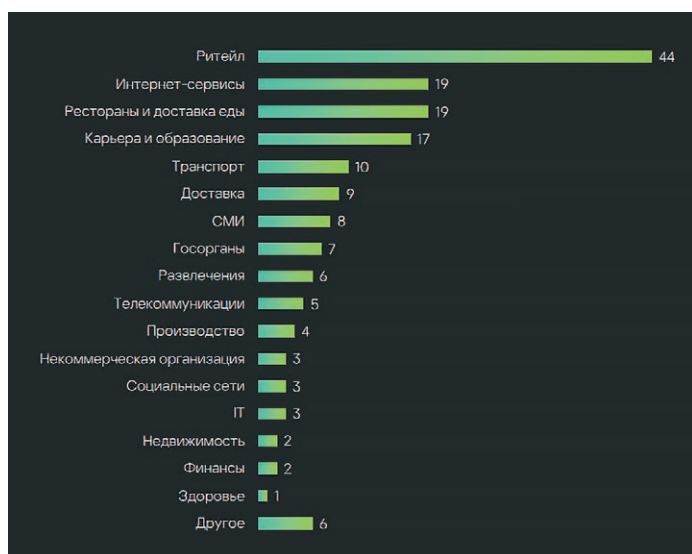


Рисунок 1. Значимые утечки данных в разных отраслях экономики РФ в 2022 г.

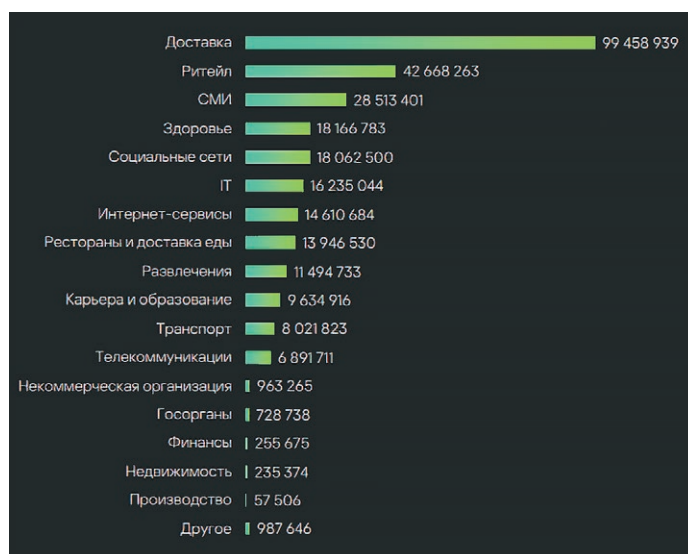


Рисунок 2. Количество данных, утёкших из компаний разных отраслей экономики РФ в 2022 г.

бизнес. В этой связи радуют гармоничные показатели финансовой сферы — она удерживает позиции в конце списка значимых утечек в обеих номинациях.

По данным компании DLBI, владеющей сервисом разведки утечек данных и мониторинга Darknet, в первом квартале нынешнего года произошла 31 крупная утечка, в результате которой в открытый доступ попало 118 млн уникальных записей, что в 2,3 раза превышает уровень аналогичного периода прошлого года. Вновь в «лидерах» — те же отрасли: двойная утечка данных бонусной программы «СберСпасибо» — 52,5 млн записей, розничная сеть «Спортмастер» — 46 млн записей, база интернет-аптеки zdravcity.ru — 8,9 млн записей. А за первую половину нынешнего года злоумышленники выложили в Darknet 188,7 млн записей. Как поясняют специалисты, это коснулось таких компаний, как «Гемотест», «Почта России», OZON, DNS.

Эти данные согласуются со сведениями Роскомнадзора — согласно официальной статистике ведомства, за полгода в Сеть попало около 177 млн записей о гражданах (76 инцидентов).

При этом растущая популярность новых ИТ-решений на базе искусственного интеллекта (ИИ) обуславливает появление новых рисков утечек персональных данных. Например, для обучения нейросетей компании стремятся собирать как можно более объёмные и детализированные датасеты, сгребая подчас всю подходящую информацию, которую можно обнаружить в открытом доступе в интернете. А на этапе дообучения нейросети нередко используют реальные обращения граждан, которые фиксируют чат-боты. Так в ML-модели могут подмешиваться данные, способные существенно обогатить знания о конкретных персонах.

И неугомонные кибермошенники уже осваивают новое поле — исследуют уязвимости нейросетей на предмет поиска «чёрного хода» (backdoor) в нейронные сети, чтобы извлечь, например, из них конфиденциальную информацию. Понятно, что назрела необходимость регулировать сбор данных для обучения моделей ИИ.

ВРЕМЯ КОМПРОМИССОВ ИЛИ СОТРУДНИЧЕСТВА?

Федеральным законом «О персональных данных» № 152-ФЗ от 27.07.2006 предусмотрен единственный способ снизить риск идентификации отдельных лиц с помощью цифровых данных информационных

систем — обезличивание персональных данных. Под обезличиванием подразумеваются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту.

Однако нынешнее состояние сферы обезличивания персональных данных демонстрирует некоторую растерянность государства и общества, обусловленную неизвестной ранее спецификой взаимоотношений общества и ИТ в части технологий обезличивания ПД.

Действительно, на уровне взаимоотношений ИТ и ИБ всё традиционно — речь идёт о достижении компромисса между аспектом больших данных (нужны большие модели) и аспектом безопасности данных (борьба с утечками и неправомерным использованием ПД граждан).

Сфера больших данных сегодня на подъёме: реализуется стратегия развития в РФ рынка больших данных, которая была разработана Ассоциацией больших данных и принята к реализации в 2019 г. Она предполагает два сценария развития — базовый и агрессивный, которые, как ожидается, обеспечат вклад технологий больших данных в ВВП России на уровне 1,2% ВВП и 1,8% ВВП соответственно к 2024 г. (рис. 3).

При этом умеренный эффект должны обеспечить три подхода:

- ◆ упрощённый доступ и обработка данных;
- ◆ R&D-песочницы для исследования больших данных;
- ◆ стратегии больших данных традиционных индустрий.

А целям агрессивного развития сектора Big Data соответствуют ещё три подхода:

- ◆ обеспечение возможности обмена/обогащения данных;
- ◆ финансирование инноваций и ресурсная экосистема;
- ◆ внутренние стимулы для инновационных отраслей.

Они более агрессивны и по эффекту от использования больших данных, и по сложности имплементации, говорят в Ассоциации больших данных (АБД). Предполагается, в частности, широкий обмен/обогащение данных. Например, рыночные игроки делятся друг с другом анонимными/обезличенными персональными данными на коммерческой основе, поощряется обмен отраслевыми данными внутри и между отраслями через саморегулируемые стандарты (например, обмен эксплуатационными данными доменных печей).

	Прогноз ВВП на 2024 г., млрд руб. ^{1 23}	Доля в 2024 г. по сравнению с 2019 г., % от ВВП ²
Торговля	14 778	1,8
Недвижимость	10 277	1,1
Горнодобывающая отрасль	8 883	1,5
Строительство	6 936	0,2
Транспорт	6 782	0,9
Прочие	6 513	1,0
Профессиональные услуги	4 906	1,6
Финансовые учреждения	4 425	1,9
Промышленные товары	3 865	1,5
Нефтехимическое производство	3 756	1,5
Сельское хозяйство	3 665	0,5
Здравоохранение	2 935	1,0
Транспортные средства и оборудование	2 891	0,3
Энергетика	2 889	1,3
Потребительские товары	2 754	1,6
Телекоммуникации и технологии	2 536	1,7
Развлечения	833	1,6
Государственный сектор	7 770	н/д
Всего	97 393	1,2

Рисунок 3. Рост вклада больших данных в ВВП России. Базовый сценарий. Источник: «Стратегия развития в РФ рынка больших данных», Ассоциация больших данных, 2019 г.

При этом государство делится определёнными типами релевантных данных с частным сектором (например, аудио или видео с камер наблюдения), а инновационные команды получают выделенный доступ к «озёрам данных» с труднодоступной отраслевой информацией, например эксплуатационным данным сетей электроснабжения.

По оценкам Анны Серебряниковой, президента АБД, которые она представила на конференции First Russian Data Forum в апреле этого года, рынок больших данных в России может вырасти к 2024 г. до 319 млрд руб. (170 млрд руб. в 2021 г.), а дополнительный эффект от использования больших данных для отраслей экономики составит при этом 1,6 трлн руб. операционной прибыли.

Однако техническое налаживание обмена данными между бизнесом и государством с достижением компромисса между сферами информационных технологий и информационной безопасности — это только один аспект происходящего. Он отражает традиционный подход к внедрению ИТ-решений:

они рождаются в сфере ИТ, а затем приходят в общество в виде готовых услуг и сервисов. Общественные процессы сводятся при этом к принятию или неприятию новых технологических предложений, а технологии регулирования выступают позади технических инноваций, обставляя запуск технического решения в эксплуатацию некоторыми ограничительными условиями.

В ситуации с обезличиванием ПД регулирование проникает на уровень непосредственно управления данными (можно сказать, на уровень Data Governance) и фактически становится участником технологических решений. Надо сказать, что эту особенность момента понимают в Роскомнадзоре. Вот как об этом сказал Милош Вагнер, заместитель руководителя Роскомнадзора, на конференции First Russian Data Forum: «Цифровая экономика рассматривает вопросы базы данных с точки зрения их максимально эффективного использования, но мы в Роскомнадзоре рассматриваем их и как актив человека. Большие данные, прежде всего, связаны с правами человека: правом на конфиденциальность

личных данных, правом на неприкосновенность частной жизни».

Эта особенность нынешнего момента заставляет по-новому взглянуть на расклад сил, традиционно действующих на поле цифровых преобразований: технические решения, регулирование, отраслевые практики информатизации. В этом смысле абсолютно прав Борис Глазков, вице-президент по стратегическим инициативам «Ростелекома», описавший современный мир как поле регуляторных экспериментов в сфере управления данными и алгоритмами. Причём это поле охватывает территорию всей планеты — везде, включая технологически развитые страны Запада и Востока, эти эксперименты ещё далеки от завершения. Как это выглядит в нашей стране?

РЕГУЛИРОВАНИЕ: ДУХ ЗАКОНА И БУКВА ПРИКАЗА

С методической точки зрения, живо развиваются направления, связанные с технологическими аспектами обработки БД и использованием методов ИИ. Так, Росстандарт предоставил доступ к стандартам в сфере ИИ, подготовленных ударными темпами Техническим комитетом по стандартизации № 164 «Искусственный интеллект» (всего 61 стандарт). Этот набор включает, в частности, ряд стандартов для анализа больших данных в области клинической медицины и телемедицины, автомобильного транспорта, навигации воздушных судов, дистанционного зондирования Земли, речевых технологий, ситуационной видеоаналитики.

Также Росстандарт утвердил ГОСТ для ИИ-систем в сельском хозяйстве, а Минсельхоз РФ уже взялся за разработку стандартов по обмену данными среди участников рынка. Минцифры создаёт стандарт персональных данных для систем и сервисов, использующих средства ИИ, включая унификацию методов обезличивания персональных данных. Александр Шойтов, замминистра цифрового развития, связи и массовых коммуникаций РФ, поясняет, что речь идёт о разработке методов унификации для искусственного интеллекта — это необходимо в первую очередь для субъектов КИИ.

Есть Кодекс этики данных, разработанный под эгидой Ассоциации больших данных, базирующийся на принципах саморегулирования в сфере обработки и использования данных, Белая книга «Свод лучших практик в сфере добросовестного использования данных» и реестр добросовестных участников

рынка данных¹. К настоящему моменту в нём, правда, зарегистрировалось всего 24 участника.

Что же касается самой методологии обезличивания персональных данных, то она вообще-то началась давно. Поправки <https://sozd.duma.gov.ru/bill/992331-7> в закон о персональных данных, регулирующие оборот обезличенной информации, были внесены на рассмотрение Госдумы правительством ещё 21 июля 2020 г. Но до сих пор они находятся на стадии второго чтения. Уже и Президент России дважды обращал внимание на пробуксовку законопроекта, а в начале этого сентября поручил правительству и Госдуме принять законопроект до конца года.

Основным документом, регулирующим использование методов обезличивания ПД в нашей стране, является приказ Роскомнадзора № 996 «Об утверждении требований и методов по обезличиванию персональных данных», утверждённый 10 лет назад — 5 сентября 2013 г. В нём определены четыре основных метода обезличивания: введение идентификаторов, изменение состава или семантики, декомпозиция и перемешивание (рис. 4, 5).

Роскомнадзор также описал основные свойства обезличенных данных:

- ◆ Полнота — сохранение всей информации о персональных данных конкретных субъектов или группах субъектов, которая имелась до обезличивания.

- ◆ Структурированность — сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания.

- ◆ Релевантность — возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме.

- ◆ Семантическая целостность — соответствие семантики атрибутов обезличенных данных семантике соответствующих атрибутов персональных данных при их обезличивании.

- ◆ Применимость — возможность обработки персональных данных с целью решения задач, стоящих перед Оператором, без предварительного деобезличивания всего объёма записей о субъектах.

- ◆ Анонимность — невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации.

¹ https://ac.gov.ru/uploads/Projects/PDF/Kodeks_etiki/reestr_v6.pdf

Метод	Принцип работы	Секретность	Проблемы реализации
Введение идентификаторов	Группа идентифицирующих атрибутов заменяется абстрактным идентификатором, группа хранится в отдельной таблице	Таблица перекрёстных ссылок	Выбор состава идентифицирующей группы Генерация идеинтификатора Обеспечение связи между таблицей и обогащёнными данными
Изменение состава или семантики	Изменяется структура (количество, положение и размер полей) или изменяется значение идентифицирующих атрибутов	Алгоритм модификации	Выбор состава идентифицирующей группы Генерация алгоритма модификации Обеспечение секретности алгоритма модификации
Декомпозиция	База данных разделяется на много частей, информация о связях хранится в отдельной таблице	Таблица связей	Выбор состава частей Генерация алгоритма связывания Обеспечение связи между частями
Перемешивание	Группа идентифицирующих атрибутов перемещается в запись другого человека	Алгоритм перемещения	Выбор состава идентифицирующей группы Генерация алгоритма перемещения Обеспечение секретности алгоритма перемещения

Рисунок 4. Методы обезличивания персональных данных, рекомендованные Роскомнадзором. Источник: Алгоритмы реализации методов обезличивания персональных данных в распределённых информационных системах. Е. Ю. Мищенко, А. Н. Соколов. Доклады ТУСУР, 2019, том 22, №1, с. 66–70.

На фоне растущих угроз утечек персональных данных после начала СВО в августе Роскомнадзор рекомендовал операторам, осуществляющим обработку ПД, ряд подходов, снижающих риск компрометации ПД. В частности, ведомство советует минимизировать перечень персональных данных, которые организация собирает и обрабатывает, а также данные из различных категорий ПД хранить отдельно. Рекомендуется также хранить идентификаторы, указывающие на человека (Ф. И. О., email, телефон, адрес) и данные о взаимодействии с ним (оказанные услуги, проданные товары, переписка, договора и т.д.) в разных, непосредственно не связанных друг с другом базах данных. Для связи этих баз можно использовать синтетические идентификаторы, которые не позволяют отнести информацию в этих базах к конкретному субъекту ПД без дополнительной информации и алгоритмов, и хранить эти специально созданные идентификаторы отдельно от предыдущих двух баз.

На этом фоне более впечатляюще выглядит деятельность Минцифры: ведомство ставит



Рисунок 5. Обезличивание персональных данных методом перемешивания. Источник: Белая книга «Свод лучших практик в сфере добросовестного использования данных», Ассоциация Больших данных, 2023 г.

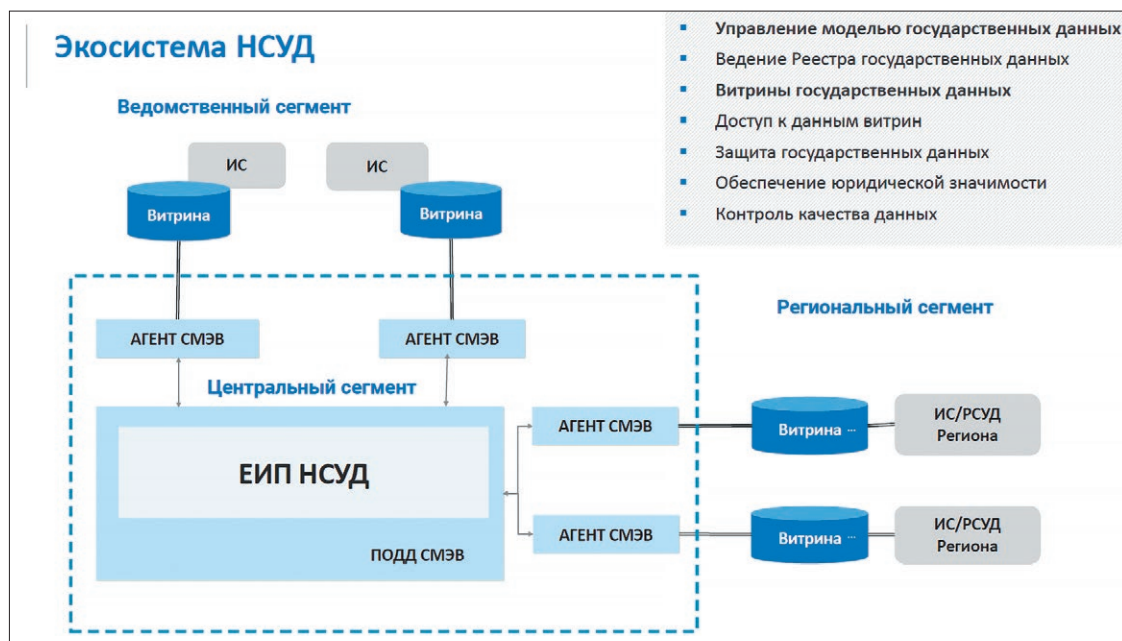


Рисунок 6. Экосистема Национальной системы управления данными (НСУД). Источник: TAdviser

задачи уровня не просто больших, а очень-очень больших данных.

КУРС НА ЦЕНТРАЛИЗАЦИЮ И ГОСКОНТРОЛЬ

Один из штрихов этой картины — перенос биометрических персональных данных в Единую биометрическую систему. Компании, получившие аккредитацию на работу с ПД, будут передавать биометрические данные клиентов в ЕБС для хранения, а оттуда получать цифровую модель данных, которую будут использовать для оказания услуг в организации.

Ещё более масштабная новация связана с практической реализацией национальной системы управления данными (НСУД), которая создаётся с целью повышения эффективности создания, сбора и использования государственных данных как для предоставления государственных и муниципальных услуг, так и в целях доступа физических и юридических лиц к информации, в том числе с использованием средств автоматизации (рис. 6).

Таким образом, государство становится крупнейшим производителем данных (обсуждается появление новой категории данных — национальные, хранящиеся в госсистемах), которыми сможет воспользоваться и бизнес. О соответствующих намерениях государства стало известно прошлой осенью. Регламент обмена данными между государством и бизнесом пока окончательно не сформирован, но известна общая архитектура — потребителю будет предоставляться

витрина так называемых санитизированных данных без технической возможности доступа к внутреннему контуру НСУД.

Понятие санитизированных данных вводится для того, чтобы из общего объёма данных, хранящихся в НСУД (на этой платформе планируется объединить данные из сотен госсистем, реестров и баз), выделить те, которые не содержат информации, относящейся к разряду банковской, налоговой тайны, тайны связи и т.д. После процедуры санитизации ими смогут пользоваться и госорганы, и бизнес (на коммерческой основе), в том числе для последующей их обработки системами искусственного интеллекта. Бизнес, в свою очередь, сможет передавать в НСУД обезличенные датасеты своих данных, которыми, в свою очередь, смогут воспользоваться другие коммерческие компании. Очевидно, что такая идея, подрывающая бизнес на данных, вызвала неприятие у крупных владельцев персональных данных клиентов (операторов сотовой связи, интернет-компаний и т.д.).

Специально для задач обезличивания данных в рамках инфраструктуры НСУД будет создан центр обезличивания. По оценкам Александра Шойтова, первый вариант этого центра должен появиться к концу текущего года, а полноценная структура будет создана в 2024 г. Нормы регулирования, соответствующие данной конфигурации механизма работы с обезличенными ПД, также находятся в состоянии разработки. Планируется, что поправки в 152-ФЗ вступят в силу 1 сентября 2024 г.

Ассоциация больших данных, представляющая интересы крупных коммерческих владельцев больших данных, намерена встроиться в происходящие процессы: она предложила Минэкономразвитию РФ установить экспериментальный правовой режим «Доверенный посредник в сфере данных». Цель — дать возможность ИТ-разработчикам и аналитикам данных протестировать механизмы безопасного использования обезличенных данных для создания своих интеллектуальных систем.

Между тем жизнь корпоративного сектора в условиях противостояния растущим угрозам продолжается. И сегодня область ИТ-решений обезличивания персональных данных — горячий рынок: в ответ на острую потребность компаний в надёжной и удобной защите персональных данных, которая к тому же отвечает требованиям российских регуляторов, исследователи и разработчики предлагают разнообразные подходы, технологии и готовые продукты обезличивания ПД.

ВПЕРЕД ПО ДОРОГЕ, ВЫМОЩЕННОЙ ОД

Разнообразие ситуаций, возникающих в реальных информационных системах заказчиков, настолько велико, что на практике успешно применяется целый спектр различных вариантов преобразования персональных данных, приводящих к тому, чтобы после обработки эти данные не могли быть привязаны к конкретному человеку. Среди них:

♦ **Анонимизация.** Идентифицирующие признаки данных заменяются на другие значения. При этом данные лишаются всех специфических идентифицирующих характеристик, таких как имена, адреса, идентификаторы, номера телефонов и др. Пример — замена имён на псевдонимы. Например, вместо конкретного имени может быть использовано заменяющее значение «Пользователь 1». Особенность этой процедуры заключается в полном исключении возможности идентификации конкретных лиц, включая невозможность обратной идентификации с помощью доступной дополнительной информации и технических средств. Иными словами, анонимизация — это предельный случай обезличивания, после которого данные становятся буквально анонимными, то есть не персональными.

♦ **Псевдонимизация.** Каждому пользователю присваивается уникальный идентификатор, который используется для обработки данных. Идентификаторы должны

быть независимыми от каких-либо персональных данных и максимально защищены от раскрытия. Используя этот идентификатор, данные можно связать с конкретным пользователем, если имеется соответствующая ключевая информация. То есть псевдонимизация повышает защиту данных, но они остаются персональными. Этот метод используется в работе с текстовыми данными, например, Ф. И. О.: программа меняет фамилию, имя и отчество, которые соответствуют другому идентификатору в системе.

♦ **Агрегирование.** Метод объединения данных из различных источников с целью исключения возможности идентификации конкретных лиц. При этом персональные данные группируются по определённым критериям, например по региону или возрастной группе. В результате нельзя однозначно сказать, какие именно данные относятся к каким лицам. Так исключается возможность однозначной идентификации конкретных лиц.

♦ **Обфускация.** Замена реальных данных на их искажённые или усечённые версии: трансформация, перемешивание, дисперсия числовых значений, модификация/сброс данных и т.д. Например, можно заменить точные значения возраста диапазонами или сократить полный почтовый адрес до города или региона. Данный метод усложняет расшифровку и идентификацию персональной информации. Часто применяется для шифрования программного кода, чтобы в дальнейшем был невозможен его анализ или кража.

♦ **Скремблирование.** Преобразование данных в случайные логические цепочки без потери общих свойств. Такой метод применяется в работе с числовыми данными. Например, после применения данной операции к номеру счёта объекту присваивается 16 цифр, последовательность которых случайна.

Дело в том, что в процессе обезличивания ПД, по сути, решаются две технических задачи. Во-первых, нужно сделать так, чтобы по обезличенным данным было невозможно достоверно установить исходные данные конкретного человека. Во-вторых, при этом необходимо сохранить смысл этих данных (семантические признаки, особенности связей между отдельными атрибутами). Только в этом случае они смогут качественно выполнять свою роль исходных данных при их аналитической обработке.

Так, полностью анонимизированные данные — это, по сути, статистические данные, которые относятся к категории открытых данных. Например, статистика Росстата или

данные социологических опросов – это полностью анонимизированные данные, но всё-таки «загрубленные», с точки зрения социально-демографических деталей опрашиваемой аудитории, и в большинстве случаев точно не пригодятся для обучения нейросетей.

Однако универсального метода, который способен на 100% обезличить данные с 100% сохранением ценности таких данных, не существует. «Реальность идентификации субъекта зависит от конкретного контекста», – подчёркивает юрист Денис Садовников в своей статье на ресурсе <https://zakon.ru>. Более того, она будет меняться с течением времени, поскольку могут появиться либо новые дополнительные сведения, либо новые технологии идентификации личности. Вот почему в каждом конкретном случае необходима оценка вероятности идентификации по обезличенным данным. Причём она должна проводиться периодически с учётом изменения контекста, круга доступной информации, развития технологий и их доступности.

Эта оценка определяется в первую очередь тем, какие усилия должны будут приложить третьи лица для идентификации человека по обезличенным данным: затраты денежных средств на такие усилия, временные и человеческие ресурсы, наличие технологии, позволяющей выполнить идентификацию без особых усилий и затрат, значимость цели идентификации и выгоды от её осуществления.

Между тем правовые нормы обезличивания должны формулироваться технологически нейтрально и по возможности максимально учитывать будущее развитие информационных технологий, подчёркивает Денис Садовников. А это развитие в части технологий обезличивания весьма активно движется вперёд.

ОБЕЗЛИЧИВАНИЕ И ПЕРСПЕКТИВЫ ШИФРОВАНИЯ

Действительно, сегодня речь идёт о задачах, связанных с передачей больших объёмов данных на обработку во внешнюю облачную модель машинного обучения и на централизованную обработку сложной аналитической системой, расположенной во внешнем контуре. В этом случае методы обезличивания, хорошо работающие на уровне внутренних баз данных, становятся неприменимы.

Гомоморфное шифрование. В последние годы во всём мире идут эксперименты с использованием математического аппарата полностью гомоморфного шифрования (Fully

Homomorphic Encryption, FHE). Причина всеобщего внимания к этому методу понятна: технологии FHE позволяют выполнять операции над зашифрованными данными, не раскрывая их, благодаря чему имеют огромный потенциал применения в решении задач хранения и обработки персональных данных.

Интересно, что понятие «гомоморфное шифрование» появилось ещё в 1978 г. и принадлежит авторам алгоритма RSA. Через год после его разработки они предположили возможность выполнения произвольных операций над зашифрованными данными без их расшифрования. Действительно, полностью гомоморфное шифрование представляет собой обобщение классического шифрования, говорят авторы статьи² из компании «Криптонит» и МГУ: «Оно позволяет не только защищать конфиденциальные данные, но и выполнять их обработку, оперируя только лишь соответствующими шифртекстами (без использования ключа расшифрования)». Это свойство FHE обуславливает широкие возможности его практического применения, в первую очередь для организации удалённых вычислений: пользователь загружает данные на удалённый сервер в зашифрованном виде, выполняет над ними вычисления, а полученный результат расшифровывает в своей локальной системе.

Стоит отметить, что математическая реализация полностью гомоморфного шифрования подразумевает гомоморфизм системы шифрования относительно операций умножения и сложения (в смысле компьютерной алгебры это две базовых операции, с помощью которых можно реализовать любой математический алгоритм). Этого удалось достичь лишь в 2009 г. сотруднику IBM Крейгу Джентри в своей диссертационной работе. Но и появившиеся ранее системы частично гомоморфного шифрования нашли своё место на рынке. Так, криптосистемы RSA и Эль-Гамала гомоморфны относительно умножения, криптосистема Пэяе гомоморфна относительно сложения. Криптосистема Бонэ – Го – Ниссим допускает преобразования с произвольным количеством сложений и только одно умножение.

В целом гомоморфное шифрование открывает настолько многообещающие возможности удалённой обработки данных без рисков компрометации обрабатываемых

² Об использовании библиотек полностью гомоморфного шифрования. А. А. Гаража, И. Ю. Герасимов, М. В. Николаев, И. В. Чижов. International Journal of Open Information Technologies, vol. 9, no. 3, 2021, с. 11–22.

персональных данных, что на рынке уже появилось немало программных библиотек гомотоморфного шифрования, в том числе с открытым кодом. В разных странах мира, в том числе и России, команды исследователей и инженеров выполняют проекты такого рода в различных прикладных областях.

♦ Медицина — возможность передавать чувствительные к раскрытию персональные данные между различными специализированными учреждениями. Хранение и обработку таких персональных данных можно осуществлять даже на базе недоверенных облачных платформ, подчёркивают специалисты «Криптонита».

♦ Финансовые организации — работа скоринговых моделей.

♦ Городское и государственное управление — агрегация и централизованная обработка персональных данных граждан или данных городской инфраструктуры (умные города) в зашифрованном виде для получения статистических отчётов не требует больших вычислительных ресурсов и может быть осуществлена с помощью современных схем гомотоморфного шифрования.

Интересен опыт создания гомотоморфной свёрточной нейронной сети³, которая работает с зашифрованными данными пользователей. Эта сеть, созданная в Сингапуре, предназначена для анализа изображений.

Однако нужно иметь в виду, что на текущий момент технологии полного гомотоморфного шифрования обладают рядом серьёзных ограничений. Например, существенные накладные расходы схемы шифрования делают гомотоморфные вычисления весьма ресурсоёмкими. А перенос «тяжёлых» вычислений типа инженерных расчётов или рендеринга видео в облако на базе соответствующей аппаратной базы, с сохранением конфиденциальности данных в виде FHE, пока не является окончательно решённой задачей, говорят эксперты.

Сокращение длины ключа и шифротекстов для оптимизации производительности системы FHE ведёт к снижению стойкости криптозащиты. Это не очень хорошее решение, особенно ввиду приближающихся угроз со стороны квантовых компьютеров.

Известно, что широко используемые на практике алгоритмы асимметричного шифрования: RSA, DSA, ECDSA и т.п. — теряют криптостойкость, то есть секретный ключ находится за полиномиальное от размера публичного ключа время⁴. Последствия от появления квантовых компьютеров для алгоритмов симметричного шифрования и хеш-функций не столь катастрофичны, но реализации алгоритмов FHE такого рода неизвестны.

Кроме того, технологию FHE невозможно использовать в многопользовательских системах, так как в этом случае агрегируемые данные зашифрованы на различных секретных ключах. Для таких ситуаций разработаны другие подходы.

Мультиключевое гомотоморфное шифрование. Технология мультиключевого гомотоморфного шифрования (Multi-Party Computation, MPC) базируется на подходе «разделения секрета» (Secret Sharing), предполагающем, что в рамках некоторой коалиции участников (где даже есть значимая вероятность компрометации одного или нескольких хранителей секрета) каждый участник получает только долю секрета, и полностью воссоздать его может только вся группа в полном составе.

Сергей Голицын, директор по анализу данных и моделированию компании Platforma, рассказывает в своём блоге на Хабре, каким образом обмен секретами заменяет обмен реальными данными, на примере двух участников: на каждом сервере строятся две аналитических модели, а в процессе обучения моделей их веса корректируются, при этом градиенты передаются между серверами. «Сами по себе модели бесполезны, потому что они обучались на «секретах». Но если взять две модели и просуммировать их веса, то в результате получается рабочая модель, которая учитывает данные обоих серверов», — рассказывает эксперт.

К числу нынешних ограничений технологии MPC также относится высокое потребление вычислительных ресурсов при построении реальных моделей. Чтобы обеспечить нормальную скорость построения модели, нужно использовать полностью связанные или свёрточные нейронные сети, которые очень требовательны к производительности «железа», говорит Сергей Голицын и уточняет: «Можно использовать логистическую регрессию, но для обработки big data также нужны очень

³ The AlexNet Moment for Homomorphic Encryption: HCNN, the First Homomorphic CNN on Encrypted Data with GPUs. Ahmad Al Badawi, Jin Chao, Jie Lin, Chan Fook Mun, Sim Jun Jie, Benjamin Hong Meng Tan, Xiao Nan, Khin Mi Mi Aung, Vijay Ramaseshan Chandrasekhar. Institute for Infocomm Research, A*STAR, Singapore. March 22, 2022.

⁴ Квантовый переход финтех, Е. Покатаева, BIS Journal № 2/2023.

мощные серверы и много времени. Также с MPC пока нельзя использовать один из самых популярных алгоритмов анализа данных — градиентный бустинг. Ведь в MPC самая долгая операция — это сравнение двух чисел, из-за чего бустинг не даёт практически никакого прироста в скорости, а даже наоборот».

Несмотря на то что теоретические корни MPC уходят в научные изыскания ещё 80-х годов прошлого века, о реальных внедрениях известно немного. Самый известный кейс связан с Facebook: компания открыла доступ к исходному коду CrypTen — MPC-фреймворку, интегрированному в популярную библиотеку машинного обучения PyTorch. Но есть и российские примеры внедрений. Так, в 2020 г. Московское правительство профинансировало создание городской MPC-системы на базе решения российского стартапа UBIC. Речь идёт о создании платформы совместных безопасных вычислений на основе агрегированных данных, которыми смогут пользоваться как государственные организации, так и частные компании.

Дифференциальная приватность. Differential Privacy (DP) — ещё один способ реализации максимально точных запросов в статистическую базу данных при одновременной минимизации возможности идентификации отдельных записей в ней.

Центральная идея метода, который изначально был предложен компанией Cynthia Dwork в 2006 г., — внесение в данные некоторого «шума» (параметр ϵ , называемый «потерей приватности», privacy loss), который позволяет обеспечить определённый уровень конфиденциальности данных отдельных лиц при снижении их точности. Собственно, само слово «дифференциальная» применительно к приватности подразумевает обеспечение баланса между приватностью и точностью данных при выкладывании в публичный доступ агрегированных данных в приватных датасетах.

Главная сложность практического применения метода DP заключается в определении того, куда именно и сколько шума нужно добавлять, рассказывают эксперты компании «Домклик» в своём блоге на Хабре. Один из самых популярных механизмов зашумления — механизм Лапласа.

Это очень интересный подход, поскольку он предполагает, что абсолютно любая информация является идентифицирующей, а значит, не нужно выполнять сложную работу по определению всех идентифицирующих

атрибутов в наборе данных. И ещё он устойчив к атакам с использованием вспомогательной информации, не допуская установления взаимосвязей с целью восстановления анонимизированных данных. К тому же возможны реализации DP с использованием как доверенного, так и недоверенного хранилища исходных данных.

Основные недостатки подхода лежат в сфере обеспечения необходимой точности данных, которые предназначены для использования внешними аналитиками. Для улучшения этого параметра метод DP можно комбинировать с другими методами. Например, в варианте с перемешивателем (shuffling model) каждый источник вначале добавляет небольшое количество шума в свои данные, а затем отправляет их перемешивателю, который добавляет ещё шума перед отправкой в хранилище данных.

Эксперты считают перспективным сочетание дифференциальной приватности с полностью гомоморфным шифрованием или мультиключевым шифрованием. Считается, что технология DP находится в фазе активного исследования. Практические внедрения связаны с решениями крупнейших глобальных вендоров: Apple, Google Rappor, Microsoft PINQ. Ими же созданы открытые библиотеки механизмов дифференциальной приватности: IBM/differential-privacy-library (Python), Google/differential-privacy (C++), Brubinstein/diffpriv (язык R).

КАК СТРОИТЬ РЕГУЛИРОВАНИЕ ОБЕЗЛИЧИВАНИЯ В МЕНЯЮЩЕЙСЯ СРЕДЕ?

Как обеспечить технологическую нейтральность регулирования оборота обезличенных данных в условиях, когда технологическая среда представляет собой поле активных экспериментов с внедрением инновационных подходов в реальные проекты? Простого ответа на этот вопрос нет, ведь государство впервые столкнулось с такой специфической задачей, где в слове «нормотворчество» столь велико значение творческой составляющей.

Методы управления обезличиванием ПД в существенной мере зависят от специфики предметной области, в которой работает та или иная компания. Эти отраслевые особенности определяют, в частности, специфике бизнес-процессов, в которые включены персональные данные: в госуправлении они принципиально иные, чем в здравоохранении, где медицинский персонал разного уровня в течение всего рабочего дня получает

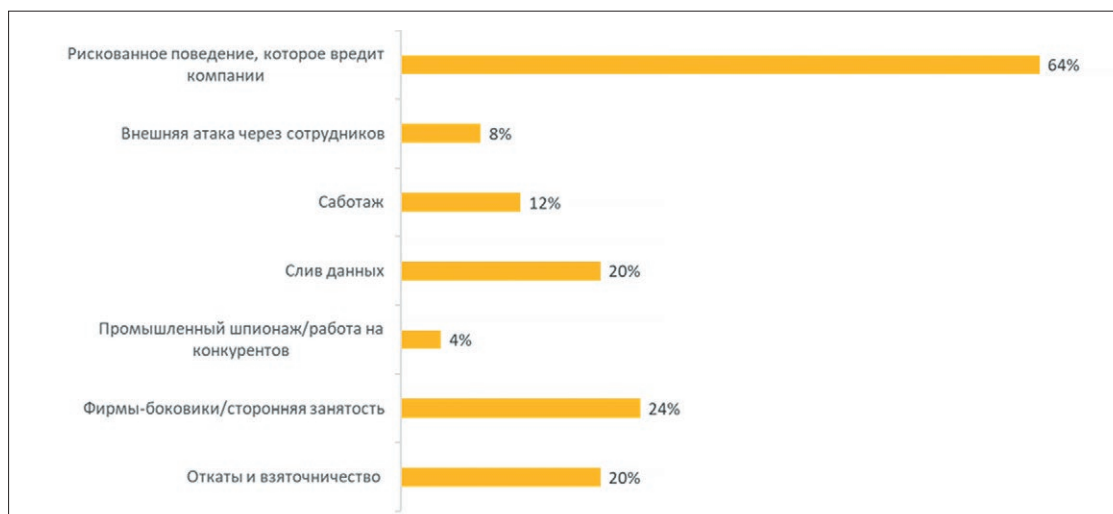


Рисунок 7. Какие инциденты по вине сотрудников происходили в компании в 2022 г.

Источник: «СёрчИнформ», исследование утечек из медицинских организаций РФ, март 2023 г.

доступ к ПД пациентов, обрабатывает их и передаёт друг другу, а также внешним организациям. К этим условиям даже стандартные средства управления доступом к данным плохо применимы. Как рассказывают эксперты в области медицинской информатизации, создание сложной, разветвлённой модели прав доступа сегодня практически невыполнимо для медицинской организации, на практике обычно выбирают очень простую модель прав доступа и думают, как перейти от предоставления прав доступа к учёту реального доступа с регистрацией всех фактов просмотра сотрудниками медицинских записей конкретных пациентов.

Применяемые методы обезличивания должны коррелировать с реальным ущербом, который могут понести частные лица и организации в результате утечек персональных данных. Здесь также наблюдается интересная ситуация. Так, согласно данным исследования утечек данных из медицинских организаций России, которое выполнила компания «СёрчИнформ», в 2022 г. с проблемами такого рода столкнулась каждая пятая клиника страны. Причём чаще всего утекали персональные данные (45%) и информация о клиентах и сделках (64%) — рис. 7.

Однако компания DLBI в ходе мониторинга Darknet обнаруживает считанные единицы баз данных медицинского профиля, выставленных на продажу. Это не ходовой товар, поясняют эксперты, так как на этих данных трудно построить прибыльную мошенническую схему. Медики подтверждают: для нас не так страшны утечки медицинских данных, сколько отсутствие последних в нужном месте или невнимательное отношение к ним.

В общем-то, стремление упростить регламенты информационной безопасности свойственно компаниям любой отрасли. Другое дело, что во многих оно дополняется дефицитом квалифицированных специалистов в ИТ и ИБ. А грамотный подход к обезличиванию данных в конкретной компании требует сегодня ещё и специфической юридической подготовки. Для подавляющего числа компаний и предприятий понятия «обезличивание» и «анонимизация» являются синонимами, а это очень грубая ошибка. Более того, тут не поможет даже знание европейской практики GDPR, несмотря на методическую общность европейского и отечественного правового регулирования.

В европейских юрисдикциях понятие «обезличивание» вообще не используется, рассказывает Денис Садовников. Для обозначения данных, отделяемых от идентификаторов субъекта, приняты категории «анонимизация» и «псевдонимизация». Российскому понятию обезличивания соответствует европейская псевдонимизация. А их анонимизация не имеет прямого аналога в отечественном законодательстве. Именно анонимность данных является там динамичной категорией и определяется каждый раз в конкретном случае с учётом контекста, характера данных, целей обработки, доступных технологий и ресурсов, потенциальных рисков и т.д. Но во многих случаях даже анонимизированные наборы данных представляют остаточные риски для субъектов.

Впрочем, в европейском законодательстве есть полезный элемент, который обеспечивает возможность настройки норм регулирования на специфику динамично

меняющейся технологической и цифровой среды. Постулируется факт того, что технологии анонимизации и обратной идентификации составляют область интенсивных исследований и быстрого развития технологий, в связи с чем невозможно дать набор точных сценариев или конкретных мер, которые гарантированно обеспечат осуществление анонимизации. Поэтому каждый случай должен рассматриваться индивидуально с учётом контекста, а конкретные используемые методы подлежат оценке.

Гибкие критерии оценки и соответствующие балансирующие тесты — это важная черта правового регулирования защиты данных в европейских юрисдикциях. Ключевым элементом данной системы, обеспечивающим её функционирование, являются сильные и независимые надзорные органы, отмечает Денис Садовников.

А ещё отрасли отличаются потребностями в наиболее актуальных средствах информатизации. Если для госструктур это сбор и агрегирование больших объёмов разнотипных данных, которые должны быть обезличены для последующей разнообразной аналитической обработки, включая drill down до уровня исходных данных, доступных отдельным категориям пользователей, то для медицинских работников сегодняшний день — это обработка информации с большой долей чувствительных персональных данных на удалённых площадках.

Например, в Москве в рамках Центра диагностики и телемедицины департамента здравоохранения Москвы функционирует единый радиологический информационный сервис (ЕРИС). Он объединяет рабочие места рентгенолаборантов, врачей-рентгенологов, включает единый архив диагностических изображений и сервис удалённых консультаций. По оценкам Анастасии Раковой, заммэра Москвы по вопросам социального развития, по состоянию на август в составе ЕРИС работало более 50 сервисов искусственного интеллекта по 23 клиническим направлениям, с их помощью медики проанализировали около 10,5 млн медицинских изображений.

Постоянно растёт количество разнообразных медицинских гаджетов, которые

используют люди. Порождаемые ими огромные объёмы цифровых данных, которые скапливаются в разнообразных цифровых хранилищах, должны стать основой для множества умных и полезных медицинских сервисов, предлагаемых населению. Задача применения продвинутых технологий обезличенной обработки персональных данных в здравоохранении, в частности, гомоморфного шифрования — архиактуальная, по оценкам медицинских информатизаторов. Но есть проблема — нет возможности вести соответствующие проекты в правовом русле.

Выступая весной на конференции «Цифровая медицина 23», ректор Высшей школы организации и управления здравоохранением Гузель Улумбекова отметила, что отрасли ещё предстоит создать эффективную систему управления информацией в здравоохранении, включающую сбор достоверных первичных данных, их систематизацию и открытость источников информации обезличенных данных для анализа.

Пример со здравоохранением показывает, что выработать эффективную систему обезличивания персональных данных можно только с активным участием отраслевых специалистов. По сути, регулятор в области персональных данных должен занять активную позицию, подобную той, на которой стоит Минпромторг РФ: он собирает разработчиков компьютерного «железа» и ПО вместе с заказчиками для того, чтобы они в условиях тесных рабочих контактов определяли, какие ИТ-системы необходимо разработать и вывести на рынок, чтобы они наилучшим образом закрывали потребности компаний из различных отраслей экономики.

Несомненно, нужно использовать энергию российских разработчиков, которые активно создают собственные технологические решения для обезличивания данных, потенциал спроса на эти решения и высокий интеллектуальный уровень отечественных специалистов, который поможет организовать систему тестирования различных решений, структуру оценок эффективности в зависимости от реальной среды применения и соответствующие критерии.

BIS Journal благодарит российских специалистов, поделившихся с редакцией своим опытом применения различных технологий обезличивания персональных данных в конкретных проектах и выделивших важные элементы этих процессов.

СТРОЖЕ ЗАКОНА

ДОЛЖЕН БЫТЬ ПОДХОД БАНКА К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ



Илья ШАЛЕНКОВ
партнёр, руководитель
группы по оказанию
услуг в области
кибербезопасности Kept



Анна ЧЕБОТАРЁВА
старший консультант
группы по оказанию
услуг в области
кибербезопасности Kept

Банки сегодня не только финансовые организации, но и экосистемы с широким спектром дополнительных услуг: от голосовых помощников до продажи сим-карт и туристических сервисов. Для оказания такого разнообразия услуг финансовые организации обрабатывают большое количество ПДн клиентов, агрегируют информацию, собранную из разных источников и делают на её основе выводы, иногда очень критичные для клиентов. Но что может быть сложного в обработке ПДн, когда есть чёткие требования законодательства? Почему бы их «просто» не исполнять? Давайте разбираться.

ПЕРВАЯ СЛОЖНОСТЬ

Трактовка термина «персональные данные», которая разнится у представителей Роскомнадзора и бизнеса.

Например, Роскомнадзор считает номер мобильного телефона номером конечного устройства, на основании которого нельзя идентифицировать субъекта, и поэтому не относит его к персональным данным. Также согласно определению Верховного Суда РФ от 21.07.2023 № 305-ЭС23-12160, номер телефона и адрес электронной почты также не являются персональными данными. Поэтому некоторые компании используют в качестве идентификатора номер мобильного телефона и позволяют себе не рассматривать его как персональные данные, закрывая глаза на дополнительную информацию о субъекте, обрабатываемую наравне с номером телефона (например, транзакции, сессии подключения и т.п.). Согласно всё той же позиции Роскомнадзора, если речь идёт о базе данных,

которая включает номер мобильного телефона и дополнительные сведения о субъекте, то такая информация будет подпадать под определение персональных данных, поскольку позволяет идентифицировать субъекта и, следовательно, её обработка должна соответствовать требованиям 152-ФЗ.

Отсутствие единого подхода в отрасли к пониманию того, что есть персональные данные, может привести к нарушению прав субъектов персональных данных и требований законодательства. При формировании критериев отнесения данных к персональным мы рекомендуем учитывать риски для субъектов и потенциальный ущерб для компании в процессах обработки их данных.

В этом вам могут помочь ответы на следующие вопросы.

◆ Какое влияние на субъекта оказывает обработка его данных: изменение материальных условий субъекта, его психологического состояния, окружения? «Неперсональные» данные не оказывают воздействие на субъекта при их обработке.

◆ Что будет с субъектом в случае нарушения целостности, доступности и конфиденциальности обрабатываемых данных? Попробуйте смоделировать условия, при которых субъект не получает своевременный доступ к данным / данные субъекта частично или полностью разрушаются / данные доступны злоумышленнику. «Неперсональные» данные не оказывают воздействие на субъекта при нарушении их безопасности.

◆ Может ли сама компания по всем обрабатываемым данным определить конкретного субъекта? При ответе важно обратить внимание на полный объём обрабатываемых компанией данных о конкретном человеке:

помните, что в обработке участвуют и ваш департамент, и коллеги из соседнего, а также не забудьте про веб-сайты и приложения. Если ответ «да», то это персональные данные.

♦ К каким сторонним ресурсам с дополнительной информацией о субъекте у компании есть доступ? Помимо ресурсов компании, для обработки могут привлекаться данные, полученные от третьих лиц и источников, например, из социальных сетей, мессенджеров, агрегаторов данных. В совокупности или по отдельности такие данные также могут быть персональными, поэтому следует проверить их на выполнение трёх вышеприведённых условий.

ВТОРАЯ СЛОЖНОСТЬ

(Не)объединение баз персональных данных.

Согласно ч. 3 ст. 5 152-ФЗ, запрещено объединение баз персональных данных, которые обрабатываются в несовместимых между собой целях. Тут может возникнуть ряд вопросов.

♦ Какие цели можно считать несовместимыми между собой?

♦ Являются ли несовместимыми цели обработки персональных данных одного субъекта, но для разных услуг, сервисов?

♦ А что подразумевается под совместимостью?

♦ Что надо учитывать при объединении персональных данных?

Рассмотрим в качестве примера ситуацию с принятием решения о выдаче кредита с двух точек зрения: со стороны банка и со стороны субъекта. Для принятия решения банк обрабатывает большие объёмы данных о потенциальном клиенте: от кредитной истории до профилей в социальных сетях. Банку необходимо удостовериться в платёжеспособности клиента, для чего банк зачастую анализирует данные, полученные не напрямую от субъекта, а порой даже и без уведомления самого субъекта об этом.

Рассмотрим ту же ситуацию со стороны субъекта. Потенциальный клиент может не знать, что банк проводит подобный анализ, не знает об используемых источниках, алгоритмах принятия решений.

В этом случае мы сталкиваемся с ещё одной сложностью: каждый оператор (банк) может трактовать норму закона по-своему с учётом задач и целей бизнеса, которые могут быть несовместимы с позицией субъекта ПДн и не учитывать его права. А в законе отсутствуют критерии для определения совместимых целей обработки ПДн.

При определении критериев несовместимости целей стоит учитывать:

♦ Направленность обработки — такая обработка нужна субъекту для получения услуги или бизнесу для продажи услуги?

♦ Риски для субъекта — что будет в случае объединения баз?

♦ Риски для бизнеса — что будет в случае нарушения безопасности данных объединённой базы?

Если по результатам вашего анализа вы пришли к выводу, что цели обработки персональных данных между собой несовместимы, следует разделить персональные данные по базам и продумать потоки данных между подразделениями компании, а также между компанией и третьими лицами с учётом этого разделения.

ТРЕТЬЯ СЛОЖНОСТЬ

Обезличивание персональных данных.

Возможным выходом из ситуации с запретом на объединение баз данных с несовместимыми целями могла бы стать обработка обезличенных персональных данных. В Приказе Роскомнадзора № 996 представлены методы по обезличиванию данных. Также согласно позиции Роскомнадзора обезличивать персональные данные могут только муниципальные и государственные органы. Но на дне открытых дверей Роскомнадзора 27 июля 2023 года была высказана позиция¹, согласно которой коммерческая организация может применять методику, если персональные данные обрабатываются с целью проведения статистических исследований или других исследовательских мероприятий.

Стоит отметить, что приведённые в методике методы «обезличивания персональных данных» не исключают «обратимость» этой операции (то есть, по сути, это «псевдоанонимизация»). Поэтому практическое применение методики не поможет решить ситуацию, так как данные и после выполненных действий будут оставаться персональными.

Аналогичные вопросы ранее уже поднимались. Например, Минцифры предлагал актуализировать и пересмотреть методику по обезличиванию персональных данных. Также Президент поручил принять изменения в Федеральный закон «О персональных данных» (проект № 992331-7), включающие уменьшение количества согласий в письменной форме путём дачи согласия на

¹ Тезисы выступлений представителей РКН <https://assets.kept.ru/upload/pdf/2023/09/ru-roskom-nadzor-open-day-overview-27072023.pdf>



несколько целей обработки персональных данных. Однако принятие новых законов и внедрение правок в существующие нормы — процесс небыстрый, а бизнес нацелен на оказание услуг, разработку новых сервисов здесь и сейчас.

Учитывая вышесказанное, рекомендуем использовать алгоритмы обезличивания, которые исключают неправомерную повторную идентификацию личности субъектов, устраняют связь между субъектом и данными, не теряя при этом ценность данных для статистических, исследовательских, исторических или архивных целей обработки.

В качестве вывода: финансовым организациям зачастую приходится искать баланс между соблюдением закона и построением эффективных бизнес-процессов. Использование следующих принципов поможет выйти на путь такого баланса:

1. Не собираем всё подряд: минимизация собираемых данных с чётким

пониманием бизнес-необходимости их обработки.

2. Не храним в одной корзине: разделение персональных данных по базам.

3. Не всегда обрабатываем персональные данные: обезличивание / уничтожение персональных данных на определённых этапах жизненного цикла обработки с учётом бизнес-необходимости.

4. Не раскрываем никому: шифрование данных, к которым может получить доступ злоумышленник (внешний периметр, внутренний периметр в случае не доверенной среды).

5. Держим всё под контролем: формирование системы управления персональными данными с чётким и формализованным подходом к обработке и защите, доступным и понятным пользователям данных и самим субъектам.

Поэтому рекомендуем не ограничиваться текущей позицией регулятора и требованиями закона: подходы к обработке и защите персональных данных в компании должны играть на опережение.

«ИСКЛЮЧИТЬ РИСК УТЕЧЕК МОЖНО»



ПРИМЕРЫ — ГОСУСЛУГИ, ДЭГ И ЦПРР ФНС РОССИИ



Артём КАЛИХОВ
генеральный директор,
Web3 Tech

Передача персональных данных (ПД) во внешние информационные системы используется во многих отраслях экономики. В первую очередь стоит упомянуть федеральные проекты, где ключевую позицию занимает сервис Госуслуг. Трудовая, экономическая, социальная, медицинская и другие сферы охватываются здесь в режиме одного окна. Но за единым интерфейсом скрывается множество различных процессов, связанных с передачей данных граждан. Как показывает практика, основной риск здесь представляет не уязвимость систем, а недостаточная осведомлённость граждан — конечных пользователей — в вопросах информационной безопасности. Поэтому каких-либо массовых прецедентов, связанных с неправомерным использованием данных, мы тут не наблюдали.

Вопрос передачи ПД во внешние информационные системы становится менее острым в силу того, что информационные системы, по крайней мере те, что работают с персональными данными, становятся всё более масштабными, всеохватывающими. Современные технологии, в том числе блокчейн и криптография, позволяют создавать информационные системы федерального масштаба, безопасность которых можно обеспечить уже на архитектурном уровне, за счёт тщательной настройки прав доступа и внутренней логики. В таких условиях теряет актуальность само понятие «внешняя информационная система»: нет передачи данных — нет рисков.

ПОДХОДЫ К ОБЕЗЛИЧИВАНИЮ ПД

Правила обращения с ПД в России предписаны сразу несколькими законодательными актами. Помимо профильного 152-ФЗ «О персональных данных», действуют 98-ФЗ «О коммерческой тайне» и 395-ФЗ «О банковской тайне». Кроме того, процессы могут регулироваться внутренними требованиями компании, например службой ИБ.

Обезличивание персональных данных можно осуществлять различными способами, но на практике чаще других применяются следующие.

- В Единый день голосования в 2020-2023 гг. избиратели из ряда регионов России использовали федеральную блокчейн-систему дистанционного электронного голосования, разработанную Ростелекомом совместно с Web3 Tech по заказу ЦИК. В дистанционном голосовании 2023 г. проголосовало около 1,4 млн. избирателей из 25 субъектов РФ.

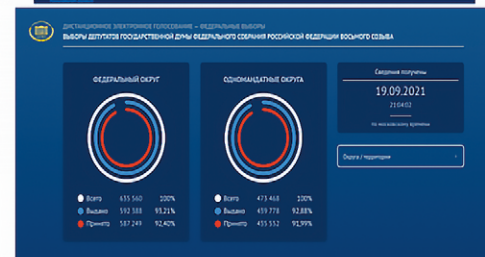
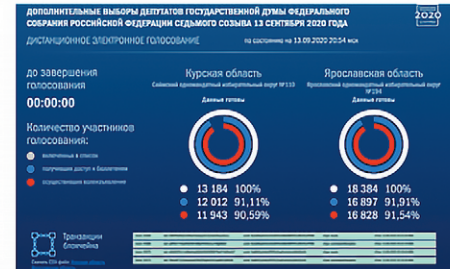
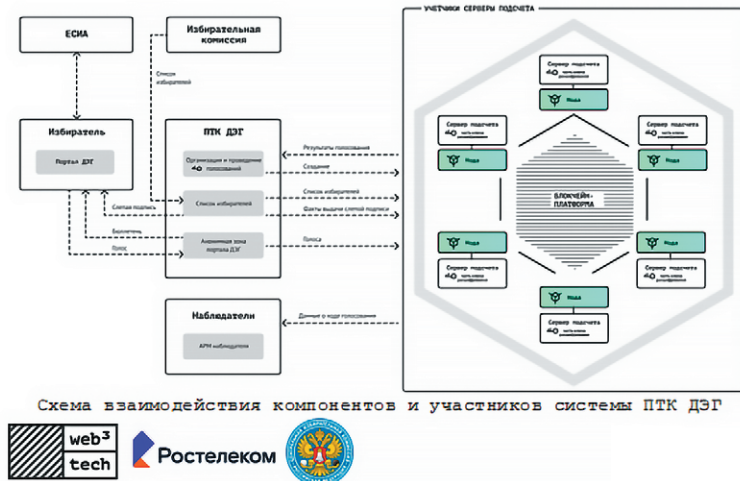


Рисунок 1. Федеральная блокчейн-система ДЭГ

♦ Использование идентификаторов — предполагает замену данных условными обозначениями. С этой целью оформляют таблицу идентификаторов, которую применяют в дальнейшем для расшифровки.

♦ Замена семантики — заключается в изменении либо обобщении информации, не несущей практической пользы для компании. Как вариант, её могут заменить статистическими сведениями.

♦ Декомпозиция — большой объём данных разделяют на отдельные части таким способом, чтобы каждый блок по отдельности не имел практической ценности.

♦ Перемешивание сведений — подразумевает такой вариант перестановки информации, чтобы полученный результат не позволял её идентифицировать.

Существует ряд технических решений, которые позволяют обезличить персональные данные с применением технологии искусственного интеллекта. Большое количество коммерческих ИТ-компаний и банков предоставляют инструменты подобного рода. Большой популярностью пользуется технология гомоморфного шифрования, которая позволяет передавать зашифрованные данные для их последующей обработки непосредственно в зашифрованном виде.

КРУПНЫЕ ПРОЕКТЫ С ОБЕЗЛИЧИВАНИЕМ ПД

Один из масштабных проектов, связанных с персональными данными, — федеральная система дистанционного электронного голосования (ДЭГ), которую наша компания совместно с ПАО «Ростелеком» разрабатывает по заказу ЦИК РФ. И в этом году голосование в регионах России уже в четвёртый раз проводилось на основе технологий блокчейна и криптографии. Система разработана таким образом, что участие в дистанционном голосовании не может создать никаких дополнительных рисков утечки данных. Как это реализовано?

После авторизации на портале Госуслуг избиратель перенаправляется в анонимную зону голосования, где идентификация осуществляется по открытому ключу. Установить связь между конкретным пользователем и его открытым ключом не может ни одна сторона, даже Web3 Tech — разработчик системы, полностью обеспечивающий реализацию блокчейн-инфраструктуры. При этом в анонимном контуре каждый идентификатор связан с собственным ключом и слепой подписью — эти механизмы обеспечивают невозможность подтасовки результатов голосования без деанонимизации избирателя (рис. 1). Это также необходимая мера.

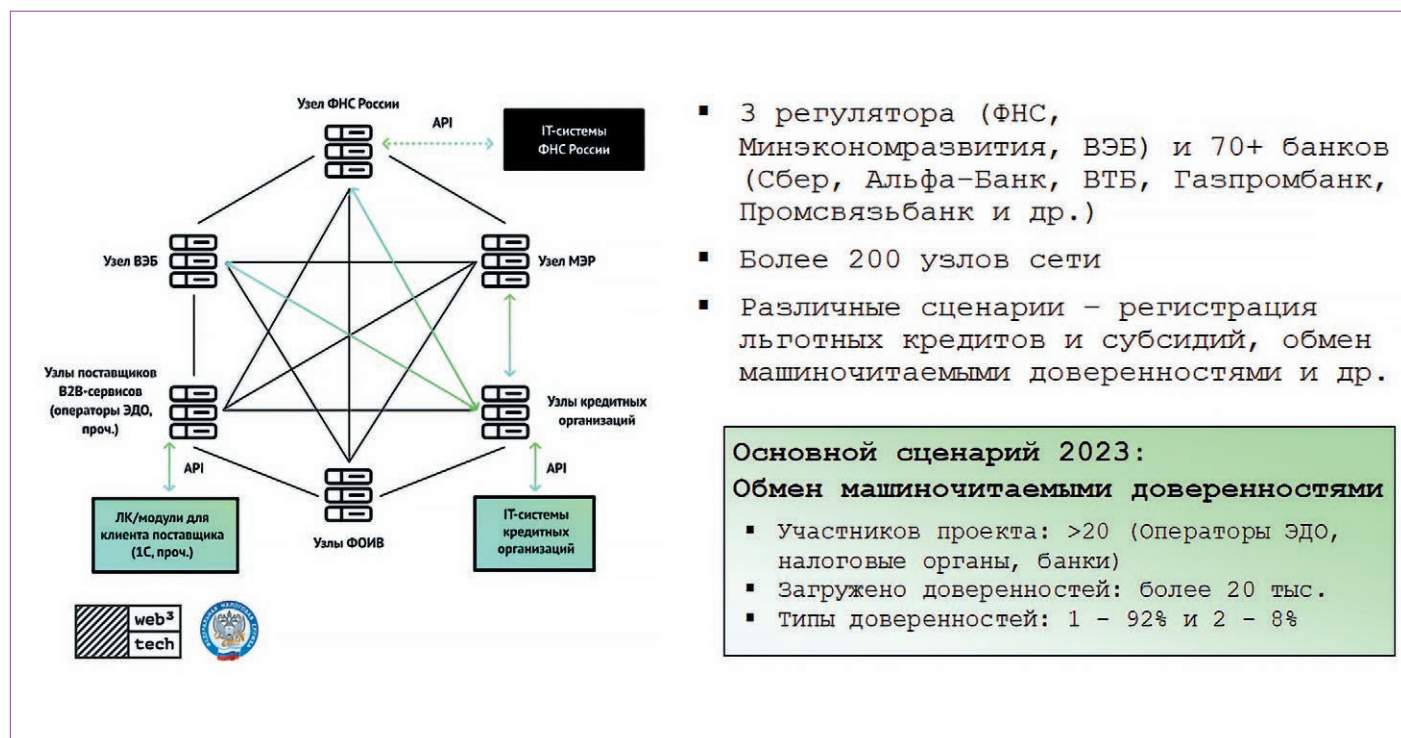


Рисунок 2. ЦПРР ФНС: крупнейшая госкорпоративная блокчейн-сеть РФ

Также мы развиваем вектор работы с персональными данными и в рамках другого проекта – цифровой платформы распределённого реестра (ЦПРР) ФНС России. В настоящее время на этой платформе запущен проект кредитных досье – единой базы документации налогоплательщиков, предоставляемой участникам платформы, операторам ЭДО и кредитным организациям.

Персональные данные входят здесь в закрытую часть профилей налогоплательщика и могут быть предоставлены организациям только по его согласию – в виде электронного разрешения, подписанного УКЭП (усиленной квалифицированной электронной подписью). Сами эти данные передаются через приватное хранилище по защищённому каналу напрямую между налогоплательщиком и организацией, которой он согласился предоставить эти данные (рис. 2).

ГОМОМОРФНОЕ ШИФРОВАНИЕ

Технология гомоморфного шифрования – важная часть наших проектов, как вышеупомянутой федеральной системы электронного голосования, так и сервиса для блокчейн-голосований WE.Vote. Здесь гомоморфное шифрование позволяет подсчитывать голоса прямо в зашифрованном виде, то есть полностью обеспечить тайну голосования. А расшифровке подвергаются уже готовые результаты.

Сам по себе термин «гомоморфное шифрование» означает, что с зашифрованным текстом мы можем проводить определённые математические действия, результат которых будет точно соответствовать результату тех же действий, проведённых на открытых данных. Гомоморфность – одно из свойств криптографических систем, в том числе криптосистемы Эль-Гамала на эллиптических кривых, которая применяется у нас. Она же, кстати, используется и в актуальном в РФ криптографическом стандарте цифровой электронной подписи ГОСТ 34.10–2018.

Федеральное электронное голосование проходит в течение строго ограниченного периода времени, по истечении которого приём голосов сразу прекращается. С этого момента и до получения зашифрованных итогов все операции с голосами осуществляются в зашифрованном виде.

Сначала с помощью технологии Zero-knowledge Proof (доказательства с нулевым разглашением) все бюллетени проверяются на корректность заполнения. Это необходимо для защиты бюллетеня от компрометации с помощью изменения бюллетеня и отправки невалидных данных. Технически это очень сложная схема, но и она благодаря доказательствам с нулевым разглашением не сможет повлиять на ход голосования.

Затем с помощью гомоморфного шифрования происходит сложение всех бюллетеней, в

результате чего получается зашифрованная сумма всех голосов. Для расшифровки суммы голосов используется закрытый ключ голосования — исключительно с его помощью можно расшифровать результаты, зашифрованные парным ему открытым ключом.

Кроме того, в процессе подготовки к голосованию закрытый ключ разделяют и каждую часть передают на хранение ответственным лицам — представителям политических партий и общественных движений — на отдельных носителях. После голосования этот ключ вновь собирают, чтобы расшифровать итоги электронного голосования.

Работа с голосами в зашифрованном виде предоставляет ещё одно важное преимущество — возможность сторонним наблюдателям отслеживать весь процесс подсчёта. Начиная с выборов 2021 г. на основе открытого исходного кода мы предлагаем специальный инструмент, который со стороны может проверить ход обработки зашифрованных голосов и убедиться в отсутствии фальсификаций на этом этапе. Этот инструмент, доступный на разных платформах, был успешно протестирован независимыми наблюдателями; отчёты можно легко найти в Сети.

Аналогичным образом технологии гомоморфного шифрования реализованы и в нашем сервисе WE.Vote — готовом решении для электронных голосований и опросов разного уровня. При выполнении всех требований к безопасности и тайне голосования WE.Vote способен реализовать не только стандартные голосования со сложением голосов, но и более сложные схемы: весовые голосования, мажоритарные, с решающим голосом. Такая гибкость делает сервис подходящим для множества сценариев. Например, с его помощью ряд ведущих вузов России проводит голосования по присуждению учёных степеней, поскольку регламент работы WE.Vote полностью соответствует всем требованиям ВАК (Высшей аттестационной комиссии) в этой сфере.

ОГРАНИЧЕНИЯ В ПРИМЕНЕНИИ

Основные ограничения в применении гомоморфного шифрования связаны с высокими требованиями к вычислительной инфраструктуре, так как операции над зашифрованными данными требуют больше ресурсов, чем аналогичные операции над незашифрованными данными. Поэтому гомоморфное шифрование едва ли подходит для сценариев, где нужно обеспечить обработку в реальном времени или высокую пропускную

способность. Это ограничение учтено, кстати, и в проекте федерального ДЭГ: гомоморфное шифрование вступает в дело строго после получения и проверки зашифрованных бюллетеней на валидность.

Таким образом, можно сказать, что не существует каких-либо данных, которые не поддаются гомоморфному шифрованию в принципе, но на практике всегда нужно учитывать, сможет ли ваша инфраструктура таким образом обработать все необходимые данные за нужное время. Без нагрузочного тестирования здесь не обойтись.

Стоит отметить, что в составе конкретной криптографической системы гомоморфное шифрование может работать в ограниченном режиме, то есть поддерживать не все, а только некоторые операции с зашифрованным текстом, например сложение или умножение. Это приводит к ряду ограничений в реальных проектах.

Ещё одна важная особенность гомоморфного шифрования — недостаточная стандартизация этой сферы. С 2017 г. этим занимается консорциум в составе нескольких крупнейших западных ИТ-компаний, и актуальная версия опубликованного ими стандарта датируется аж 2018 годом... Недостаток стандартизации приводит к отсутствию универсальных подходов и инструментов в этой сфере, но одновременно с этим открывает возможности для энтузиастов.

В целом для того, чтобы работа по обезличиванию передаваемых данных давала отличный результат, необходима уверенность в безопасности канала передачи данных, а значит, должны использоваться специальные инструменты для обеспечения безопасности, такие как использование протокола TLS при передаче. Подобные решения существуют как в программном, так и в аппаратном исполнении.

Также при передаче зашифрованных данных необходимо учитывать, что их объём в большинстве случаев будет больше, чем объём незашифрованных данных. А для обработки данных в зашифрованном виде с применением технологии гомоморфного шифрования потребуются гораздо большие вычислительные мощности и специальное программное обеспечение, требующее оптимизации под конкретные вычислительные задачи.

ЗАЩИТИТЬ ИИ, ЧТОБЫ ОН ЗАЩИТИЛ НАС

ОТВЕТ НА ВЫЗОВЫ — КРИПТОАНКЛАВ



Денис СУРЖКО
начальник управления
перспективных
алгоритмов машинного
обучения банка ВТБ

Технологии искусственного интеллекта (ИИ), получившие стремительное развитие в последние годы, в ряде отраслей кардинально меняют подходы к ведению бизнеса. Например, в продажах они способствуют появлению новых более эффективных методов анализа поведения клиента и его потребностей, а следовательно, возможности своевременного предложения ему релевантных продуктов и услуг. В том числе в формате уникального предложения.

Однако не стоит забывать о вкладе ИИ в развитие технологий обеспечения безопасности. Причём как физической, так и информационной: интеллектуальные камеры с трекингом по лицам и возможностью распознавания опасного поведения, а также различные системы, направленные на выявление мошеннических действий с последующей автоматической блокировкой счетов и невозможностью списания денежных средств.

Таким образом, де-факто технологии ИИ уже обеспечивают нашу безопасность, помогают предотвращать и раскрывать преступления. Ключевым препятствием для их повсеместного внедрения являются опасения относительно приватности данных, что справедливо порождает этические и регуляторные ограничения. Например, камера видеонаблюдения может помочь найти злоумышленника, но одновременно может знать маршрут ваших передвижений в те моменты, когда вы совершенно этого не хотите.

В этой связи на первое место по важности выходит безопасность данных, находящихся в

информационных системах. И если безопасно хранить и передавать данные в рамках одной организации — это вполне посильная задача, то их вывод вовне — вопрос совершенно иного уровня сложности.

ЗАЧЕМ ОБМЕНИВАТЬСЯ ДАННЫМИ?

Если принять во внимание гипотезу, что большинство крупных розничных компаний уже затратили 20% усилий для получения 80% результата от анализа собственных данных, а также то, что ключевую роль в развитии технологий ИИ играет объём доступных для исследователей выборок данных, то можно прийти к логическому выводу, что наиболее перспективным направлением в области анализа данных являются партнёрства, в рамках которых будет происходить обмен данными.

Именно наличие больших объёмов данных, требуемых для обучения ML-моделей, способствует развитию современной индустрии машинного обучения и появлению высокоэффективных ИИ-систем. В том числе тех, которые обеспечивают нашу информационную и физическую безопасность. Таким образом, обеспечение безопасности данных становится первостепенной задачей для всех участвующих в процессе сторон.

Для большинства компаний всё это стало весьма непростой задачей. Обычно для каждого источника данных требуется обучение специализированных моделей Deep Learning либо проработка нетривиальных подходов к обезличиванию данных, а это связано с организацией наукоёмкого и трудоёмкого процесса на стороне каждого партнёра по обмену данными.

КАК БЕЗОПАСНО ОБМЕНИВАТЬСЯ ДАННЫМИ?

Для того чтобы снять вышеуказанные препятствия, необходима синергия технологий ИИ и информационной безопасности. Одним из решений может стать создание криптоанклавов — некоторой криптозащищённой области, в которую партнёры передают данные для хранения и анализа. При этом доступа к

Что такое криптоанклав?

Партнеры передают данные в криптозащищенную область, получая гарантии



- Отсутствие доступа у других участников анкклава к их данным
- Применение строго регламентированных алгоритмов для анализа их данных
- Возможности получения «на выходе» из анкклава исключительно результатов применения моделей на данных участников анкклава без доступа к исходной информации.



Рисунок 1. Криптоанклав — криптозащищённая область, в которую партнёры передают данные для хранения и анализа. При этом доступ к данным партнёры не имеют, а анализ данных осуществляет ИИ

данным не имеет никто из партнёров, а их анализ осуществляет программный робот, реализованный внутри анкклава — ИИ. Только он может обрабатывать имеющиеся данные и строить модели. На выходе доступны только результаты применения модели на данных участников, но не сами данные (рис. 1).

Современный уровень развития ИИ позволяет полностью автоматизировать процесс построения, внедрения и проверки качества моделей и при этом снять любые этические и регуляторные ограничения. У ИИ нет сознания в человеческом понимании. Он не склонен к мошенничеству и злему умыслу. И ему можно доверить любые данные. Более того, он умеет контролировать качество данных в рамках этого слепого обучения и может стать тем инструментом, который повышает уровень безопасности без нарушения приватности. Единственное, его самого необходимо защитить от взломов и внешних воздействий. Для этого мы предусмотрели механизмы защиты анкклава как на физическом уровне, так и с точки зрения информационной безопасности — от прямых и косвенных утечек.

Стоит отметить, что объединение данных происходит на низком уровне таким образом, чтобы алгоритмы машинного обучения

и искусственного интеллекта могли использовать их максимально эффективно.

Кроме того, в современных реалиях важным аспектом предлагаемого нами подхода является его импортонезависимость. Решение разработано нами совместно с МФТИ и может быть сертифицировано. У нас нет ограничений на использование оборудования, а область его применения шире, чем у аналогичных западных решений, — от анализа рисков и CRM-моделирования до информационной безопасности. В настоящее время мы работаем над созданием программно-аппаратного комплекса (ПАК), обеспечивающего защиту на программном и физическом уровнях и предполагающего возможность масштабирования.

На наш взгляд, криптоанклав — это адекватный технологический ответ на вызовы современности, в которой, с одной стороны, нужно всё больше данных для развития ИИ; с другой стороны, необходимо соблюсти все этические и нормативные ограничения. Особенно когда речь заходит об объединении данных коммерческих и государственных информационных систем.

«БИЗНЕС ЗАИНТЕРЕСОВАН В РЕШЕНИЯХ, ОБЕСПЕЧИВАЮЩИХ „УМНОЕ“ ОБЕЗЛИЧИВАНИЕ И СОХРАНЯЮЩИХ СМЫСЛ ДАННЫХ»



Никита НАЗАРОВ
технический директор
ИТ-компании HFLabs

Начну с законодательного аспекта. С точки зрения государства, обезличивание должно соответствовать Методическим рекомендациям по применению приказа Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных». В этом документе приведены официальные способы обезличивания (маскирования) данных. Всего их четыре: декомпозиция, перемешивание данных, введение идентификаторов и изменение семантики.

У каждого из этих методов есть свои плюсы и минусы, но главная проблема заключается в том, что они далеко не в полной мере отвечают запросам бизнеса. Дело в том, что все эти методы обеспечивают безопасность персональных данных внутри контура организации. А у бизнеса, помимо этого, есть и другой интерес — он хочет знать о своих клиентах как можно больше. Особенно это актуально для крупных компаний, которые работают в высококонкурентной среде.

ПРАКТИЧЕСКИЕ ПОДХОДЫ К ОБЕЗЛИЧИВАНИЮ ДАННЫХ ПРИ ПЕРЕДАЧЕ В ДРУГИЕ ОРГАНИЗАЦИИ

Решить эту задачу можно, например, с помощью обмена обезличенными клиентскими данными между компаниями, которые входят в одну группу. Например, при обмене данными между банком и телеком-оператором можно найти общих клиентов и предложить им кобрендинговые продукты. Или

проанализировать, какое количество клиентов банка уже пользуется услугами телеком-оператора, и решить, стоит ли запускать для них особую программу лояльности.

На рынке уже есть примеры пересечения клиентских баз компаний с помощью технологий обезличивания данных. Например, в прошлом году совместно с Platforma, разработчиком решений для бизнеса на основе больших данных, мы впервые протестировали процесс безопасного мэтчинга данных двух крупных игроков.

Как это происходило? Каждый из участников проекта с помощью модуля специального ПО обезличивал имеющиеся у него клиентские данные, а затем передавал их в федеративный хаб (рис. 1). Третья сторона — в данном проекте это Platforma — предоставила так называемую чистую комнату, где происходило пересечение данных и формирование межотраслевого суперпрофиля клиента. Так мы понимали, что клиент компании 1 с идентификатором 01 и клиент компании 2 с идентификатором 02 — это один и тот же человек. Таким образом, в этом проекте предусмотрен обмен только обезличенными данными — для статистических и аналитических целей.

Для обезличивания данных в этом проекте использовался математический аппарат хеширования — алгоритм, в соответствии с которым производится замена слова или какого-то подмножества на строку из определённых символов. Алгоритм является необратимым, так как к хешированной строке добавляется соль — определённое число случайных символов.

Несмотря на то что хеширование пока не включено в официальный перечень способов обезличивания, интерес к нему неуклонно растёт. И регулятор, и игроки рынка активно ищут пути обеспечить бизнесу безопасный обмен данными. В этом направлении работает, например, Ассоциация больших данных, которая создала специальную песочницу для проведения экспериментов по пересечению данных от разных поставщиков.



Рисунок 1. Каждый из участников проекта с помощью модуля специального ПО обезличивал имеющиеся у него клиентские данные, а затем передавал их в федеративный хаб

Кроме того, примерно год назад Минцифры заявило о запуске системы Госдата.хаб. Этот проект призван объединить потоки обезличенных данных госорганов. Предполагается, что впоследствии государство будет мотивировать бизнес также предоставлять в Госдата.хаб обезличенные данные и потенциально получать за их передачу вознаграждение. Правда, встают вопросы о том, кто будет обезличивать эти данные и гарантировать, что датасеты не выдуманы, а также обеспечить безопасность реальных данных.

Ещё одна инициатива по обмену данными исходит от Банка России. Этот регулятор уже представил концепцию открытых данных на базе открытых API. Однако пока в ней речь идёт не о персональных данных как таковых, а об информации, связанной с оказанием финансовых услуг и направленной на повышение их доступности. Если коротко, то цель создания открытого API — упростить гражданам взаимодействие с банками, создать единое окно для оказания всем банковских услуг (модель Open Finance). В будущем логичным продолжением этой инициативы может стать и обмен обезличенными данными граждан (развитие до модели Open Data).

ОБЕЗЛИЧИВАНИЕ ДАННЫХ ДЛЯ ВНУТРЕННЕЙ ОБРАБОТКИ

Если обмен обезличенными данными с другими организациями — это вопрос будущего

для многих компаний, то их использование во внутренних процессах — дело сегодняшнего дня. И в этой сфере уже есть зрелые решения и примеры успешного использования.

Данные являются сердцем почти любой автоматизированной системы, которая стоит в контуре организации, работающей с физическими и юридическими лицами. Чтобы протестировать систему, работающую с данными клиентов, необходимо наполнить её информацией так, чтобы, с одной стороны, процесс тестирования был выполнен корректно, а с другой стороны, тестовые среды не пришлось защищать так же серьёзно, как и те, где фигурируют реальные данные граждан.

Это известная проблема. Исторически она решалась, например, путём обрезки данных (использование лишь части из всего массива) или генерацией синтетических данных. Но в первом случае риск утечек всё равно остаётся, а во втором возникают вопросы к качеству данных. Иногда использовался тот самый алгоритм перемешивания из приказа Роскомнадзора. Но его сложно назвать панацеей, так как этот метод лишает данные смысла: например, паспорта становятся недействительными, а регионы проживания не соответствуют номерам телефонов клиентов.

Бизнес заинтересован в решениях, которые обеспечивают умное обезличивание и сохраняют смысл данных, например,

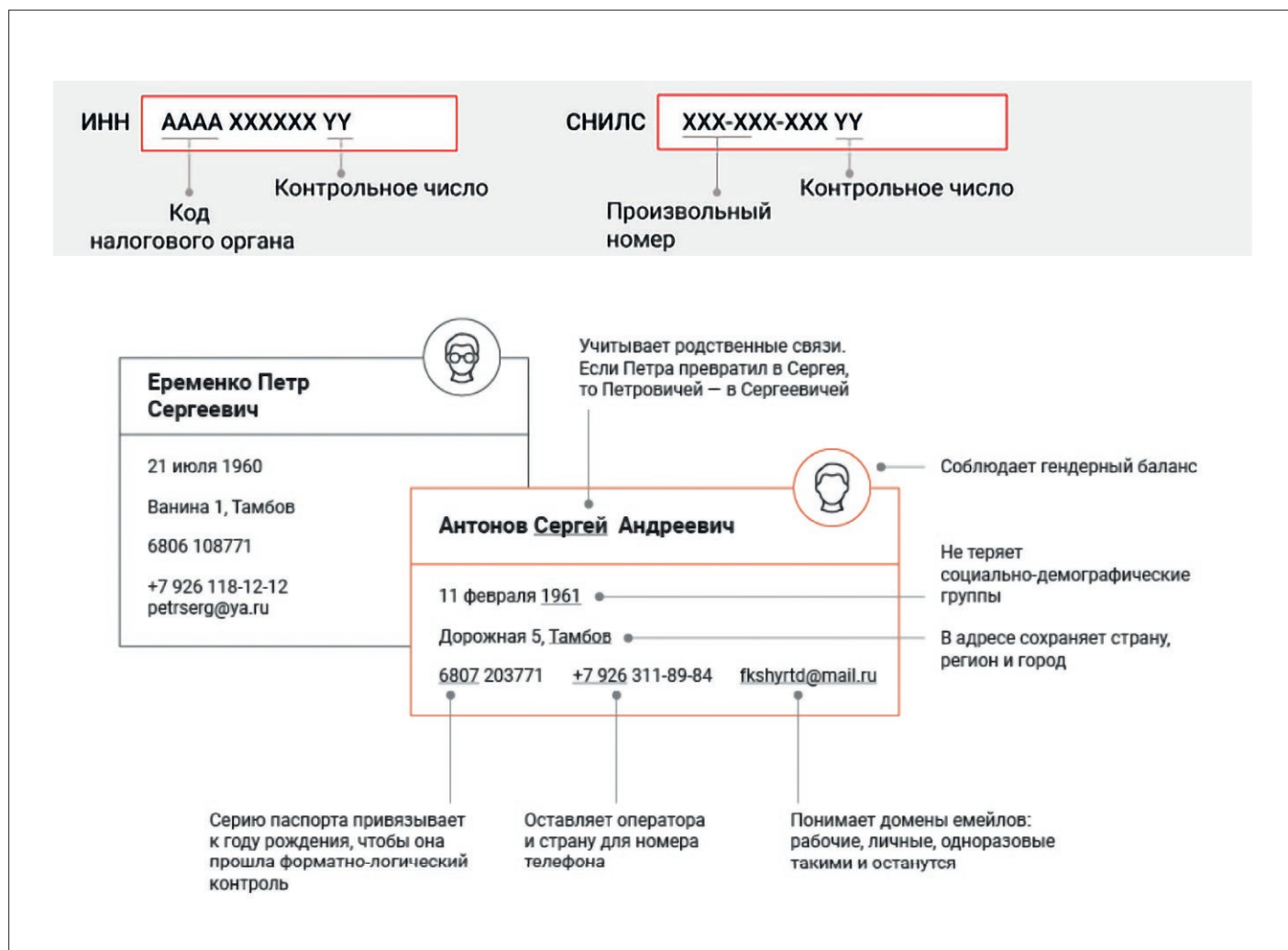


Рисунок 2. Чтобы после замены предыдущих цифр ИНН и СНИЛС сохранили валидность, «Маскировщик» пересчитывает контрольное число

заменяют имена, исходя из их популярности и пола, сохраняют валидность паспортов и родственные связи между людьми. В перспективе умное маскирование данных позволит безопасно настраивать модели машинного обучения.

Сегодня на рынке представлены решения по обезличиванию данных такого рода, например, «Маскировщик» (HFLabs), «Сфера» (Т1), «Гарда Маскирование» («Гарда Технологии»). Так, «Маскировщик» впервые был опробован в банке «Открытие», где требовалось замаскировать данные клиентов из определённого сегмента: 1 млн записей был обработан за три минуты. База клиентов в результате обезличивания сохранила консистентность и семантические особенности.

Достичь этого мы смогли за счёт использования большого набора справочников — они помогают сохранить семантику, качество и полноту данных. Например, «Маскировщик» оперирует справочниками фамилий, имён

и отчеств с указанием пола и популярности, справочником операторов по Россвязи, телефонными кодами стран и т.д. Также наше решение различает типы данных и понимает их структуру — ИНН, СНИЛС, номера паспортов, телефонов, имейлы и др. «Маскировщик» разбирается, какие данные и в каком порядке идут в строке. Он понимает, какие цифры в номере и серии паспорта или в номере телефона можно менять на случайные, а какие — подбирать по справочникам. Он способен рассчитать новую дату рождения с учётом сроков замены паспорта — чтобы подменённый документ остался действительным.

Ещё пример: структура ИНН и СНИЛС включает контрольные числа. Эти данные зависят от предыдущих цифр в строке, их вычисляют по специальному алгоритму. Чтобы после замены предыдущих цифр ИНН и СНИЛС сохранили валидность, «Маскировщик» пересчитывает контрольное число (рис. 2).

ИСКАТЬ КОМПРОМИСС!

И ЭТО НЕИЗБЕЖНО



Сергей ВЕЛЬЦ
технический директор
и сооснователь
ООО «Кибертоника»

Проблемы утечек персональных данных особенно остро стоят в банках, ведь инциденты, связанные с утечками, сильно вредят репутации банков и создают реальные риски для клиентов. Поэтому во всех местах, где в банке есть чувствительные данные, которые обрабатываются или передаются, вопросы защиты и обезличивания весьма актуальны. Причём надо понимать, что некоторые бизнес-процессы традиционно сложно реализовать на базе обезличенных данных, например, из области AML/ПодФТ, антифрода, кредитного скоринга.

Иногда приходится слышать суждение о том, что отличным подспорьем в данном вопросе может стать реализация концепции открытых данных на базе открытых API, разработанная Банком России. Утверждается, что подход Open API даёт возможность построить реальную безбарьерную среду для оборота данных и дело, как говорится, за малым. Не соглашусь с этими утверждениями. В теории, может быть, безбарьерная среда достижима и в долгосрочной перспективе мы к этому придём, но на практике до этого пока очень далеко. В качестве примера можно привести опыт внедрения открытых данных / OpenAPI (это немного разные вещи) в Европе. Там это уже несколько лет работает, но пользовательский опыт (UX) оставляет желать лучшего, пользователям неудобно этим пользоваться. И этот фактор — одна из причин того, что популярность сервисов растёт медленно.

С нашей точки зрения, открытые данные — это про удобство, повышение конкуренции и демополизацию, но никак не про безопасность. Поэтому нужны новые подходы, которые могли бы дополнить модель открытых данных или помочь рынку, работая параллельно с ней. Что это за подходы?

На этот вопрос можно отвечать долго. Дело в том, что общепринятых стандартов нет, но активно развиваются разнообразные академические и прикладные исследования, а также прототипы технологий. Есть забавная обобщающая аббревиатура PET (Privacy Enhancing Technologies), которая объединяет такие подходы, как федеративное машинное обучение, дифференциальная приватность, технологии на базе блокчейна, MPC и многие другие. Исследовательских работ много, но как всё это выглядит с точки зрения практической реализации?

ПРАГМАТИЧЕСКИЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ПРИВАТНОСТИ

Мы за прагматичный подход — пользователей нужно защищать уже сейчас и при этом учитывать реалии российской технологической и регуляторной среды. Поэтому мы занимаемся решениями на базе криптопротоколов и распределённых вычислений. Также на рынке есть любопытные и успешные пилоты на базе MPC.

Но для начала нужно зафиксировать, что понимается под конфиденциальностью. На практическом уровне это означает, что:

1. Никто, кроме запрашивающего данные, не может однозначно идентифицировать субъекта.
2. Участники системы не видят, кто делает запросы.

Чтобы реализовать эти свойства, мы разработали криптопротокол, состоящий из двух частей. Сначала участники обмена данными осуществляют процедуру Private Membership Test, с помощью которой выясняется, у кого из участников есть интересующие данные, причём без раскрытия идентификатора записи (например, номера телефона). Затем между нужными участниками проводится процедура Oblivious Transfer: данные передаются, но отвечающая сторона точно не знает, какие данные были переданы.

Отдельно отметим, что обе процедуры нужно реализовать не только безопасно, но и с высокой производительностью, чтобы обслуживать объёмы запросов крупных банков. Для этого пришлось подумать над структурами данных и реализовать протокол поверх эллиптических кривых.

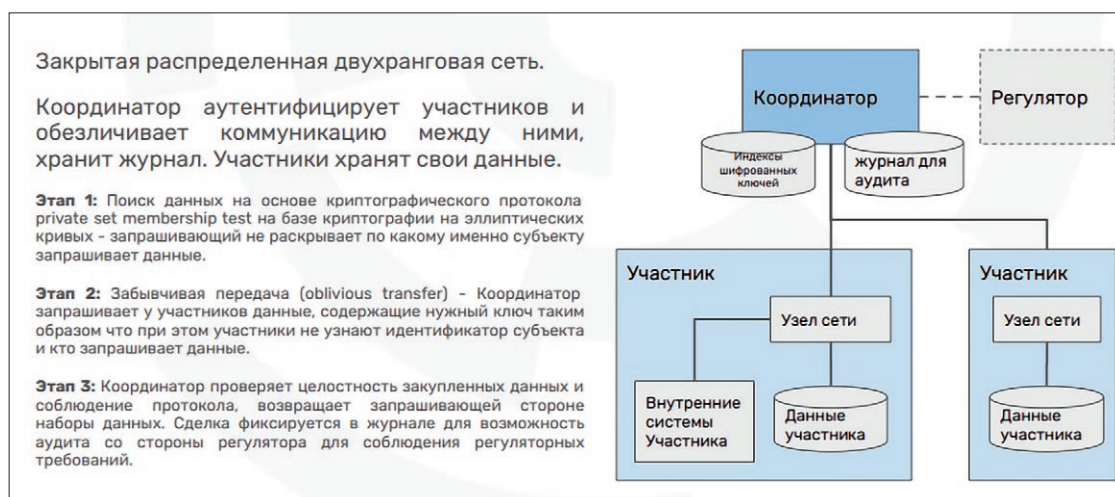


Рисунок 1. Схема решения КРАБ — Криптографическая Распределенная База

В результате мы вывели на рынок решение КРАБ (криптографическая распределённая база), которое поддерживает распределённое хранение данных на основе криптопротокола и распределённую идентификацию (рис. 1).

Гарантии безопасности решения КРАБ обеспечиваются следующим образом:

1. Децентрализация. Каждый участник хранит и контролирует собственные данные. Координатор ведёт учёт, но данные не хранит.
2. Обезличенность. Участники сети, за исключением запрашивающего, не могут однозначно идентифицировать субъекта, по которому запрашивается информация. Это предотвращает кражу лидов.
3. Анонимность. Участники сети не знают, кто с кем обменивался информацией и кому принадлежат полученные записи.
4. Журналирование. Координатор записывает факты сделок, что обеспечивает возможность проводить аудит, и контролирует участников на предмет недобросовестного поведения (перебор, синтетические данные и др.).

Каждый узел распределённой базы представляет собой независимую виртуальную машину, стоящую у участника обмена данными. Вместе с доступностью сети на уровне не менее 99,9% у координатора это обеспечивает надёжность сети.

КРАБ В БАНКЕ

В мировом финтехе стремительно набирают популярность сервисы класса BNPL (Buy Now Pay Later — «Купи сейчас, заплати потом»), которые помогают разбить стоимость покупки на равные части и выплачивать в течение одного-двух месяцев. Эксперты говорят, что к 2030 г. в русле развития e-commerce

BNPL-сервисы станут общепринятым способом оплаты, а мировой объём рынка достигнет 4 трлн долл.

На российском рынке BNPL-сервисы пока являются новинкой. Пожалуй, ключевым драйвером их развития является «Тинькофф Банк». Он использует для безопасной обработки данных клиентов решение КРАБ. Мы помогаем коллегам обмениваться данными, чтобы лучше считать платёжную нагрузку и осуществлять риск-скоринг, включая защиту от мошенников. В результате потеря оказывается меньше, конечные клиенты получают лучшие условия — это ситуация win-win.

В настоящее время «Кибертоника» и «Тинькофф Банк» прорабатывают новые кейсы в области антифрода, машинного обучения, которые выйдут на уровень промышленного внедрения в 2024 г.

В целом, говоря об обезличивании клиентских данных и борьбе с их утечками, стоит выделить два ключевых тезиса:

1. Криптография — это, конечно, хорошо, но это только часть комплекса мер по информационной безопасности. Только весь комплекс в целом обеспечивает защищённость ИТ-решений.
2. Обезличить данные так, чтобы гарантированно в любом случае нельзя было определить субъекта и при этом иметь возможность решать полезные прикладные задачи, крайне сложно. Может быть, даже невозможно. Приходится искать компромисс. И это неизбежно, ведь на практике, помимо обезличивания, обычно приходится соблюдать такие важные требования, как возможность аудита работы системы, выполнение запросов от субъектов или регулятора.



ЦИФРОВАЯ МЕДИЦИНА

«САМА ПО СЕБЕ ОБРАБОТКА ДАННЫХ И ИХ ПЕРЕДАЧА НЕ СОЗДАЮТ РИСКИ. РИСКИ СОЗДАЁТ ЧЕЛОВЕК, КОТОРЫЙ ИМЕЕТ К НИМ ДОСТУП»



Дмитрий СЕМЁНОВ
директор проектов
ИТ-компании «ТехЛАБ»

Цифровизация экономики уже несколько лет остаётся приоритетной темой государственного развития. В авангарде сфера здравоохранения и медицины: телемедицинские технологии, дистанционный мониторинг состояния пациента, системы поддержки врачебных решений, применение ИИ – эти и другие направления

органично вписались в российскую действительность. Правда, этот факт не облегчает решение сложных регуляторных аспектов, касающихся дальнейшего развития цифровой медицины. Один из таких по-настоящему болезненных вопросов – обработка персональных и обезличенных данных пациентов. Исходя из опыта работы компании «ТехЛАБ», которая занимается разработкой сервисов цифрового здравоохранения, выделим три важных аспекта.

1. ЕЖЕДНЕВНАЯ РАБОТА С ПДН — ОБЯЗАТЕЛЬНАЯ ЧАСТЬ ЦИФРОВИЗАЦИИ МЕДИЦИНЫ

Все государственные больницы и поликлиники, а также частные медорганизации ежедневно обрабатывают огромный объём

информации о пациенте. Сбор сведений для медицинских систем и сервисов, используемых врачами, их обработка, передача и аналитика происходят на самых разных этапах взаимодействия медицинских специалистов и тех, кто получает медпомощь. Например, даже процесс записи пациента на приём к врачу или госпитализацию сопровождается обработкой его персональных данных, которая жёстко регламентирована в законодательстве РФ.

При этом разрозненность каналов связи между пациентами и медорганизациями (ведь записаться пациент может через сайт медорганизации, по телефону или даже через Госуслуги), а также отсутствие единой системы взаимодействия между кол-центрами в регионе повышает риски злонамеренных и контрпродуктивных случаев применения современных технологий. Более того, повышается и вероятность случайных ошибок при работе с данными пациентов. Всё это может привести к дополнительным проблемам с кибербезопасностью медорганизаций и судебным разбирательствам. Подобные риски несёт процесс сбора, передачи, обработки данных и для других медицинских задач.

Идеальная ситуация — когда сами сведения не выходят за рамки защищённого информационного контура. По большей части медицинские специалисты в рамках одной медорганизации готовы работать с ПДн пациентов. Сложности начинаются, когда данные необходимо передавать в другие системы или осуществлять их обмен между иными медицинскими и немедицинскими организациями, решениями, контрагентами (провайдеры, облачные хранилища, разработчики ПО). И тут на сцену выходят разные методы обезличивания информации.

2. ОБЕЗЛИЧЕННЫЕ ДАННЫЕ В МЕДИЦИНЕ: СПЕЦИФИКА И ОСОБЕННОСТИ ПРИМЕНЕНИЯ

К персональным данным относятся такие сведения, как фамилия, имя, отчество, дата рождения, адрес проживания, пол, вес, рост, сведения о состоянии здоровья и др. При этом сведения о состоянии здоровья пациента, причины его обращения за медицинской помощью, диагноз и особенности лечения являются врачебной тайной и относятся к специальной категории персональных данных.

Ключевой нормативный акт, которым должны руководствоваться медицинские организации при работе с персональными

данными, — 152-ФЗ «О персональных данных», который предусматривает, в частности, регламент обработки данных непосредственно медицинской организацией. Порядок обработки персональных данных охватывает такие процессы, как сбор, запись, систематизация, накопление, хранение, уточнение и обновление, извлечение, использование, передача, блокирование, удаление, уничтожение данных, а также процесс обезличивания данных. Именно он в отрасли цифрового здравоохранения обладает важными специфическими чертами.

Следует подчеркнуть, что для отрасли медицины процесс обезличивания данных исключительно важен: он позволяет обучать на медицинских сведениях пациентов современные системы и сервисы — в первую очередь с использованием искусственного интеллекта. Более того, для моделей машинного обучения сами персональные данные не столько нужны, сколько даже вредны — именно поэтому предпочтительнее использовать деперсонализированные данные, то есть обезличенные, однако с сохранением ключевых для модели параметров. Например, имя пациента, дата его рождения, адрес, паспортные данные для обучения модели не так важны, как медицинские сведения — результаты лабораторных и диагностических исследований, протоколы медицинских консультаций, заключения врачей, сведения из анамнеза и др.

Однако для медицинских задач понятия обезличенных и анонимных данных не тождественны. Более того, в настоящее время отсутствует метод, который мог бы полностью обезличить данные с сохранением их ценности для дальнейшего использования. Так, собрав несколько наборов данных (даже обезличенных) и применив к ним математическую обработку, можно косвенно установить личность человека, к которому они относятся, а значит, и его персональные данные. Пусть даже не имея доступа к персональным данным пациента, но зная имя врача, который его принимал, и время приёма, можно выяснить данные пациента, обратившись к расписанию в регистратуре.

Таким образом, обезличивание персональных данных — это не гарант полной анонимности, но способ значительно снизить риски нарушения прав граждан при обработке персональных данных или при их утечке. Так, в медицинских системах чаще всего используют замену частей сведений идентификатором (когда вместо Ф. И. О. пациента используется числовое обозначение) и обобщение

(например, когда вместо даты рождения указывается только год или даже просто возраст).

В медицинских информационных системах, которые внедряются в больницы, также применяются алгоритмы обеспечения безопасности личных сведений, например, передача данных шифруется по криптографическому протоколу TLS, или безопасность обеспечивается благодаря фрагментарной архитектуре построения, которая разбивает общий информационный массив на отдельные ячейки. Это значительно снижает риски, связанные с обработкой персональных и обезличенных данных пациентов. Но самый главный результат — данные становятся полноценным «цифровым топливом» для решений на базе ИИ, которое необходимо, если мы хотим совершенствовать технологии, повышать качество диагностики пациентов и беречь время врача.

3. РИСК УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В сфере цифрового здравоохранения этот риск остаётся, что неудивительно: вот уже более четырёх лет медицина входит в тройку приоритетных целей для злоумышленников. Так, в первом квартале 2022 г. медучреждения в РФ заняли второе место в мире по количеству атак (11%), уступив лишь госорганам (16%), и за три первых месяца прошлого года медицинские данные составили 15% всей похищенной киберпреступниками информации. Главными киберугрозами для организаций из медицинской отрасли признана кража конфиденциальной информации и шифрование файлов с последующей остановкой работы медицинских систем и оборудования.

Например, совсем недавно стало известно, что мошенники пытались похитить информацию о пациентах в медучреждениях под видом помощи в процессе защиты персональных данных: они рассылали по больницам уведомления от имени Роскомнадзора о выявлении нарушений в части обработки персональных данных (хотя это было не так) и запрашивали к ним доступ для устранения «нарушений».

Ещё один известный канал утечек — WhatsApp (принадлежит корпорации Meta, признанной в России экстремистской и запрещённой). По результатам недавних опросов, 93% врачей пользуется этим мессенджером для рабочих коммуникаций — они делятся с коллегами медицинскими данными пациентов, чтобы получить второе мнение, проводят телемедицинские консультации

для пациентов. Так в зарубежный мессенджер попадает важная информация о состоянии здоровья пациентов вместе с их персональными сведениями, что тоже повышает риски утечек и киберугроз.

КАК СВЯЗАНЫ МЕЖДУ СОБОЙ ЭТИ ТРИ АСПЕКТА

Разумеется, деперсонализация данных несколько снижает риски утечек ПДн. Однако не может нивелировать их полностью. Более того, для реализации этих рисков очень большое значение имеет человеческий фактор: часто утечка информации происходит просто по неосмотрительности пользователей или в результате невнимательного отношения врачей и младшего медицинского персонала к сохранению врачебной тайны.

Особо подчеркну: сама по себе обработка данных и их передача не создают риски. Риски создаёт человек, который имеет к ним доступ. И мероприятия по снижению рисков можно начать с регистрации всех попыток доступа к данным, как успешных, так и нет. Это позволит идентифицировать тех, кто обращается к данным, а значит, и определять надёжность человека. А сложное нормативное регулирование лишь усугубляет недостаточную осмотрительность тех, кто работает со сведениями, — как самих пациентов, так и врачей и других специалистов, тем самым упрощая злоумышленникам достижение их целей.

Медицинская отрасль остро нуждается в таком регулировании, которое в первую очередь позволит быстро вводить в научно-практический оборот новые массивы разнообразных обезличенных данных и создавать с их помощью цифровые модели, в которых остро нуждается российская медицина. Цифровой медицине надо вместе с регуляторами найти ту грань, где регламенты оборота персональных медицинских данных помогают упорядочить и оптимизировать процессы обезличивания данных и их обработки во внешних системах (диагностических, рекомендательных и подобных) — и при этом минимизируют риски утечек исходных данных. Найти эту грань вполне возможно совместными усилиями сообщества медицинских специалистов и всех регуляторов, частных к задачам защиты данных.

ПОМОГУТ ОБОРОТНЫЕ ШТРАФЫ И ДРУГИЕ МЕРЫ

ПО МНЕНИЮ ЮРИСТА



Евгений ЦАРЁВ
управляющий RTM Group

Защита персональных данных и вообще информации от утечек уже давно лежит не только и не столько в технической области, сколько в юридической и даже политической. Количество инцидентов растёт: по данным аналитиков, в 2023 г. число утечек в крупных компаниях увеличилось в полтора раза по сравнению с прошлым годом. Среди них такие, например, как двойная утечка данных бонусной программы «Сберспасибо» (суммарно 52,5 млн записей), ресурса zdravcity.ru (8,9 млн записей) и «Спортмастер» (46 млн записей).

Неудивительно поэтому, что всё больше усилий по обеспечению защиты информации предпринимают не только коммерческие компании, но и государственные организации. Каждый из регуляторов вносит свою лепту, выступая с новыми инициативами и подзаконными актами. Несмотря на то что это общемировой тренд, в России он имеет свою специфику.

ОСОБЫЙ ПУТЬ

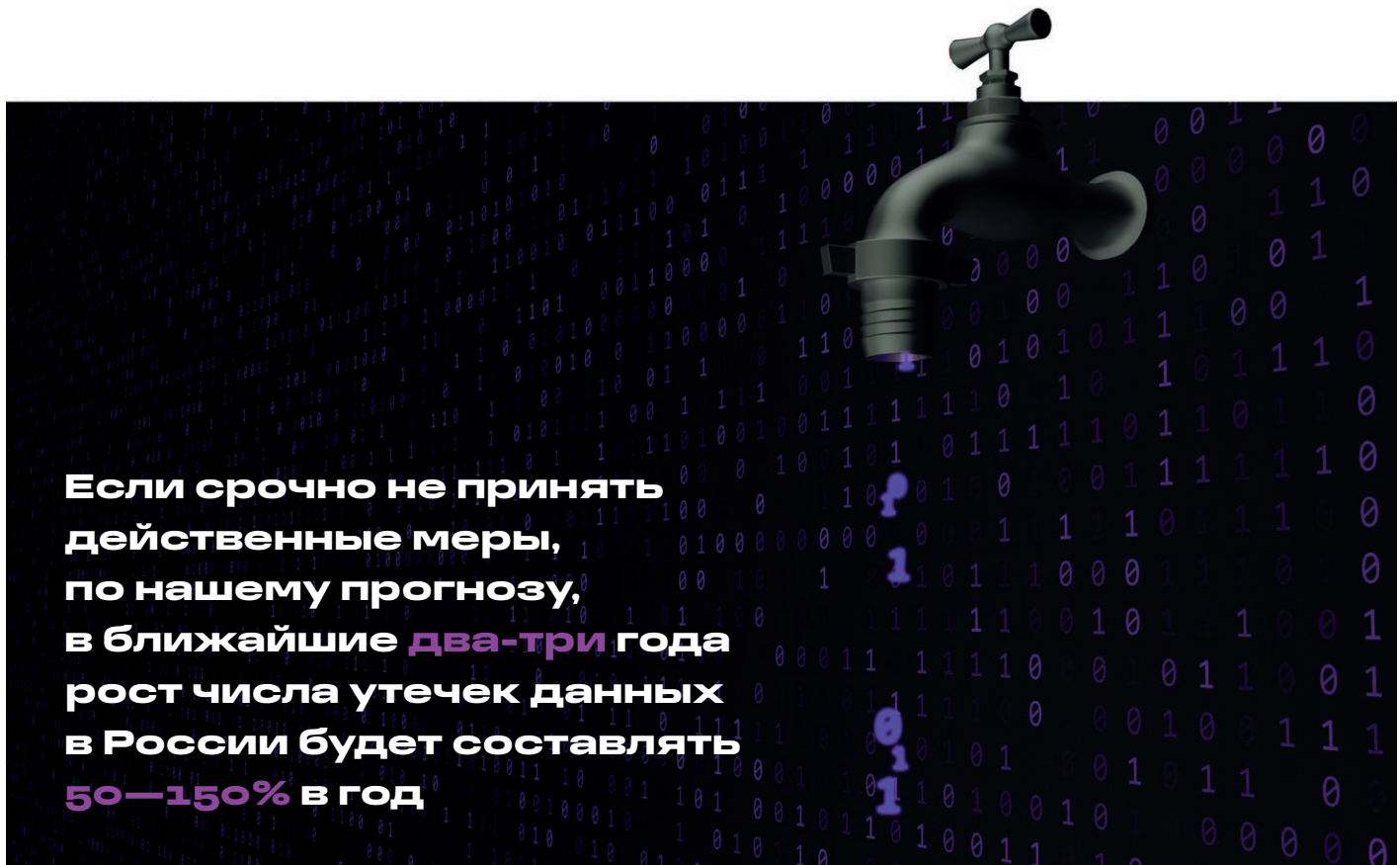
Появившийся 15 лет назад закон о защите персональных данных изначально разрабатывался как один из документов, призванных обеспечить соответствие России требованиям ВТО (Всемирной торговой организации). Однако уже в тот момент регулирование пошло в сторону технической

защиты информации. За прошедшие 17 лет тематика защиты персональных данных существенно эволюционировала. За это время закон многократно использовали отдельные государственные структуры, министерства и ведомства для решения собственных задач.

Так, он сыграл большую роль в поддержке отечественных производителей средств защиты информации. В 2008–2010 гг. значительно вырос рынок решений информационной безопасности, на что серьёзно повлиял закон о персональных данных и то, что через пару лет после его появления регуляторы стали предъявлять технические требования по обеспечению безопасности. Особый акцент делался, конечно, на использовании сертифицированных средств ЗИ (в большинстве своём — отечественных).

Выраженный политический окрас применения закона о персональных данных виден в направлении, связанном с «приземлением» иностранных ИТ-компаний. Здесь всё строилось во многом на том, чтобы обязать зарубежных ИТ-игроков, обрабатывающих персональные данные граждан РФ, хранить такие сведения внутри страны. Это подразумевает создание центров обработки данных, установку серверов, разделение данных иностранных пользователей и российских и хранение последних на территории РФ. Здесь прослеживаются явно политические мотивы.

Несмотря на такую длительную историю развития как юридической, так и технической стороны защиты данных, проблема с утечками в России так и не решилась. Напротив, мы видим, что она становится острее год от года. По-прежнему остаётся много проблем как в техническом, так и в правовом поле. Если срочно не принять действенные меры, по нашему прогнозу, в ближайшие два-три года рост числа утечек данных в России будет составлять 50–150% в год.



ПРИЧИНЫ БОЛЬШОГО КОЛИЧЕСТВА УТЕЧЕК

Очевидно, что государственное давление так и не привело к состоянию защищённости. Более того, основываясь на нашей практике по проведению судебных и внесудебных компьютерных экспертиз, можем заявить, что реальное количество и размер утечек существенно больше того, что мы видим в новостях.

Реальная безопасность персональных данных находится в России на довольно низком уровне, и у этого есть несколько основных причин:

1. Отсутствие каких-либо репутационных последствий для организации, которая допустила утечку ПД. Она не испытывает отток клиентов по результатам инцидента. Российские граждане привыкли к постоянным утечкам и не относятся к сведениям о себе как большой ценности. Однако в действительности каждый новый инцидент приводит к последствиям. Появление на чёрном рынке всё новых баз со свежими данными россиян создаёт плодородную почву для массовых атак методами социальной инженерии. Именно актуальность имеющихся у злоумышленников сведений о гражданах является определяющим фактором успешности того или иного варианта мошеннической схемы.
2. Чрезвычайно низкий финансовый ущерб для организаций, допустивших утечку имеющихся данных. Здесь нужно разделять сведения о юридических лицах и информацию о физических лицах. Дело в том, что в РФ по умолчанию открыто огромное количество данных о хозяйствующих субъектах. Например, ФНС публикует базы юридических лиц, судебная система также открыта, любой может найти сведения о судебных процессах организации и физлиц и так далее. Но наибольшее количество утечек связано с обычными гражданами, и это несёт в себе самую большую опасность для общества.
3. Нарушение норм ИБ. В большинстве инцидентов, связанных с утечками, с которыми мы сталкивались, были допущены грубые нарушения лучших практик обеспечения информационной безопасности, а также действующих стандартов и нормативных документов. Стандартизация ИБ развивается много десятилетий. Всё, что нужно конкретной организации, — это систематически выполнять необходимые процедуры и требования. Однако для реального бизнеса это нетривиальная задача, хотя и вполне выполнимая. Компании, допустившие большие утечки, не всегда, но, как правило, совершали грубые нарушения требований безопасности.
4. Проблема с кадрами. Дефицит специалистов каждый год нарастает, и это при

том, что высшая школа в принципе не может подготовить достаточное количество специалистов с минимальными знаниями. Игра с переманиванием квалифицированных кадров превратилась просто в гонку зарплат. Спрос на все категории специалистов на рынке настолько высок, что его уже невозможно покрыть переподготовкой или новыми выпускниками.

ЧТО ДЕЛАТЬ?

Неужели, если организации и государственные структуры за столько лет не смогли решить проблему с утечками, это невозможно сделать? Это не так. Ниже приведём самые важные направления и меры, внимание к которым точно будет иметь нужный эффект.

1. Самый большой потенциал по борьбе с утечками связан с введением оборотных штрафов за подобные инциденты. Реализация такой меры не сразу, но постепенно приведёт к сокращению их количества. Однако здесь важно адекватное администрирование данной нормы. С одной стороны, необходимо не допустить необоснованных и завышенных размеров штрафов, с другой — важно обеспечить и продемонстрировать неотвратимость штрафа или иных санкций для лиц и организаций, допустивших утечку.

Введение оборотных штрафов также быстро позволит решить проблему недофинансированности направления защиты информации. Вопрос о том, как убедить руководство выделить средства на покупку какого-нибудь нужного продукта для защиты информации, — чуть ли не самый популярный на любом профильном мероприятии. И вот когда все увидят, что для бюджета гораздо менее болезненно выделить средства на ЗИ и принять меры, чем платить объёмные штрафы, дело сдвинется.

2. Другим важным направлением в части борьбы с утечками является развитие и совершенствование нормативной базы. В частности, до сих пор нет чёткого определения, что такое «утечка данных». Это кажется странным, но это факт. Даже при обсуждениях под словом «утечка» каждый понимает что-то своё. И это лишь небольшой пример несовершенства нормативной базы, а таких «недопонятий» и несовершенств — множество.

3. Также важно развивать стандартизацию ИБ и прививать культуру проведения периодических аудитов ИБ как технических, так и «бумажных». Например, сегодня

отсутствует необходимость проведения оценки соответствия, тем более силами внешних аудиторов, для организаций, которые имеют отношение к критической информационной инфраструктуре. На мой взгляд, это неправильно. Нужно внедрять в регуляторику самые эффективные меры обеспечения безопасности и контролировать их систематическое применение.

По результатам экспертиз, которые мы проводим после утечек, в 9 случаях из 10 мы выявляем очень примитивные причины. На техническом уровне — это отсутствие актуальных обновлений, слабые пароли и неправильные права доступа. Выявить такие ситуации можно периодическими пентестами. В теории можно снизить количество утечек в 10 раз только одной этой мерой. И примеры уже есть. Когда Банк России обязал банки проводить периодические пентесты каждый год, количество успешных атак на банки снизилось на порядок. Аналогичное требование можно выставить для держателей крупных баз персональных данных.

4. Информационная безопасность как отрасль очень слабо автоматизирована. Подготовка любого отчёта, приказа, журнала и прочего происходит вручную силами дорогих специалистов. Всё взаимодействие с госорганами происходит по старинке. Нужен условный 1С для безопасности, который позволил бы ускорить и оптимизировать все процессы.

5. Отдельное внимание нужно уделить работе с судебной системой. Это финальная точка регулирования. Именно здесь часто возникают проблемы, а после введения тех же оборотных штрафов проблем станет ещё больше. Судебная практика развивается несистемно, отсутствует единообразное понимание проблемы со стороны следственных органов и судей.

Если предпринять мощные и единовременные усилия по всем этим направлениям, возможно будет не только не допустить дальнейшего роста инцидентов, но и сократить их количество. Важно при этом, чтобы действия всех ответственных структур были хорошо скоординированы, понятны, чтобы организации осознавали их необходимость и поддерживали. От этого зависит будущее не только отдельных направлений и структур, но и страны в целом.

СКДПУ НТ КОМПАКТ

**система контроля действий
внешних и внутренних
администраторов,
поставщиков ИТ-услуг
и других привилегированных
пользователей.**

ПРЕИМУЩЕСТВА:

- **Функциональность.**
Несмотря на компактные размеры имеет полный набор функций комплекса СКДПУ НТ.
- **Универсальность.**
Система одинаково удобна в использовании и на распределенных по разным территориям точках крупного бизнеса, и в информационной структуре небольших компаний.
- **Быстрое развертывание.**
Продукт устанавливается не в разрыв сетевого трафика и не требует агентов на целевых системах, что особенно важно при подключении к критическим ресурсам. Уже готов к использованию.



КОМУ НЕОБХОДИМ:

- Геораспределенным корпорациям (сети АЗС, электростанции, банки, магазины и др.),
- Малому и среднему бизнесу, работающему с чувствительными данными.

**Легкий и компактный контроль
привилегированного доступа –
СКДПУ НТ Компакт.**

it-bastion.com



ООО «АйТи БАСТИОН»

119501, Россия, Москва,
ул. Староволынская, 15, к. 1.

E-mail: info@it-bastion.com
Тел.+7 (499) 322 36 67

Больше информации на сайте:
www.it-bastion.com



ЧЕМ СИЛЬНЕЕ БУДУТ НА НАС ДАВИТЬ, ТЕМ ЖЁСТЧЕ БУДЕТ ОТВЕТНАЯ РЕАКЦИЯ



Василий ПИСКАРЕВ
председатель Комитета
Государственной Думы
по безопасности и противодействию
коррупции

В минувшем сентябре в России прошли выборы различного уровня, в том числе избирались 26 глав субъектов Федерации и депутаты законодательных собраний в 16 регионах. Подводя итоги, можно сказать, что российская избирательная система успешно преодолела этот рубеж, несмотря на усиленные попытки Запада и киевского режима активно вмешаться, запугать избирателей и повлиять на итоги голосования.



В особенной степени такое давление ощущалось в новых субъектах Федерации, где выборы проходили в условиях военного положения и постоянных обстрелов со стороны вооружённых формирований Украины. Но запугать людей и сорвать выборы не удалось. Избирательная система сработала чётко.

Показала свою устойчивость и система дистанционного электронного голосования (ДЭГ). Инфраструктура ЦИК РФ пережила 175 тысяч кибератак, но технологическое ядро при этом не пострадало. В этом году в выборах с применением компьютерных технологий в 25 регионах участвовало почти 4 миллиона наших сограждан.

Сегодня можно с уверенностью сказать, что попытки Запада дискредитировать электронную систему голосования результатов не принесли. Но нужно понимать, что это был лишь один эпизод кибервойны против нашей страны, а угрозы и вызовы в сфере информационной безопасности сохраняются. Наши противники совершенствуют технологии, и нам тоже нельзя останавливаться на достигнутом.

ЗАПАД РЕПЕТИРУЕТ ВМЕШАТЕЛЬСТВО В ПРЕЗИДЕНТСКИЕ ВЫБОРЫ

Мы хорошо понимаем, что нынешние выборы замыкают для Запада многолетний цикл тренировок по

деструктивному воздействию на нашу избирательную систему перед президентскими выборами 2024 года. За это время были опробованы многочисленные методики манипулятивного воздействия на избирателей и технологии дестабилизации внутренней обстановки у нас в стране.

Речь фактически идёт об идеологических диверсиях стран Запада как в отношении самого процесса формирования добровольного волеизъявления граждан, так и в отношении всей нашей избирательной системы.

По имеющимся данным, с начала текущего года под буквально ежедневным внешним информационным давлением находились как избирательное законодательство, так и все этапы избирательного процесса: выдвижение и регистрация кандидатов, агитационная деятельность, процедуры голосования, работа избирательных комиссий, наблюдателей и так далее.

ПОД ПРИЦЕЛОМ НАШИ ДЕТИ

Информационные атаки на избирательную систему России традиционно осуществлялись иностранными агентами, представителями нежелательных и экстремистских организаций, зарубежными СМИ в первую очередь из США, Англии, Германии, Франции, Латвии, Литвы и других стран НАТО и медиаресурсами, которых мы насчитали более 100, а также бежавшими за рубеж гражданами России, которые за гарантии политического убежища и безопасности там, у западников, отработывали сценарии по дискредитации нашей страны, открыто поддерживали нацистов, призывали к введению санкций и проведению диверсий в нашем государстве.

В этом году против нашей страны опробовали новые технологии. Мы зафиксировали деструктивную деятельность специальных зарубежных новостных медиапроектов о политике для подростков от 12 лет.

Наряду с уже традиционной дискредитацией школьной программы, «Разговоров о важном», пропагандисты этих новостных выпусков (иноагенты) начали осваивать новое направление — активное внушение и навязывание детям сфабрикованной критически-ложной оценки нашей действующей избирательной системы.

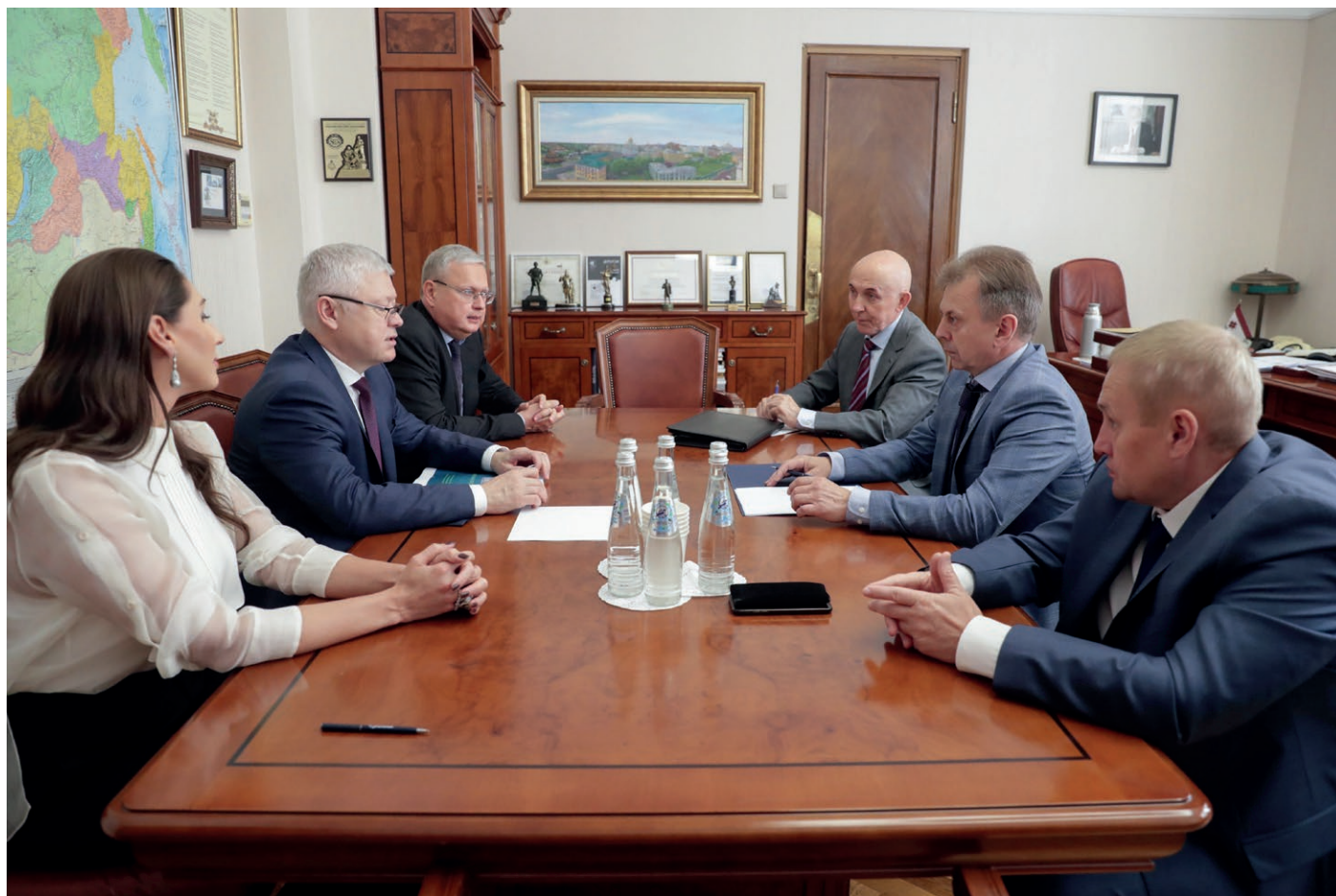
Это действительно опасно, потому что дети через несколько лет сами станут избирателями или могут быть избраны в органы власти. Важно, чтобы они принимали решения не под влиянием наших противников.

Можно заметить, что борьба Запада за умы наших детей и молодёжи не только не снижает своих темпов, а наоборот, активизируется. Всё это требует нашего особого внимания и принятия мер в соответствии с законами Российской Федерации.

СОЦСЕТИ — ПЛОЩАДКА ИНФОРМАЦИОННЫХ БИТВ

Противник бьётся и за расширение взрослой аудитории. Например, в июне текущего года около 30 СМИ-иноагентов вступили в коммуникацию с компаниями Apple, YouTube, Twitter, Microsoft, Google и Meta¹ с целью

¹ Корпорация Meta признана в России экстремистской организацией.



Встреча Комиссии Государственной Думы по расследованию фактов иностранного вмешательства с членом ЦИК РФ Игорем Борисовым

увеличения охвата и беспрепятственного распространения своего ядовитого контента на российскую аудиторию в предвыборный период, в том числе в рамках подготовки к президентским выборам 2024 года.

Мы также заметили традиционно активную работу по дискредитации текущей избирательной кампании со стороны уже государственного Агентства США по глобальным медиа (USAGM), куда входят СМИ-иноагенты «Радио Свобода» и «Голос Америки»². Собственно, они задают планку.

Кроме изготовления и разгона фейковой информации, USAGM провело в конце июля 2023 г. в Черногории для российских журналистов, как они себя называют, «в изгнании», тренинг по распространению через соцсети, в том числе в ходе выборов, «грязного» контента, ориентированного на население России.

Выявлены факты давления на избирателей и членов избирательных комиссий, в том числе в новых субъектах Российской Федерации, уже и со стороны еврочиновников, посольств ряда стран Запада, иностранных неправительственных организаций, действующих при поддержке посольства США в Киеве и Центра информации и документации НАТО на Украине. Обращение Комиссии

Государственной Думы с просьбой дать правовую оценку таким действиям уже рассматривается компетентными органами. Ожидаем решения о признании деятельности замеченных во вмешательстве в избирательный процесс организаций нежелательными в России.

ПРОВОКАЦИЙ УДАЛОСЬ ИЗБЕЖАТЬ

В период подготовки к выборам мы находились в постоянном контакте с коллегами из ЦИК России. В частности, мы передали в Центризбирком материалы о подготовке иноагентами за рубежом активных участников провокаций на избирательных участках. Речь идёт о заброске в нашу страну псевдонаблюдателей-провокаторов для создания «нужной» иностранным СМИ картинки. Наша информация была доведена Центральной избирательной комиссией до сведения руководителей избирательных комиссий субъектов Российской Федерации, и провокаций удалось избежать.

Конечно, Запад усердно готовится к нашим президентским выборам. Активизирована деятельность их спецслужб и «агентов влияния». Таких примеров, к сожалению, собрано немало. Надо быть готовым к любым провокациям.

Их спецслужбы тщательно изучают данные о проблемных моментах в регионах нашей страны и оценивают их влияние на протестные настроения перед выборами.

² «Радио Свобода» и «Голос Америки» включены Минюстом России в реестр иноагентов.



Василий Пискарев на заседании Комитета Государственной Думы по безопасности и противодействию коррупции

При этом вместо, так скажем, традиционных форм вмешательства НАТОвцы всё чаще стали применять методы запугивания экстремистского и террористического характера, организовывать диверсии и политические убийства. Всё это сопровождается подготовленными информационными кампаниями с целью расшатать внутривнутриполитическую ситуацию в России.

Сомнений быть не должно, эти действия не останутся без внимания и ответа.

За последнее время нами уже принято около 30 законов, направленных на защиту суверенитета и противодействие вмешательству извне во внутренние дела нашей страны.

И работа в этом направлении будет продолжена.

Чем сильнее на нас будут давить, тем жёстче будет наша ответная реакция.

ЗА ОПРАВДАНИЕ МАССШУТИНГА ПРИДЁТСЯ ОТВЕТИТЬ

Одной из последних инициатив, направленных на защиту наших детей от разрушительного воздействия из-за рубежа, стал внесённый в Государственную Думу мною совместно с коллегами законопроект, которым предлагается дополнить статью 280 Уголовного кодекса РФ («Публичные призывы к осуществлению экстремистской деятельности»). Ответственность будет

грозить также за публичное оправдание или пропаганду экстремизма наравне с ответственностью за призывы к осуществлению экстремистской деятельности. Наказание по этой статье предусматривается от штрафа до 300 тысяч рублей и вплоть до пяти лет лишения свободы.

Считаем, что принятие наших поправок будет важной профилактической мерой, направленной в первую очередь на то, чтобы защитить детей и молодёжь от деструктивного влияния экстремистской идеологии и попыток вовлечь их в противоправную, опасную деятельность. Этот законопроект — наша реакция, в частности, на пропаганду так называемого массшутинга — массовых убийств в учебных заведениях и детских садах. Оправдание подобных страшных преступлений и попытка представить их «модными» в молодёжной среде через интернет и соцсети крайне опасная тенденция, и мы должны такие веяния, которые насаждаются в русскоязычном интернет-пространстве внешними силами, решительно пресекать.

Уверен, что принятие предлагаемых поправок будет способствовать эффективной борьбе с этим злом и защите безопасности России.

«ИБ — ДАВНО САМОСТОЯТЕЛЬНАЯ ОТРАСЛЬ»

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ ОДИН ИЗ СОЗДАТЕЛЕЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

Борис Николаевич МИРОШНИКОВ

Вице-президент группы компаний «Гарда»

Родился в 1950 году. Генерал-полковник милиции в отставке. Генерал-лейтенант ФСБ в отставке.

Образование: техническое — МВТУ им. Баумана, юридическое — Академия ФСБ, кандидат юридических наук.

Работая в органах государственной безопасности и внутренних дел, занимался разработкой и внедрением в оперативную практику новых методов оперативно-розыскной деятельности, информационно-аналитической работы, создавал и руководил различными подразделениями. В частности, в ФСБ России — Управление компьютерной и информационной безопасности, в МВД России — Бюро специальных технических мероприятий (ранее в этих ведомствах таких подразделений не существовало).

Принимал участие в разработке внутригосударственных и международных нормативных правовых актов в области информационной безопасности, борьбы с преступлениями в сфере высоких технологий и кибертерроризмом. Организатор международного сотрудничества по борьбе с киберпреступностью и кибертерроризмом. Является членом Оргкомитетов различных международных конференций по информационной безопасности и борьбе с киберпреступностью, членом различных экспертных советов.

Является Президентом Национальной ассоциации международной информационной безопасности (НАМИБ), членом Научного совета Совета безопасности Российской Федерации.

Участвовал в формировании системы подготовки специалистов соответствующего профиля, преподавал в Университете и Академии управления МВД, Академии ФСБ, МТУСИ и МИФИ. Владеет английским языком.

Имеет звание «Почетный сотрудник госбезопасности», награжден орденами «За военные заслуги», «За заслуги перед Отечеством» 3-й и 4-й степени, более 20 медалями.



ИБ В МИРЕ

— **Борис Николаевич, скажите, существует ли в мире единое представление об информационной безопасности или в каждой стране её воспринимают и относят к ней по-разному? В чём это выражается? Как выглядит и какое место в таком контексте занимает ИБ в России?**

— Разумеется, единого представления нет, его и не может быть, если мы по сей день говорим о цифровом разрыве. Все страны идут

в цифровизацию своим путём: коротким или долгим. Страны-лидеры на этом пути также остаются лидерами. У этой группы есть общее в целом представление об ИБ: о безопасности критической инфраструктуры, о защите финансовой сферы, о борьбе с высокотехнологичной преступностью и так далее. Они готовят своих специалистов на одних материалах, они же создали у себя специальные ведомства по ИБ, что тоже их объединяет.

Другая группа стран ещё не до конца осознала проблему и только начинает строить у себя системы ИБ. Поскольку цифровизация здесь на начальном этапе, страны-лидеры готовы им всё предоставить: железо, софт, обучить специалистов, создать национальную структуру по ИБ и впредь сопровождать. А кто сомневается — тому бесплатно или в рассрочку, надолго. И сомнения пропадают. Одна беда — с суверенитетом, независимостью придётся расстаться. Тоже надолго.

И третья группа — самостоятельная. Китай и Россия — её основа. В Китае есть Комиссия по делам информатизации при ГосСовете, Национальный центр по противодействию киберугрозам и ряд других органов, участвующих в обеспечении национальной ИБ. Работает «Золотой щит», из него в своё время выделился «Великий китайский файрвол», который тоже надёжно защищает национальное информационное пространство КНР.

У нас в России эти вопросы курирует Совет безопасности. Исполнители — ряд известных ведомств, каждое на своём участке. Суммарно можно утверждать, что наше информационное пространство достаточно хорошо защищено. События последних лет наглядно это продемонстрировали.

Можно упомянуть ещё один критерий разбивки стран на группы. Первая группа — передовые, развитые, которым есть что прятать и защищать из соображений национальной безопасности. А секреты прячут друг от друга, ибо противодействуют. Другая группа — страны, у которых нет таких больших тайн и секретов, поэтому они ограничиваются простыми, но необходимыми системами: финансовая, управленческая, персональные данные. Вот через эти системы они идут к пониманию ИБ в целом и в государственном масштабе.

Например, в Индонезии оператор связи обязан хранить в тайне все переговоры, всю информацию своих клиентов, никто не имеет права подслушивать или перехватывать информацию. Защита и охране подлежат тайна личной жизни, здоровья, финансовое положение. Примерно так строят свою политику ИБ множество стран этой группы.

ИБ В РОССИИ

— **Можно ли считать ИБ в России самостоятельной отраслью? Если да, то почему она регламентируется одновременно множеством регуляторов (ФСБ, ФСТЭК, Минцифры, Банк России...)? Если нет, то как она структурируется и насколько это оптимально?**

Судьба безопасника вообще незавидна. Он источник проблем, он придумывает какие-то неудобные для людей режимы и регламенты, он вечно грозит какими-то рисками, вечно требует каких-то денег, и от него нет никакой прибыли!

— Конечно, можно. Это давно самостоятельная отрасль. По функциям, по технологиям, инструментам, специалистам, их подготовке, по научному обеспечению этих проблем. И в конце концов, по мышлению. Есть Айтишники и есть айтишники: одни с большой буквы, другие — с маленькой. Они разные. Те, кто собирает информационную систему на предприятии, в банке, в ведомстве... И те, кто занимается информационной безопасностью там же. Отлично помню ожесточённые споры разного уровня руководителей о том, где должна быть функция ИБ: в департаменте информатизации или в департаменте безопасности. Сначала побеждали первые, теперь, похоже, вторые. Собственно, эти споры продолжаются и до сих пор.

Судьба безопасника вообще незавидна. Он источник проблем, он придумывает какие-то неудобные для людей режимы и регламенты, он вечно грозит какими-то рисками, вечно требует каких-то денег, зачастую больших, и от него нет никакой прибыли! А ведь это противоречит основной цели бизнеса — получению выгоды!

С другой стороны, зачатую руководители часто думают, что разбираются во всём. И конечно, в безопасности. Но их уровень знаний в этой области, как правило, оставляет желать лучшего. Поэтому далеко не всегда принимаются верные решения в области безопасности.

Что касается структуры и регуляторов, мне представляется, что уже лет 20 в стране есть потребность в наличии органа исполнительной власти, ведомства, которое отвечало бы за информационную безопасность, было бы координатором, дирижёром и диспетчером. Но существует другой взгляд, система функционирует, и — результативно! Такая распределённая система: у ФСБ свои задачи, у ФСТЭК — другие, у Минцифры — третьи.

Верю в анализ, в научный прогноз, который делают настоящие специалисты, и в волю. А истерики рекламных кампаний лишь «искажают реальную картину потребностей в сфере ИБ» и обслуживают коррупцию

И все они регуляторы, которые выполняют свои функции в зоне своей ответственности. В результате — надёжный щит! Правда, встаёт вопрос: какой ценой с организационной точки зрения?

О СТРУКТУРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

— Существует ли в принципе представление об идеальной структуре информационной безопасности в России, какой она должна быть? Возможно ли достичь такого идеала или любая структура — это всегда игра случая, продукт безжалостной государственной эволюции?

— Не существует и не надо. Структура ИБ диктуется нормативами. Их много — от каждого регулятора понемножку. Где критическая инфраструктура, где финансы, где топливная энергетика, и везде-везде — персональные данные. Вариантов поведения два: первый — пройти проверку и удовлетворить регулятора; второй — построить реальную модель угроз для конкретного случая и создать систему ИБ для конкретного случая. Вот это и есть недостижимый идеал. Кстати, не всегда эти два решения совпадут.

С одной стороны, необходимость выполнять нормативы и требования регуляторов, а с другой — баланс между страхами, реалистичными оценками угроз и финансовыми возможностями.

О ЦПК, ЦЕРТАХ И УБК

— На страницах BIS Journal ведётся дискуссия о создании Центра противодействия угрозам (ЦПК) в финансовых организациях. Некоторые смотрят ещё шире и предлагают создать этаким СуперкиберМВД в сфере ИБ в масштабах страны. Как вы к этому относитесь?

— Отрицательно. В финансовой сфере борьба с правонарушениями централизована в достаточной степени. В своё время как раз для этого создали Финцерт в Центробанке. Правда, по мнению многих специалистов, эта сфера несколько заорганизована усилиями главного регулятора и можно бы чуть-чуть отпустить вожжи контроля, а ответственность в полной мере вернуть финансовым организациям. Они же любят самостоятельность! Почему за их разгильдяйство должен отвечать ЦБ? Когда на машине скорой помощи написано EMERGENCY, понятно, что это неотложно, срочно, немедленно! Так переводится это слово. Когда на Западе придумали «ЦЕРТы» (CERT, Computer Emergency Response Team), от английского «немедленное реагирование на компьютерные инциденты», тогда и наши коллеги начали, повинаясь моде, тоже создавать «ЦЕРТы». И возникло сомнение: либо вы не понимаете, что там написано, либо вы намеренно нам врётё. Ибо ничего немедленного в действиях «ЦЕРТов» не было. Напротив — неторопливое собирание информации об инцидентах и потерях... Далее следовал трудный драматический выбор ответственного за ИБ о том, что лучше: пропустить удар от хакера или получить штрафные санкции от регулятора?

Что такое СуперкиберМВД, не знаю. Но в МВД в прошлом году после многочисленных заявлений о создании киберполиции создали новое подразделение для борьбы с этими преступлениями. Притом что ещё в 1998 году в МВД была создана линия с этими же функциями. То есть для работы и получения результатов всё есть. А мифический Центр противодействия финансистов должен научиться взаимодействовать с силовиками — новым управлением в МВД, называется УБК. Опыт у нас в стране богатый, специалистов достаточно, и это наш главный ресурс.

О РЫНКЕ

— Считаете ли вы рынок в сфере ИБ идеальным регулятором, как говорят многие? Не кажется ли вам, что агрессивная реклама и нагнетание ИБ-компаниями апокалиптических настроений в своих интересах искажают реальную картину потребностей в сфере ИБ?

— Нет, не считаю. Игры в чудодейственные рыночные механизмы, во всяком случае в нашей стране, чудес не принесли. Верю в анализ, в научный прогноз, который делают настоящие специалисты, и в волю. А истерики рекламных кампаний лишь «искажают реальную картину потребностей в сфере ИБ» и обслуживают коррупцию.

О ПРОБЛЕМЕ КАДРОВ

— Как относитесь к проблеме кадров в сфере ИБ?

— Верно отмечено: не проблема недостатка, а проблема кадров. Стало привычным говорить о недостатке специалистов в области ИТ. И никто не возражает. Это реально так? Или это очередная кампания? Очередная крайность, между которыми мы вечно колеблемся. У нас было, кто помнит, перепроизводство инженеров. Ещё великий юморист тех времён Аркадий Райкин изволил шутить под аплодисменты зрителей: «В семье горе — муж-инженер». Это предполагало нищую и маловостребованную категорию граждан. Потом были экономисты. Их плодили с невиданной скоростью, но счастья они так и не принесли, как известно. Ни себе, ни стране. Потом был уклон в сторону юристов. Как же, Америка — страна юристов! Вот в чём их секрет! Мы будем как Америка. И будет нам счастье! Ну и что?

Теперь вот — айтишников, видите ли, не хватает. Какие-то запредельные цифры звучат. А вопрос — каких айтишников? Они же разные! Кого не хватает? Разработчиков! Но разработчик — это талант, это самородок. Его надо искать, образовывать, растить... Их не может быть много.

А есть ещё категория, которая, как из кубиков, складывает нужную конфигурацию защиты информационной структуры. Это, пусть не обижаются, ремесленники. От них не требуется «Лунная соната». От них требуется грамотное высокопрофессиональное ремесло.

А вот ещё новость: гуманитарные учебные заведения тоже, оказывается, готовят специалистов по ИБ. Им кругозор нужен. Видимо, это так и есть. Кто же против кругозора?

Но вот вопрос в связи с заявленной нехваткой. Что лучше: 10 хороших специалистов или 100 плохих? Суворов ещё учил: бей не числом, а умением.

ПРО ИМПОРТОЗАМЕЩЕНИЕ

— Каковы перспективы импортозамещения в сфере ИБ? Будет ли являться уникальностью нашей ИБ плюсом?

— Убеждён, что мы обладаем достаточным потенциалом, чтобы полностью решить эту проблему. Да, простые задачи уже решены, и нужна только воля, чтобы внедрить повсеместно наши отечественные продукты. На другие задачи требуется время. И те самые мозги, о которых мы говорили выше, и, конечно, мотивация. Причём мотивация — это далеко не всегда деньги. Есть компании,

которые развиваются без господдержки и дают прекрасные результаты. Мы в стране создали и развиваем по-своему уникальную систему информационной безопасности. И мы будем способны поделиться своими наработками, продуктами и опытом с дружественными странами. У них есть потребность, у нас — возможность её удовлетворить. Один БРИКС чего стоит! Теперь БРИКС плюс!

ПРО BIS JOURNAL

— Какое место в становлении и развитии ИБ в России, на ваш взгляд, должны занимать отраслевые СМИ, в том числе BIS Journal? Нам важно понимать свою роль в общем процессе, а поняв, играть её достойно, ощущать себя полезными своей отрасли, профессии безопасника.

— Наверное, в силу возраста я всегда предпочитаю «читать бумагу». Пробовал по-другому, но не нравится. «Невкусно!» Очень ценю ваш журнал, изучаю регулярно, по мере появления. Он в лучшую сторону отличается от других таких же — отраслевых. У вас нет раздражающей комплиментарности, помпезности. Вы интересны деловитостью и демократичностью — у вас много интересных и разнообразных авторов. Что нужно? Нужен спор, дискуссия. Показ альтернативы, другого мнения.

Важно и то, о чём мы говорили: какие специалисты нужны? Каких перебор? Разбор ошибок! Это всегда важнее, чем убогие «лучшие практики». Маловато обзоров зарубежного опыта. Объективного. Тем более что опыт там средний, рассчитанный на среднего западного обывателя, а не на нашего бунтаря. Но это не беда, опыт — это всегда интересно. Только в умном исполнении.

Вы очень нужны! Прислушивайтесь к людям, и они это оценят. Успехов!

Мы в стране создали и развиваем по-своему уникальную систему ИБ. И мы будем способны поделиться своими наработками, продуктами и опытом с дружественными странами

«ОДИН ПЛЮС ОДИН — НАМНОГО БОЛЬШЕ, ЧЕМ ДВА»

СОВМЕСТНЫЕ ПРОЕКТЫ — ШАНС ДЛЯ РОССИЙСКИХ КОМПАНИЙ ДОБИТЬСЯ ГЛОБАЛЬНОГО УСПЕХА



Андрей ЕФРЕМОВ
директор по развитию
бизнеса «Лаборатории
Касперского»

СИТУАЦИЯ НА РЫНКЕ

— Как вы оцениваете ситуацию на рынке, насколько успешно идет трансформация отрасли ИБ, достигнута ли импортонезависимость?

— Ситуацию на российской рынке ИБ я бы назвал стабильной, но непростой. Поскольку ИТ-сервисы продолжают работать, отрасль справляется с защитой национальной экономики, несмотря на огромное количество атак. Есть стабильность, хотя, честно говоря, не очень устойчивая. С рынка ушли многие игроки, в некоторых сегментах — технологические лидеры. Не все продукты и сервисы получили адекватную замену, но большая работа со стороны отечественных вендоров продолжается. Все крупные российские компании, которые пользовались ушедшими с рынка продуктами и услугами, знают, что переход на отечественный софт и железо — процесс очень непростой. Мы как вендор ИБ делаем все, чтобы помочь клиентам максимально качественно закрыть потребности с помощью конкурентоспособных и качественных решений. Но при этом мы как ИТ-заказчик не всегда довольны локальными продуктами.

ПОТЕНЦИАЛЬНАЯ ЛОВУШКА

— С 2022 г. на нашем рынке случился взлет спроса на местные ИБ-продукты и сервисы. Это — шанс для скачка в

развитии российских ИБ-вендоров. Насколько получается использовать этот шанс?

— Сперва про «Лабораторию Касперского». Мы успешно закрыли ниши, где были необходимы решения по обеспечению кибербезопасности и начали наращивать присутствие в смежных областях. Российский рынок активно развивается, и это хорошая почва, чтобы создавать и интегрировать в нашу экосистему новые продукты, на базе уже сформулированных потребностей. В этом году мы представили рынку решение для построения надежной сетевой инфраструктуры с возможностью интеграции средств ИБ — Kaspersky SD-WAN — и уже закончили его первое внедрение в крупной энергетической компании. Это решение обеспечивает защищенную передачу данных, что позволяет нам двигаться дальше и строить концепцию SASE (Secure Access Service Edge) как следующий этап развития сетевых технологий.

Развиваются наши XDR-решения. Мы запустили защиту для контейнерных сред. При этом мы видим спрос на эти решения и на глобальном рынке, и мы планируем его удовлетворить, предложив заказчикам зрелую платформу для обеспечения кибербезопасности.

Согласен, рост спроса на домашнем рынке — великий шанс, но в то же время и потенциальная ловушка для российских вендоров. Исходный посыл вроде бы прост — заместить привычные продукты и сервисы. Россияне десятилетиями пользовались продуктами от мировых лидеров, и вдруг многие из них в одночасье «превратились в тыкву». Срочно нужна замена этим привычным продуктам, замена лихорадочно разрабатывается, наши вендоры честно пытаются повторить потребительский опыт, который был до февраля 2022-го. Но у мировых гигантов на разработку своих решений уходили годы и даже десятилетия.

И какой вывод? Он прост: замещая функционал механически, российские вендоры могут что-то заработать и чему-то научиться, но в результате получатся далеко не идеальные копии лидерских продуктов трех-пятилетней давности. У нас их, конечно, купят, но на международном рынке с такими продуктами вообще никаких шансов не будет. Концентрация исключительно на импортозамещении и отказ от международной конкуренции в долгосрочной перспективе означает стагнацию и усугубит технологическое отставание российской ИБ-индустрии и основных игроков отрасли от передовых практик международного рынка.

ОРИЕНТАЦИЯ НА ЭКСПОРТ

— «Лаборатория Касперского» — один из немногих российских ИТ-вендоров, исторически ориентированных на экспорт. Насколько новая геополитическая реальность повлияла на ваш международный бизнес, на ваши приоритеты?

— В этих сложных условиях наша стратегия с ориентацией на мировые рынки подтвердила свою правильность. Стратегические продукты, на которые мы делали и делаем ставку, развиваются, их продажи растут по всему миру. Чтобы быть конкурентными на мировой арене, мы продолжаем двигаться в сторону платформенного подхода для обеспечения кибербезопасности всех видов корпоративных клиентов. Наши продажи в России значительно выросли. При этом, к сожалению, на ряде рынков они по понятным причинам снизились. Мы остаемся экспортной компанией, мы видим, что возможности на доступных для нас рынках — гигантские, и наши продажи в ряде регионов продолжают расти. В первую очередь это Ближний Восток, Южная Америка, ряд азиатских стран. Я считаю, что даже в нынешних условиях ориентация на экспорт крайне важна для долгосрочного успеха бизнеса.

ПРИЗЫВАЕМ ОБЪЕДИНИТЬ УСИЛИЯ

— Вы не раз призывали российские компании объединять усилия с «Лабораторией Касперского» и вместе выходить на внешние рынки. Есть ли примеры таких альянсов? И зачем все эти сложности, не лучше ли работать в автономном режиме, не завися от капризов партнеров?

— Очень надеюсь, что скоро поделюсь новостями об успехах по созданию альянсов, но пока могу сказать только, что работа в

этом направлении идет, и оптимизм нас не покидает. Зачем нам это надо? Чтобы реализовывать большие проекты. Мы можем делать их сами, но это будет долго, мы можем покупать компании, но это будет дорого. Объединение усилий позволяет добиваться успеха быстрее и дешевле, причем, понятно, не только нам, но и партнерам. В эффективном альянсе сложение усилий позволяет добиваться большего, чем просто арифметическая сумма усилий. Один плюс один может стать намного больше, чем два. Я считаю, что такие совместные проекты — это огромный шанс именно для российских компаний добиваться глобального успеха. Если вы — компания-лидер, если у вас есть амбиции строить высокотехнологичный экспорт, то нам с вами есть о чем поговорить.

РАБОТАЕМ В РОССИИ

— Почему вы приглашаете именно российских партнеров?

— Национальная ИТ-отрасль, несмотря на высокий спрос на отечественном рынке, живет в сложных условиях. В стране не так много долгосрочных инвестиционных денег, колебания валютных курсов усложняют стратегическое планирование, компании сталкиваются с дефицитом кадров, есть объективные проблемы с электронно-компонентной базой. При том у российских компаний имеется колоссальный опыт и инженерный потенциал мирового уровня, который не всегда, к сожалению, получается трансформировать в создание конечных масштабируемых продуктов. Совместные проекты лидеров рынка позволят компенсировать эти слабости и в полной мере использовать наши сильные стороны.

Вообще, в России умеют создавать новые вещи высочайшего уровня — от атомных станций до финтеха, от операционных систем (включая нашу специализированную KasperskyOS) до Госуслуг и средств ИБ. Хотелось бы разрабатывать большие упакованные прорывные проекты для глобального рынка, а это трудно делать в одиночку.

ЗАВЕДОМО НЕПРОДУКТИВНО

— Что из происходящего в российской ИБ вам не нравится?

— Меня расстраивает, что большие ресурсы тратятся на жесткую конкуренцию за очень небольшой рынок. Причем с некоторыми продуктами — практически заведомо без шансов создать что-то глобально конкурентоспособное. Это как строить десяток параллельных туннелей — заведомо непродуктивно.

Создание прорывных ИБ-продуктов для текущего глобального рынка — интересная и перспективная задача, у нас огромный опыт и экспертиза, и я верю, что мы можем создавать лучшие в мире решения

— Речь о межсетевых экранах?

— Да, но не только про них, есть ряд проектов по импортозамещению, где идет параллельная работа по созданию решений, в лучшем случае аналогичных зарубежным продуктам пятилетней давности.

ТРИ СТРАТЕГИИ

— Экспортные альянсы — это часть стратегии «Лаборатории Касперского»?

— У нас три стратегии для разных технологических волн, в которых мы существуем. Первая, среднесрочная стратегия на ближайшие несколько лет, подразумевает развитие наложенных средств безопасности, выстраивание лучшего на рынке продуктового предложения — B2B-платформы, закрывающей все потребности заказчика в ИБ. Это в том числе включает помощь нашим заказчикам в создании собственного центра мониторинга безопасности (SOC) или предоставление сервисов управляемой защиты от наших экспертов — Kaspersky MDR. Кстати, уже сейчас, наверное, самые передовые SOC в России успешно используют наше SIEM-решение KUMA (Kaspersky Unified Monitoring and Analysis Platform). Мы развиваем экосистему, которая обеспечивает кибербезопасность как классических корпоративных ИТ-инфраструктур, так и промышленных сетей и систем автоматизации (OT). В рамках этой экосистемы мы обеспечиваем и защиту конечных устройств (EDR), и защиту сети (NDR), достигая функциональности передового XDR-решения, причем для различных платформ (Windows, Linux, MacOS, Android и т.д.)

Но мы видим и следующую технологическую волну — переход с повсеместного использования уязвимого ПО на выстраивание ИТ на принципах secure-by-design, конструктивной безопасности, мы это называем кибериммунностью. Для этой волны — наша

долгосрочная стратегия, которую мы реализуем уже сегодня, развивая нашу собственную операционную систему KasperskyOS и экосистемы вокруг нее.

Третья наша стратегия — это мостик между технологическими волнами, переход от решения задач информационной безопасности вокруг текущих ОС к созданию ИТ-систем на основе конструктивной безопасности.

Мы ищем партнеров для проектов во всех трех стратегиях. Создание прорывных ИБ-продуктов для текущего глобального рынка — интересная и перспективная задача, у нас огромный опыт и экспертиза, и я верю, что мы можем создавать лучшие в мире решения. Также нам очень интересно создавать вместе продукты и решения в более широкой ИТ-сфере для переходного периода. И, конечно, необходимы партнеры, чтобы создать полноценную альтернативу потребительскому опыту от текущих лидеров рынка. Строительство полной кибериммунной экосистемы на основе конструктивной безопасности, которая будет конкурентоспособной на мировом уровне, — это задача огромного масштаба и амбиций.

МЫ СТРОИМ БУДУЩЕЕ

— Главный фактор успеха на международном рынке?

— В нашем случае — качество технологий и продуктов. Мы проводили партнерскую конференцию в этом году, и наши B2B-партнеры даже в западных странах говорят нам, что надеются на ослабление ограничений, так как они хотят продавать и распространять наши решения, поскольку они эффективно удовлетворяют запросы заказчиков, имеют высокое качество.

В целом я считаю, что для долгосрочного успеха надо иметь большие амбиции и стремиться создавать новый опыт для потребителей. Только так можно срезать углы и стать лидером на уже сложившемся рынке. Выходить на рынок с копией чужого, пусть и передового, решения — значит биться за каждую продажу, конкурировать по цене, имея заведомо более низкую рентабельность, более долгую окупаемость, а значит и меньше ресурсов для долгосрочного развития.

Чтобы добиваться успеха, надо иметь большую мечту. Мы строим ИТ-опыт будущего, который будет актуален для наших детей и внуков, внедряем безопасность на уровне ДНК ИТ-систем. И я призываю других лидеров рынка с большими амбициями объединять усилия и строить цифровое будущее вместе с нами.



Kaspersky Unified Monitoring and Analysis Platform

Центральный элемент единой платформы безопасности

- Мониторинг и анализ инцидентов ИБ
- Поточная корреляция в режиме реального времени
- Автоматическое обогащение данными об угрозах
- Масштабируемая архитектура и низкие системные требования
- Тесная интеграция с решениями «Лаборатории Касперского» и сторонних производителей
- Обеспечение соответствия законодательству в сфере безопасности объектов КИИ

kaspersky АКТИВИРУЙ
БУДУЩЕЕ

kaspersky.ru/enterprise

ДиалОгНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

РЕПОЗИТОРИЙ АФТ КАК ОБЪЕДИНЯЮЩАЯ СИЛА

СОВМЕСТНОЕ ТЕСТИРОВАНИЕ, РАЗРАБОТКА И ПРИНЦИПЫ DEVSECOPS



Олег МОРГУН
руководитель
управления
развития технологий
Ассоциации ФинТех

Перед участниками финансовой отрасли стоит множество задач, в том числе обеспечение технологического суверенитета и ускорение процесса цифровизации с использованием отечественных ИТ-решений. О том, где участникам рынка искать доверенное

ПО, как организовать совместную разработку и тестирование решений, а также ускорить процесс внедрения DevSecOps, рассказывает руководитель управления развития технологий Ассоциации ФинТех Олег Моргунов.

ОБЪЕДИНИТЬ УСИЛИЯ

Сегодня компании финансового рынка как никогда раньше сосредоточены на поиске решений, которые полностью закроют их потребности, отвечая при этом всем требованиям безопасности, нормативным и функциональным требованиям, а также требованиям технологического суверенитета. Кроме этого, участники рынка говорят о потребности в совместной разработке и тестировании инструментов, в том

ТЕХНОДАЙДЖЕСТ ОТ АССОЦИАЦИИ ФИНТЕХ



МCKINSEY СОСТАВИЛА РУКОВОДСТВО ПО ГЕНЕРАТИВНОМУ ИИ ДЛЯ СГО

Эксперты предлагают руководителям ИТ-подразделений сфокусироваться на девяти ключевых действиях при внедрении генеративного ИИ:

1. Определить позицию компании в отношении внедрения генеративного ИИ и ознакомить с ней сотрудников.
2. Определить примеры использования генеративного ИИ, которые повышают ценность бизнеса.
3. Попытаться сосредоточиться на развитии потенциала генеративного ИИ при разработке ПО, сокращении технического долга и минимизации ручного труда.
4. Воспользоваться существующими сервисами или адаптировать модели с открытым исходным кодом для разработки собственных решений.
5. Модернизировать технологическую архитектуру предприятия для эффективной интеграции и управления моделями генеративного ИИ.
6. Разработать инфраструктуру данных, обеспечивающую качественный доступ к данным из различных источников.

7. Создать централизованную команду по разработке платформы генеративного ИИ, которая будет обеспечивать продуктовые и прикладные команды утверждёнными моделями.

8. Вкладывать средства в повышение квалификации ключевых специалистов, таких как разработчики ПО, инженеры по данным, инженеры MLOps и специалисты по безопасности.

9. Оценить и смягчить риски, связанные с моделями, данными и законодательством в новом ландшафте генеративного ИИ.

IBM ОПУБЛИКОВАЛА ОТЧЁТ «ГЕНЕРАТИВНЫЙ ИИ В ОРГАНИЗАЦИЯХ: СОВРЕМЕННОЕ СОСТОЯНИЕ РЫНКА»

Средний ROI проектов с использованием генеративного ИИ растёт, и руководители компаний ожидают, что к 2025 году он превысит 10%. В связи с этим организации планируют повысить темпы внедрения технологии в ближайшие два года. Если в 2022 году только 23% руководителей заявили, что в их организациях был опробован, внедрён, эксплуатируется или оптимизирован

числе — кросс-отраслевым (ИТ-компания, банки, страховые, телеком-операторы и т.д.). Согласно опросам и консультациям, проведённым на площадке Ассоциации ФинТех, участники рынка готовы объединять усилия для создания и развития новых отраслевых решений. Но для этого нужна независимая площадка, на которой решения будут собираться, классифицироваться, тестироваться, проверяться, а также совместно разрабатываться.

РАВНОУДАЛЁННАЯ ПЛОЩАДКА

Работа над Репозиторием АФТ, который должен объединить специализированные ИТ-решения для финансовой отрасли, началась в сентябре 2022 года. Для того чтобы соблюсти интересы участников рынка, важно было хранить, тестировать и разрабатывать решения именно на равноудалённой площадке.

Члены Ассоциации высказались за то, чтобы такой независимой площадкой стал Репозиторий АФТ. И уже 2 марта 2023 года первый зампред Банка России Ольга Скоробогатова сообщила о его создании.

Что уже сделано? На площадке Ассоциации совместно с участниками АФТ и Банком России проведён анализ специфических

требований финансовых организаций по развитию ИТ-ландшафтов, а также текущих поставщиков ИТ-решений для финансовой отрасли. По результатам этой работы в промышленную эксплуатацию введена новая (вторая) версия Репозитория, в которой реализованы консолидированные требования участников АФТ, представителей ИТ-рынка и Банка России:

♦ поставщики ИТ-решений получили бизнес-аналитику своих ИТ-решений в разрезе функциональных карт финансовых организаций и других классификаторов:

- функциональная карта банка;
- функциональная карта СК;
- функциональная карта НПФ;
- классификатор Минцифры;
- решения для обеспечения ИБ;

♦ ИТ-решения с открытым кодом;

♦ для представления ИТ-решений в Репозитории АФТ используются как классификаторы функциональных, так и выделенный классификатор ИТ-решений для обеспечения информационной безопасности финансовой организации;

♦ реализовано несколько вариантов гибкого, многофакторного, адаптивного поиска ИТ-решений;



Рисунок 1. В целом руководители в большей степени нацелены на расширение потенциала и обеспечение роста за счёт повышения качества обслуживания и в меньшей степени — на снижение затрат

генеративный ИИ, то к 2024 году этот показатель вырастет до 62%. Руководители считают, что внедрение генеративного ИИ открывает такие возможности, как повышение качества контента, стимулирование конкурентоспособности и расширение компетенций сотрудников. В целом они в большей степени нацелены на расширение потенциала и обеспечение роста за счёт повышения качества обслуживания и в меньшей степени — на снижение затрат (рис. 1).

ЕВРОКОМИССИЯ ПРЕДСТАВИЛА СТРАТЕГИЮ ПО РАЗВИТИЮ МЕТАВСЕЛЕННОЙ

Стратегия, представленная Еврокомиссией, разработана в контексте цифровизации и её влияния на экономику ЕС после 2030 года. В докладе говорится, что объём мирового рынка виртуальных миров вырастет с € 27 млрд в 2022 году до более чем € 800 млрд к 2030 году.

В отчёте сформулированы четыре «ключевых столпа стратегии»:

1. Люди: расширение возможностей и укрепление навыков для повышения осведомлённости, доступа к достоверной информации и формирования кадрового резерва специалистов по виртуальным мирам.

2. Бизнес: поддержка европейской индустриальной экосистемы Web 4.0 для наращивания передового опыта и устранения фрагментации.

3. Правительство: поддержка общественного прогресса и виртуальных госуслуг внутри виртуальных миров. Комиссия запускает два новых государственных проекта:

♦ **CitiVerse** — иммерсивная городская среда, которая может быть использована для целей планирования и управления городом;

♦ европейский **цифровой двойник человека**, который будет дублировать человеческое тело для поддержки принятия клинических решений и индивидуального лечения.

- ♦ в карточке ИТ-решения расширены разделы описания лицензии и ключевых элементов технологического стека;

- ♦ для удобства описания ИТ-решения в карточке используются справочники (баз данных, импортных аналогов, операционных систем, языков программирования и др.).

В данный момент полным ходом идёт процесс наполнения Репозитория, для чего организована селекция отечественных ИТ-решений для финансовой отрасли и, по мере необходимости, их тестирование. К процессу валидирования ИТ-решений из Репозитория АФТ привлечены коллегиальные органы Ассоциации — Комитет по технологиям и Совет архитекторов.

Что планируется:

- ♦ добавление новых классификаторов по самым передовым технологиям, прежде всего в области облачных технологий и искусственного интеллекта;

- ♦ встраивание в функционал Репозитория так называемого технологического бенчмаркинга от аналитиков АФТ. Он будет представлять собой сравнительный анализ решений с точки зрения используемых технологий. Бенчмаркинг будет встроен в поисковый механизм, что позволит компаниям выбирать

наиболее технологичные и современные решения;

- ♦ добавление инструментов для проверки, сборки, контроля версий и анализа уязвимостей, а также совместной разработки программных решений с открытым кодом.

СОВМЕСТНАЯ РАЗРАБОТКА И ТЕСТИРОВАНИЕ

В Репозиторий АФТ, помимо собственно реестровой и репозиторной части, встроены инструменты для совместного тестирования и разработки решений. По сути, у представителей российского финансового сектора появилась безопасная отраслевая среда для совместного тестирования, верификации и разработки. Это позволит компаниям внедрять необходимые решения быстрее и эффективнее, заметно снизит себестоимость создания специализированного ПО.

Для консолидации усилий отраслевого сообщества по разработке и применению ИТ-решений с открытым кодом на площадке АФТ создаётся центр компетенций (ЦК) по безопасной разработке. В ЦК войдут представители ключевых игроков финтех-рынка: финансовых организаций, телеком-операторов и технологических компаний. Стратегическая

4. Инфраструктура: формирование стандартов для открытых и взаимодействующих виртуальных миров и Web 4.0, исключающих доминирование в них нескольких крупных игроков.

КОМПАНИИ ПРИЗЫВАЮТ К ПОДДЕРЖКЕ РЕШЕНИЙ С ОТКРЫТЫМ КОДОМ В ЗАКОНЕ ЕС ОБ ИИ (AI ACT)

GitHub, Hugging Face, Creative Commons и ряд неназванных организаций призывают усилить поддержку разработки различных моделей ИИ с открытым кодом при рассмотрении вопроса об окончательном принятии закона.

В списке предложений, направленных в Европарламент в преддверии окончательного принятия законопроекта, — более чёткие определения компонентов ИИ, уточнение относительно отсутствия выгоды от ИИ для исследователей, работающих над моделями по открытой лицензии, разрешение ограниченного тестирования проектов ИИ в реальных условиях и установление пропорциональных требований для различных моделей.

SARTNER ОПУБЛИКОВАЛ РЕЗУЛЬТАТЫ ОЦЕНКИ ИНВЕСТИЦИЙ В ИИ

При оценке показателя окупаемости инвестиций (ROI) в ИИ 52% организаций, достигших зрелости в этой области,

ориентируются на сочетание технических и бизнес-показателей. В менее зрелых организациях чаще используются только технические показатели.

41% компаний используют для оценки ROI бизнес-показатели, связанные с успешностью клиентов. Кроме того, 47% организаций называют обслуживание клиентов одной из трёх основных бизнес-функций, получающих выгоду от применения ИИ.

Исследование также показало, что 55% организаций, ранее внедрявших ИИ, всегда рассматривают ИИ для каждого нового кейса применения, который они оценивают. Более половины организаций (52%) отмечают, что факторы риска являются критически важными при оценке новых сценариев использования ИИ.

Опрос проводился с октября по декабрь 2022 года среди 622 респондентов — организаций США, Франции, Великобритании и Германии.

SARCEMINI ОПУБЛИКОВАЛ ОТЧЁТ «ПРИМЕНЕНИЕ ГЕНЕРАТИВНОГО ИИ: ПЕРЕДОВЫЕ ОТРАСЛЕВЫЕ КЕЙСЫ»

По результатам глобального исследования, 21% опрошенных руководителей утверждают, что генеративный ИИ значительно изменит их отрасли, а 74% заявляют, что выгоды от применения генеративного ИИ перевешивают риски.

задача, которая стоит перед центром, — создать сообщество специалистов для обмена опытом, имплементации методологий и практик по открытому коду и процессам безопасной разработки, с целью повышения уровня защищённости всего жизненного цикла финтех-решений, обеспечить понятный и прозрачный процесс использования свободного программного обеспечения (СПО) на финансовом рынке.

ЦК консолидирует опыт, знания и компетенции участников АФТ по безопасной разработке и применению СПО. Центр должен создать и поддерживать методологию процессов безопасной разработки ИТ-решений финансовых организаций. В сферу ответственности центра входит идентификация, оценка и тестирование ИТ-решений на основе СПО; организация совместных проектов по развитию ИТ-решений на основе СПО. Размещаться, храниться и тестироваться созданные решения будут в Репозитории АФТ. Для развития ИТ-решений на основе СПО будет использоваться запущенная АФТ технологическая песочница.

Помимо обязательного тестирования и верификации ИТ-решений на площадке АФТ, проверять ПО, внесённое в отраслевой Репозиторий, на своих конвейерах будут и

участники Ассоциации, в результате чего в карточке решения появится «галочка» — «проверено топовым участником». Такой подход важен для критичного ПО, так как оно будет проверено на мощных конвейерах крупнейших компаний страны и, таким образом, пройдёт независимую экспертизу.

ЗАЧЕМ ЭТО РЫНКУ?

Растущая потребность в быстрой разработке и внедрении решений, с одной стороны, и всё возрастающие киберриски — с другой ставят перед отечественными компаниями вопрос скорейшего внедрения DevSecOps в свои процессы. Использование методологии DevSecOps должно привести к повышению уровня защищённости разрабатываемых решений и достижению требуемого уровня технологической независимости организаций российского финансового сектора.

Создание Репозитория АФТ преследует ещё одну важную цель — формирование отраслевого сообщества экспертов. Их совместная работа не только значительно упростит процесс внедрения DevSecOps и поможет быстрее и более качественно разрабатывать необходимые решения, но и задаст импульс дальнейшего развития финтех-рынка.

74% руководителей компаний сектора высоких технологий утверждают, что создали специальные группы и выделили бюджеты на генеративный ИИ. В сфере финансовых услуг этот показатель составляет 42%. Треть руководителей финансовой отрасли заявляют, что используют генеративный ИИ для создания синтетических данных.

В разрезе финансовых услуг топ-3 кейса пилотирования генеративного ИИ — подготовка финансовой отчётности (38%), обнаружение мошенничества (34%), а также прогнозирование денежных потоков (32%). Промышленная эксплуатация технологии по вышеуказанным направлениям пока не превышает 5%.

МВФ ОПУБЛИКОВАЛ ДВА ОТЧЁТА ПО СОЦИАЛЬНЫМ АСПЕКТАМ И КОНФИДЕНЦИАЛЬНОСТИ В МЕТАВСЕЛЕННОЙ

Согласно прогнозам аналитиков МВФ, в ближайшие три года объём рынка метавселенной достигнет \$ 1 трлн. Это будет обусловлено быстрым распространением таких технологий, как генеративный ИИ. В отчёте «Конфиденциальность и безопасность в метавселенной» подчёркивается необходимость всемирного сотрудничества стейкхолдеров для развития понимания метавселенной и выработки защитных мероприятий.

В сопроводительном выпуске «Социальные аспекты метавселенной» представлено целостное понимание влияния метавселенной на людей, экономику и общество.

БОЛЕЕ 160 КОМПАНИЙ ПРИЗВАЛИ ЕС ТЩАТЕЛЬНО ПРОДУМАТЬ РЕГУЛИРОВАНИЕ ИИ

Компании опубликовали открытое письмо против предложенного европейского Закона об искусственном интеллекте (AI Act), заявив, что он потенциально угрожает конкурентоспособности и инновационности региона. В письме предупреждается, что правила приведут к жёсткому регулированию инструментов генеративного ИИ и повлекут как риски ответственности, так и высокие затраты на соблюдение требований для компаний, разрабатывающих эти технологии.

МЕТА (ЗАПРЕЩЕНА В РФ) И MICROSOFT АНОНСИРОВАЛИ ЗАПУСК БОЛЬШОЙ ЯЗЫКОВОЙ МОДЕЛИ (LLM) ПО ОТКРЫТОЙ ЛИЦЕНЗИИ LLAMA-2

Модель будет использоваться на базе облачной вычислительной платформы Azure от Microsoft. LLaMA-2 на 70B параметров сравнима по качеству с GPT-3.5 и превосходит её по некоторым бенчмаркам. LLaMA бесплатна для исследований и коммерческого использования, а также оптимизирована для работы на Windows.

МЕЖДОМЕННЫЕ РЕШЕНИЯ

КАК ОСНОВА ЭФФЕКТИВНОГО ОБМЕНА
ИНФОРМАЦИЕЙ ДЛЯ ОБЪЕКТОВ КИИ И НЕ ТОЛЬКО



Вячеслав
ПОЛОВИНКО
руководитель
направления
собственных
продуктов
АМТ-ГРУП

Значительный объём задач в области обеспечения безопасности – от противодействия угрозам национальной безопасности и террористическим атакам до противодействия несанкционированному воздействию на функционирование промышленных, энергетических, транспортных, медицинских, финансовых предприятий, органов государственного управления и власти, крупных коммерческих компаний – требует безопасного обмена данными между организациями разных уровней. В некоторых случаях необходимость такого обмена закреплена законодательно. В зависимости от стоящей задачи информация, создаваемая

и обрабатываемая в более доверенных (закрытых) сегментах сети, может в отдельных случаях передаваться в общедоступные сегменты или сегменты с меньшим уровнем доверия и менее строгими политиками безопасности – для её использования иным кругом лиц и потребителей. Для других случаев характерна обратная ситуация – информация должна поступать из общедоступных или менее доверенных сетей в более доверенные в целях агрегации, обработки, анализа, систематизации. Передаваемые данные могут представлять собой отдельный документ, сигнал (набор сигналов), телеметрию или целые каталоги (архивы) файлов, содержащие изображения, карты, документы и базы данных.

Эффективный обмен между сетями как с одинаковым, так и с разным уровнем доверия является комплексной и непростой задачей. Помимо сохранения конфиденциальности данных, необходимо учесть такие факторы, как скорость обмена, достоверность, безопасность и надёжность передачи данных. Решения, которые при-

званы обеспечить защиту в указанных условиях, получили название междоменных.

ИНТЕГРИРОВАННЫЙ КОМПЛЕКС

Междоменные решения представляют собой интегрированный комплекс решений по обеспечению безопасности. Комплекс, как правило, состоит из специализированного программного и аппаратного обеспечения с соответствующими интерфейсами для ручного или автоматического предоставления и/или ограничения доступа к информации разных категорий значимости, а также интерфейсами для организации передачи такой информации. Помимо технических решений, организация междоменного взаимодействия предусматривает набор организационных мер, обеспечивающих корректность применения всех компонентов в составе комплекса междоменного решения.

В контексте междоменных решений можно выделить следующие компоненты защищаемой инфраструктуры:

- ♦ **домен** – логически объединённая совокупность организационно-технических активов и ресурсов, подчиняющихся единой политике безопасности;

- ♦ **доверенная сеть** (в ряде случаев сеть/система-источник) – область, формирующая наибольшие риски в отношении утраты, компрометации, нарушения заданных характеристик обрабатываемой информации, систем, сегментов, данных, процессов;

- ♦ **менее доверенная сеть** (недоверенная сеть, в ряде случаев сеть/система-приёмник) – область,

Помимо сохранения конфиденциальности данных, необходимо учесть такие факторы, как скорость обмена, достоверность, безопасность и надёжность передачи данных

формирующая наибольшие риски в части вероятности организации атак из неё на иные сегменты и сети;

♦ **периметр** – граница доверенной сети, на которой выполняется аутентификация запросов, регулируются информационные потоки, применяются организационно-технические меры для снижения рисков в отношении информации, сетей, данных, процессов.

♦ **политика безопасности** – организационно-распорядительный документ, описывающий отношения между доменами. Для каждого домена в политике определяется, какие требования к обеспечению безопасности должны быть выполнены.

ДВА ТИПА РЕШЕНИЙ

Междоменные решения, как правило, разделяют на два основных типа:

1. Междоменные решения по организации доступа (размещаются между доменом и пользователем). Обеспечивают потребителям (системам, пользователям) возможность просматривать/читать и пользоваться информацией из доменов различных уровней доверия, снабжённых соответствующими атрибутами/признаками/категориями. В предельном варианте решения по организации доступа полагаются только на мандатное управление доступом и не предполагают перемещения данных между доменами. Таким образом, «идеальное» междоменное решение по организации доступа к данным обеспечивает такое разделение между доменами, которое полностью предотвращает смешение данных между доменами, гарантирует невозможность «перетекания» (и, как следствие, утечку) данных из доменов различных уровней категорирования/классификации на любом уровне модели OSI/TCP, то есть полностью нивелирует риски утраты данных. Примерами таких решений являются: изолированные рабочие станции, решения, основанные на регламентном/временном доступе с одной рабочей станции, решения класса KVM Switch, решения на основе системы виртуализации и др.

2. Междоменные решения по организации передачи данных (размещаются между доменами) обеспечивают возможность перемещения информации между доменами различных уровней доверия. Междоменные решения по организации передачи данных должны учитывать категорирование данных, отношения между доменами и применяемую для каждого домена политику. Примерами таких решений являются: воздушный зазор, МСЭ, «диоды данных», однопользовательские комплексные решения, двусторонние комплексные решения и др.

РЕШЕНИЯ ПО ОРГАНИЗАЦИИ ПЕРЕДАЧИ ДАННЫХ

Чуть более подробно хотелось бы остановиться именно на междоменных решениях по организации передачи данных, которые, как правило, представляют собой комплексные проектные решения и не ограничиваются применением только одного СЗИ. Использование именно таких решений становится всё более актуальным в условиях появления большого количества точек сопряжения сетей организаций с другими сетями, контроль за безопасностью которых ограничен.

Несмотря на существование большого количества различных междоменных решений по организации передачи данных, в общем виде они могут быть описаны в терминах и функциях сетевых устройств или шлюзов безопасности:

♦ прежде всего, междоменные решения по организации передачи данных должны контролировать соединения между доменами, фактически реализуя логику межсетевого экрана;

♦ решения DLP, DPI, IDS должны проверять передаваемые данные и протоколы на соответствие утверждённым политикам и определять соответствующие условия по их обработке, выполнять функции блокирования и сигнализации об обнаруженных проблемах;

♦ решения класса «диод» гарантируют соблюдение политики в отношении направления передачи потока

данных на физическом уровне, предотвращая, в частности, утечку данных и реализуя функции Protocol Break.

Междоменное решение по организации передачи данных для каждой пары доменов включает в себя политики передачи. Примером политики передачи может быть направление потока данных, протокол передачи, «временные окна» доступа к домену и т.п. Применяемые политики могут быть как достаточно простыми и невносящими существенных ограничений в обмен данными, так и весьма сложными.

Можно констатировать, что для эффективного доступа к информации и передачи информации между сетями одинакового и разного уровня доверия организациям необходимы автоматизированные системы со встроенными «протоколами безопасности». Задача таких организационно-технических систем в общем виде может быть сформулирована как предоставление решения, которое позволяло бы эффективно обеспечивать доступ к данным и передавать данные между отдельными сетями/сегментами одинакового и разного уровня доверия только после прохождения ряда контролей и проверок. Фактическим решением данной задачи является организация защищённого «туннеля» между сетями/сегментами, конкретные потоки в котором формируются, одобряются и/или saniруются в моменты передачи данных. В состав такого «туннеля» должны быть включены физические средства передачи данных, трансляторы протоколов, прикладные решения для файловой передачи (в том числе передачи эл. почты), сервисы интеграции, инструменты репликации баз данных и стриминга видео/рабочих столов, решения по контролю за передачей данных, решения по аудиту, оркестраторы.

ДОВЕРЕННАЯ ДОМЕННАЯ ИНФРАСТРУКТУРА

ИМПОРТОЗАМЕЩЕНИЕ В ДЕЙСТВИИ



Денис ПОЛУШИН
менеджер продукта Aladdin
Enterprise CA, компания Аладдин



Евгений ПАУТОВ
директор департамента
разработки средств управления
ГК «Астра»

Большинство компаний используют в качестве системы управления доменом решения от Microsoft. Ввиду ухода из России иностранного вендора заказчикам нужен работоспособный сценарий импортозамещения, который бы позволил им перевести корпоративную инфраструктуру на отечественные решения, выстроив на их основе безопасную доверенную ИТ-среду. Это серьезная и масштабная задача, которая требует комплексного подхода, и она может быть решена путем интеграции совместимых продуктов. Приведем пример совместной работы таких компонентов.

Первый из них — система централизованного управления службой каталогов ALD Pro от ГК «Астра». Она позиционируется разработчиками как полноценная замена Microsoft Active Directory. Второй компонент — корпоративный центр сертификации, разработанный российской компанией Аладдин. Это решение Aladdin Enterprise CA, призванное заменить службу Microsoft Certificate Services. Третий участник интеграции — Aladdin SecurLogon — клиентское приложение, которое реализует двухфакторную аутентификацию в среде Linux.

Расскажем подробнее о продуктах и о том, как они взаимодействуют друг с другом. ALD Pro существует на рынке уже более года и внесен в реестр отечественного ПО Минцифры. Он позволяет построить доменную инфраструктуру под Linux, причем с использованием не только Astra Linux, но и других дистрибутивов, и управлять ее объектами: компьютерами, учетными записями пользователей и серверами. Когда разработчики из ГК «Астра» создавали это решение, они думали в первую очередь про администраторов систем от Microsoft, которые мигрируют на Linux и не имеют достаточных компетенций для работе с этой ОС. Написание скриптов, работа в терминале и другие тривиальные для администратора-линукоида действия вызывают у них затруднения. Поэтому ALD Pro спроектировали таким образом, что вся работа ведется в графическом интерфейсе, как это сделано в MS Active Directory.

Важным аспектом при работе с доменом является управление организационной структурой. Существуют Open Source-проекты для Linux, такие как служба каталогов FreeIPA. Однако там отсутствует возможность завести подразделения в виде структуры, иерархии, а имеется лишь «плоский» справочник. Эта недостающая

возможность реализована в ALD Pro. Поддержка организационной структуры позволяет более эффективно настраивать полномочия администраторов, а также предоставляет больше возможностей для работы с групповыми политиками, чтобы они корректно распределялись по подразделениям.

Из последних нововведений в ALD Pro можно отметить поддержку глобального каталога, появление двусторонних доверительных отношений и синхронизации объектов. Пользователям очень важна гетерогенная работа в нескольких доменах, поскольку импортозамещение происходит не одномоментно: это долгий процесс, который может занимать не один год. Соответственно, администратору и пользователям, которые находятся в домене, нужно иметь возможность работы в гетерогенной среде.

Ранее продукт обладал только базовой функциональностью. Можно было настроить контролеры доменов, в целом развернуть службу каталога в своей инфраструктуре, завести туда компьютеры, учетные записи пользователей, настроить оргструктуру и работать с групповыми политиками, а также устанавливать ОС и ПО по сети.

В результате был сделан инструмент, который в автоматическом режиме синхронизирует все учетные записи между двумя доменами. Пользователи,

которые перешли на Linux, должны иметь доступ ко всем ресурсам, которые развернуты на Microsoft Windows. Миграция ресурсов — это процесс еще более длительный, поэтому разработчики реализовали функции глобального каталога и двусторонних доверительных отношений.

Ранее доверительные отношения также существовали, однако они были односторонними. ALD Pro доверял ресурсам Active Directory, а последняя не допускала учетные записи ALD Pro в свой домен, и в этом году в системе появилась возможность настройки полноценного двунаправленного доступа между доменами.

Также совместно с компанией Аладдин в этом году в ALD Pro было реализовано совместное решение для двухфакторной аутентификации в домене с использованием токенов JaCarta.

Как работает этот механизм? Внутри корпоративной инфраструктуры используются сертификаты, которые могут выдаваться как внешним, так и внутренним пользователям для аутентификации, подключения через VPN, документооборота и т.д. Сертификаты есть не только у пользователей, но и у серверов, сервисов, устройств. Компания Аладдин предоставляет корпоративный центр сертификации, Aladdin Enterprise CA. Решение предназначено для внедрения строгой аутентификации, создания по-настоящему доверенной инфраструктуры, обеспечения устройств и объектов сертификатами и корпоративными электронными подписями. Продукт зарегистрирован в реестре отечественного ПО.

В числе ключевых особенностей Aladdin Enterprise CA можно упомянуть ориентацию на пользователей Microsoft Certificate Services, поддержку миграции с решения Microsoft, совместимость с российскими операционными системами, включая Astra Linux, а также с доменами Active Directory и ALD Pro. Также важны наличие и поддержка всего необходимого функционала для организации PKI-инфраструктуры: иерархия, настройка точек доступа CRL DP, AIA, DeltaCRL, OCSP и т.д.

Поддерживаются алгоритмы шифрования RSA и ECDSA. В ближайших

Можно создать пароль длиной до 63 символов, скрытый от пользователя и недоступный, который нельзя записать на бумажке и приклеить на монитор

планах разработчиков — добавление поддержки алгоритмов ГОСТ. Имеется ролевая модель полномочий, возможность уведомления пользователя, различные способы выпуска сертификатов. Доступен API для подключения внешних систем.

Клиентское решение Aladdin Secur-Logon также служит важным элементом в построении инфраструктуры для двухфакторной аутентификации. Оно необходимо для настройки двухфакторной аутентификации, хотя, конечно, он обладает и другими функциями. К примеру, в инфраструктуре для пользователей он позволяет применять определенные политики в части обеспечения строгости и надежности пароля. Так, можно создать пароль длиной до 63 символов, скрытый от пользователя и недоступный, который нельзя записать на бумажке и приклеить на монитор, что обычно бывает со сложными паролями. От пользователя будет требоваться вход в систему только по токену. Есть и средства для группового администрирования, групповое развертывание и удаленная настройка с рабочего места администратора, защита удаленных соединений по RDP или SSH и др. Это мощный клиентский компонент, который можно применять для настройки аутентификации по сертификату, хотя его возможности гораздо шире.

Что дает интеграция ALD Pro и продуктов компании Аладдин? Пользователь получает токен JaCarta вместе с ключевой парой, сгенерированной удостоверяющим центром Aladdin Enterprise CA. С его помощью происходит двухфакторная аутентификация. Благодаря использованию Aladdin Enterprise CA стало возможным развернуть корпоративную PKI-инфраструктуру в среде Linux и

управлять пользовательскими ключами и сертификатами. Подобная автоматизация особенно заметна и эффективна, когда речь идет о сотнях и тысячах пользователей, которых необходимо обеспечить токенами.

Второе приложение, Aladdin Secur-Logon, предоставляет удобный графический интерфейс, с помощью которого можно аутентифицироваться в системе, используя двухфакторную аутентификацию.

Важным моментом в применении решений, позволяющих использовать двухфакторную аутентификацию внутри защищенной доменной инфраструктуры, является тот факт, что она значительно повышает сохранность и безопасность учетных данных пользователей домена. Это возможно благодаря совместной работе продуктов ALD Pro и Аладдин.

Aladdin Enterprise CA подключается к каталогу ALD Pro, получает сведения об учетных записях пользователей и их свойствах, позволяет выпустить для них сертификаты и опубликовать их на контроллере домена в ALD Pro. Таким образом все пользователи домена имеют свои сертификаты для входа в домен, что повышает уровень информационной безопасности.

ALD Pro контролирует, чтобы информация об ИТ-ландшафте не стала доступна злоумышленникам, и они не смогли спланировать и совершить атаку. Ролевая модель и механизмы разграничения доступа в ALD Pro позволяют защитить от посторонних глаз множество объектов инфраструктуры: компьютеры, серверы и учетные записи пользователей. А злоумышленника, не обладающего сертификатом, контроллер домена просто не пропустит на этапе аутентификации.

ZTNA VS VPN: АНТИПОДЫ ИЛИ ДРУЗЬЯ?



Вячеслав САВЛЮК
генеральный
директор
компании
ИТ-Экспертиза



Артём ТУРЕНОК
руководитель
отдела
технических
решений
АО «ДиалогНаука»

Стратегия ZTNA (Zero Trust Network Access) сейчас на слуху. Причём она довольно часто противопоставляется старым добрым технологиям VPN (Virtual Private Network). В качестве аргумента чаще всего приводится такое утверждение: в отличие от VPN, которые предоставляют полный доступ к локальной сети, решения на базе ZTNA предпочитают никому не доверять, разрешая доступ только к тем услугам или ресурсам, к которым пользователи явно запросили.

Кроме этого, бытует мнение, что у VPN неэффективная производительность: например, концентраторы VPN могут создавать узкие места, что приводит к снижению производительности, чрезмерной задержке в обменах информацией и тому подобным неприятностям. Порой настройка VPN — дорогая и трудоёмкая процедура, требующая больших усилий со стороны службы безопасности и самих пользователей.

В общем, «переходите все на ZTNA, и будет вам счастье». Так ли это? Неужели пришло время списывать со счетов проверенный временем VPN? Давайте порассуждаем на эту тему.

А ЧТО ТАКОЕ ZTNA

В стратегии ZTNA доступ к ресурсам и приложениям предоставляется на основе строгой аутентификации и авторизации. Каждый пользователь и каждое устройство должны пройти проверку и авторизацию перед получением доступа к ресурсам. А сами

пользователи и устройства имеют только те привилегии, которые необходимы для выполнения их конкретных задач. Всё это уменьшает вероятность несанкционированного доступа и помогает предотвратить вредоносные действия.

Но, прежде чем говорить о ZTNA дальше, окунёмся в историю. Считается, что идея Zero Trust («нулевого доверия») была придумана в 2010 году аналитиком Forrester. При этом в России парадигма «доверенной среды» появилась лет на 25 раньше. Несмотря на противоположные названия, есть много объединяющих их критериев (разрешено: только определенное ПО, процессы, определены ресурсы, к которым предоставляется доступ).

Есть и отличия: главный тезис концепции «доверенной среды» — если мы сможем быть уверенными в надёжности (лояльности, доверенности) каждого элемента, нам не обязательно изолировать их в замкнутой среде. В силу принципа декомпозиции, каждый элемент защищаемой информационной системы сам по себе может быть защищён, и в этом случае соединение их в единую информационную систему с помощью защищённых каналов позволит создать вокруг информации надёжную оболочку.

«Доверенная среда» предполагает, что должно быть доверие:

- ♦ к окружению системы;
- ♦ к субъектам отношений;
- ♦ к правилам и процедурам;
- ♦ к аппаратной и программной платформе;

- ♦ к выполняемым операциям;
 - ♦ к каналам передачи информации.
- Достичь требуемого уровня доверия возможно, если обеспечивается:
- ♦ локализация информационных ресурсов;
 - ♦ счётность субъектов и объекты доступа;
 - ♦ доверенность конфигурации и настройки;
 - ♦ целостность всех элементов;
 - ♦ подконтрольность всех действий;
 - ♦ логирование всех событий.

Иными словами, для реализации концепции «доверенной среды» в информационной системе должен быть создан специальный сегмент, имеющий защиту по всему периметру и не позволяющий постороннему бесконтрольно обращаться с информацией.

Вернёмся к стратегии ZTNA. Она предполагает создание вокруг приложения или группы приложений логической границы доступа на основе идентификации и контекста, то есть учёта группы или роли пользователя, его IP-адреса, местоположения и временных ограничений. Цель ZTNA заключается в обеспечении безопасного доступа к ресурсам и приложениям в сети вне зависимости от расположения устройства или пользователя.

Стратегия ZTNA предполагает:

- ♦ каждое устройство, пользователь и приложение должны быть проверены и авторизованы перед получением доступа к ресурсам в сети. Нет доверия к устройству или пользователю на основе их сетевого положения или предыдущих разрешений;
- ♦ сеть разделяется на отдельные микросегменты (микропериметры), где доступ к ресурсам и приложениям строго контролируется. Каждое соединение и каждый запрос должны быть аутентифицированы и авторизованы на уровне микросегмента. Это позволяет ограничить доступ к ресурсам только для необходимых пользователей и устройств и минимизировать поверхность атаки;

♦ для получения доступа к ресурсам требуется не только пароль, но и учет контекста, такого как атрибуты пользователя, идентификация устройства, контекст подключения и другие факторы.

В принципе, обе точки зрения говорят о схожих сущностях. Но традиционно «дьявол кроется в деталях».

С точки зрения «нулевого доверия» прежде всего требуется постоянный мониторинг и управление доступом и привилегиями пользователей, а также мониторинг всего трафика на предмет вредоносных действий. И здесь остается открытым вопрос доверия к конечному оборудованию пользователя.

С точки зрения «доверенной среды» требуется постоянный мониторинг конфигураций, настроек и целостности рабочих мест. То есть прежде всего — формирования доверия к компьютеру конкретного пользователя.

Ну, а процедура идентификации — аутентификации — авторизации в обоих случаях является обязательной.

Обратите внимание на две весьма схожие сущности: в одном случае говорится о сегментировании сети (локализации обрабатываемой информации), в другом — о микросегментах (собственно локализации приложений).

СЛАБОЕ ЗВЕНО

Между тем, во всех описаниях стратегии ZTNA, в отличие от концепции «доверенной среды», не упоминается об одном важном элементе. Посмотрите внимательно: есть удалённый (хотя не обязательно) пользователь, которого проверили со всем пристрастием. Компьютер его тоже опознали: идентифицировали и проверили все его параметры. А ещё есть микросегмент сети, в котором находится нужное приложение.

Получаются две доверенные сущности. И тут встает вопрос: а как эти сущности взаимодействуют? По всей вероятности, здесь требуется какой-то защищенный (доверенный) канал, тем более что общение сущностей идет через заранее агрессивную среду.

На сегодня наиболее эффективным для этих целей признается шифрова-

ние. Но ведь не все приложения имеют криптографическую функцию. И тогда канал связи без криптографии оказывается самым слабым звеном защиты.

Чтобы устранить эту брешь, строго следуя стратегии ZTNA, требуется на границе каждого микросегмента ставить некое устройство, позволяющее обеспечить шифрованный обмен информацией между пользователем и выбранным приложением.

А если пользователь использует несколько приложений или несколько пользователей из разных мест хотят задействовать одно и то же приложение, что делать? Представляете, насколько это усложнит систему?!

Однако выход из этой ситуации есть. Надо построить «толстый» канал, защищенный криптографией, между пользователем и периметром сети, а уже дальше применять стратегию ZTNA. Ну а чем это отличается от классического VPN? Вот и получается, что одно без другого не даст желаемого результата.

ДОВЕРЯЙ, НО ПРОВЕРЯЙ

Для того чтобы обеспечить контекстную аутентификацию, вначале надо провести инвентаризацию удалённого компьютера, создать некий его профиль и в дальнейшем с регулярной периодичностью отслеживать его состояние, настройки, конфигурацию, целостность.

То есть необходимо в режиме реального времени проводить мониторинг:

- ♦ ГДЕ находится компьютер;
- ♦ КАК подключается компьютер;
- ♦ ЧТО установлено на компьютере;
- ♦ ЧТО запущено на компьютере;
- ♦ ЧТО делает пользователь.

При этом средство мониторинга должно как минимум уметь контролировать:

- ♦ геолокацию компьютера и структуру информационной сети;
- ♦ состав программного и аппаратного обеспечения;
- ♦ параметры настройки операционной системы, версию, обновления;
- ♦ наличие установленных средств защиты информации, их параметры и включенные компоненты защиты;

♦ установку, настройку, актуальность программного обеспечения;

♦ тип и состав подключенных USB устройств;

♦ запущенные в операционной системе процессы;

♦ процедуры login/logoff пользователей.

Сведения обо всех этих параметрах как раз и будут составлять профиль рабочего места. Но пассивное наблюдение вряд ли даст положительный эффект. Необходимо не только контролировать, но и иметь возможность управлять рабочим местом: уведомлять администратора безопасности об отклонениях, блокировать доступ в критических ситуациях или переводить компьютер в карантин.

Однако и этого мало. Нужно правильно построить хранилище, в котором и должен храниться тот самый профиль рабочего места, с которым будет проводиться сравнение. Это и будет корень доверия. Естественно, что такое хранилище должно быть надёжно защищено и исключать всякую возможность изменения профилей.

РЕЗЮМЕ

Применяя новые технологии в защите информации, не надо забывать и о уже проверенных и хорошо себя зарекомендовавших технологиях. Стратегия ZTNA не заменяет VPN, а наоборот предполагает симбиоз этих технологий.

И совокупность технологий, обеспечивающих реализацию стратегии ZTNA, по меньшей мере, но не ограничиваясь, должна позволять выполнять:

- ♦ строгую (например, двухфакторную) аутентификацию;
- ♦ мониторинг состояния и параметров компьютера пользователя;
- ♦ мониторинг состояния и параметров СРЗИ, установленных на компьютере пользователя;
- ♦ строгое разграничение полномочий пользователя (например, по мандатному принципу);
- ♦ создание защищённых каналов связи (например, применение VPN);
- ♦ возможность блокировки подключения компьютера пользователя к сети в случае нарушения установленной политики его использования.

СКУПОЙ ПЛАТИТ ДВАЖДЫ

РЫНОК ИБ ГЛАЗАМИ РОССИЙСКОГО ВЕНДОРА



Максим СТЕПЧЕНКОВ
совладелец
компании
RuSIEM

За последние полтора года представления об информационной безопасности в России принципиально изменились, а риски для компаний ощутимо возросли. О текущей ситуации на рынке, импортозамещении, новых угрозах и кадровом голоде рассказывает совладелец компании RuSIEM Максим Степченко.

О СИТУАЦИИ НА РЫНКЕ

Начиная с 2022 года, зарубежные компании уходят из страны. В целом, российские производители ИБ-решений и раньше тяготели к импортонезависимости, так что на рынке ИБ радикальных сдвигов не случилось. Произошло замещение определенных западных продуктов на отечественные, но сам набор решений при этом практически не изменился.

Компании рекомендуют примерно то же самое, что и два года назад, только акцент сместился в сторону более оперативного запуска продуктов и более комплексного подхода.

Наша компания по итогам 2022 года показала более чем двукратный рост за счет увеличения спроса, а также планомерной реализации намеченных проектов. Но неправильно будет утверждать, что этот рост обусловлен исключительно фактором импортозамещения. Сработало, в том числе, правильное технологическое позиционирование RuSIEM. Согласно нашим внутренним опросам, для 42% новых клиентов наш продукт стал «входным билетом» к применению SIEM-систем для обеспечения информационной безопасности. Конечно, внешние обстоятельства так или иначе повлияли на бизнес и нашей компании, и других разработчиков SIEM-систем. Один из важнейших факторов — постепенное усиление регуляторного давления, из-за которого утечки и взломы обходятся компаниям все дороже. Соответственно, растет востребованность SIEM-систем как класса продуктов.

Если же попытаться описать общее положение на рынке сегодня, то я бы оценил его как вакханалию.

Люди почувствовали, что есть огромная свободная ниша, и побежали ее занимать, мол, создадим множество новых межсетевых экранов, SIEM, других продуктов... и у нас все купят.

К счастью, заказчик не настолько линеен, он все-таки проводит тестирование, проверку. Тем не менее, можно говорить о подрыве рынка. Заказчики начинают тестировать одно, другое, третье решение, и у них появляется ощущение, что все российские разработки — это... ну, не очень, назовём это так.

Что с этим делать? Устанавливать критерии качества, требовать обязательную сертификацию — неправильно. Будучи сторонником поддержки малого и среднего бизнеса, я всегда говорил, что мы должны поддерживать небольшие компании. С одной стороны, стоило бы поддерживать каждый стартап, потому что из каждого может вырасти что-то хорошее. С другой, один или несколько неудачных стартапов могут испортить отношение ко всему рынку.

Поэтому я считаю, что в рамках крупных государственных организаций и инициатив было бы полезно не просто давать гранты на развитие проектов, но и выделять полигонные площадки для тестирования и получения оценок. Желательно, чтобы мы получали от какого-то ведомства — независимого, никем не ангажированного, — контроль качества в сфере ИТ, который выдавал бы оценки по некоему ГОСТу и говорил: система прошла тестирование, можно пилотировать у заказчиков. Пока этого не произойдет, отношение к российскому рынку останется негативным.

О ПРОЦЕССЕ ИМПОРТОЗАМЕЩЕНИЯ

С 1 января 2025 года использовать иностранное программное обеспечение

Если же попытаться описать общее положение на рынке сегодня, то я бы оценил его как вакханалию. Люди почувствовали, что есть огромная свободная ниша, и побежали ее занимать

на значимых объектах КИИ будет нельзя. Успеют ли госкомпании, а особенно субъекты КИИ уложиться в отведенное время? С одной стороны, сложные системы, которые внедряются в течение нескольких лет, сейчас будут замещаться более простыми, но в то же время справляющимися с нагрузками. Здесь срок замещения равен сроку внедрения «с нуля» — значит, успеют.

С другой стороны, далеко не у всего ПО есть отечественные аналоги. Новые решения могут разрабатываться не один год, что критично не только для бизнеса, но и для государства. Нам повезло — мы одними из первых поняли, что системы класса SIEM будут импортозамещаться. Однако многим организациям придется в последний момент сталкиваться с сырыми или недостаточно апробированными решениями.

Таким заказчикам придется создавать тестовые стенды, исследовать ПО, чтобы убедиться в его работоспособности, обучать персонал. Небольшая компания справится, а вот организации, где десятки тысяч сотрудников и отстроенные процессы, будет очень непросто.

А представьте, если во время атаки на компанию перестанет работать установленное в ней импортное оборудование и ПО? Мы вернемся в каменный век. Вероятность такого невелика, но она есть.

Ситуация в регионах осложнена нехваткой ресурсов и необходимых знаний. Понимая эти особенности, с 2022 года мы сделали упор на региональные проекты, коих стало в десятки раз больше.

О НОВЫХ УГРОЗАХ

Если в 2021 году мы могли говорить о том, что основная цель атак — это компании финансового сектора и ритейла, а прочие рискуют меньше, то теперь акцент сместился в сторону госсектора, объектов КИИ, СМИ и всего, что связано с охраной важных объектов и информацией.

По большому счету основные угрозы не изменились — нарушения конфиденциальности данных, доступа к данным. Но принципиально поменялось следующее: раньше компании

Я повторяю одно и то же много лет: Неуловимого Джо давно нет. Атакуют всех! А теперь добавляю: если раньше атаквали ради денег, то сейчас просто, чтобы отключить систему

из государственного или коммерческого сектора атаквали зарубежные хакеры, сегодня — кибервойска. Если раньше мы могли рассчитывать на поддержку со стороны правоохранительных органов других стран, то сегодня это невозможно, ведь зачастую эти нападения спонсируются самими государствами.

Я повторяю одно и то же много лет: Неуловимого Джо давно нет. Атакуют всех! А теперь добавляю: если раньше атаквали ради денег, то сейчас просто, чтобы отключить систему.

О НЕОБХОДИМОСТИ ИНВЕСТИЦИЙ В ИБ

Самый популярный запрос звучит сегодня так: «У нас ничего нет. Сделайте так, чтобы у нас все было правильно». Но если серьезно, то запросы самые разные. Начиная от «нас взломали, помогите!» и заканчивая «мы не доверяем нашим сотрудникам».

Естественно, основной объем запросов поступает на мониторинг событий ИБ. Основной наш продукт — RuSIEM — дает понимание о происходящем внутри инфраструктуры, позволяет «вычислить» злоумышленника до момента, пока он причинит реальный ущерб, и принять меры, чтобы купировать инцидент. Другими словами, компаниям интересны возможности, которые предлагают SIEM-системы. Рост интереса к SIEM со стороны малого и среднего бизнеса — еще одна тенденция, которую мы зафиксировали в 2022 году. С нашей точки зрения, необходимость в мониторинге и реагировании на инциденты становится базовой потребностью для компаний, где кибербезопасности уделяют

должное внимание. Без скидок на масштаб бизнеса

Растет число обращений, связанных с потребностью отслеживания состояния инфраструктуры для обеспечения ее бесперебойного функционирования. Поток запросов настолько плотный, что мы решились на выпуск специализированного продукта RuSIEM Monitoring. И тем самым поспособствовали заказчикам в решении задачи доступности инфраструктуры.

О СЛОЖНОСТЯХ ПЕРЕХОДА

Нельзя путать импортозамещение со сменой лейблов. Некоторые организации хитрят: они берут западную продукцию, наносят другую наклейку, и теперь это российский сервер. С ПО сложнее. Иногда российский продукт создается на базе зарубежных Open Source решений. Это законно. А псевдороссийский продукт, конечно, позволяет какое-то время формально выполнять требования регулятора, но где гарантия, что Минкомсвязи России не исключит его из реестра? Подобные примеры уже есть.

Скупой платит дважды. Поэтому тут нужно в первую очередь тесно взаимодействовать с бизнесом. Составить дорожную карту, понять, какие системы придется замещать, что есть на рынке, либо заказать частную разработку. Также есть отраслевые сообщества, которые составляют единую дорожную карту, выбирают единого исполнителя и разрабатывают универсальное решение.

ОТКРЫТАЯ ПЕРСПЕКТИВА

КАК МЕЖСЕТЕВЫЕ ЭКРАНЫ ПОМОГАЮТ ПРЕДОТВРАТИТЬ ВЗЛОМ КОМПАНИИ



Дмитрий ХОМУТОВ
директор
ИТ-компания
Ideco

Межсетевые экраны являются одним из основных инструментов в обеспечении безопасности сетевых систем компаний. Они играют важную роль в предотвращении взломов и защите конфиденциальности данных. Какова ситуация на этом рынке? Как работают российские решения? По просьбе BIS Journal рассказывает Дмитрий Хомутов, директор ИТ-компания Ideco.

НА РЫНКЕ СТРЕМИТЕЛЬНЫЙ РОСТ

Основная функция сетевого экрана заключается в обеспечении безопасности компьютерных сетей или отдельных узлов путём предотвращения несанкционированного доступа. Более того, сетевые экраны часто называются фильтрами из-за своей основной задачи — фильтрации и блокировки пакетов, которые не соответствуют критериям, установленным в конфигурации.

По данным исследования Центра стратегических разработок (ЦСР)¹, в конце 2022 года объём российского рынка продуктов и услуг в сфере информационной безопасности достиг 193,3 млрд рублей. В 2021 году этот показатель был ниже на 4%. Согласно данным, объём продаж средств

защиты информации в 2022 году составил 143 млрд рублей, что составляет около 74% от общего объёма рынка. В то же время доходы иностранных производителей составили 43 млрд рублей, что составляет примерно 30% от общего объёма рынка. Специалисты исследования прогнозируют, что тенденция, наблюдавшаяся в 2023 году, будет продолжаться, и клиенты в секторах B2G и B2B будут расходовать практически все свои бюджеты на продукцию отечественных поставщиков, что позволит этой части рынка вырасти в четыре раза. Аналитики из Центра стратегических исследований (ЦСИ) прогнозируют, что к 2027 году доля российских производителей на рынке составит 531 млрд рублей.

Развитие отечественных решений дополнительно связано с реализацией указа Президента Российской Федерации № 250 «О дополнительных

¹ https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_рынок_России



Аналитики из Центра стратегических исследований (ЦСР) прогнозируют, что к 2027 году доля российских производителей на рынке составит **531 млрд рублей**

первом полугодии 2023 года эта сфера теперь составляет 6% от всего рынка молодых компаний. По данным за 2023 год от газеты Коммерсантъ², наибольшее количество стартапов в России запускаются в сфере FinTech — 15,6%, и ещё 11,9% приходится на проекты в области медицины и здоровья. По данным Venture Guide³, за июнь 2023 года объём сделок в сфере кибербезопасности составил 3,55 миллиона долларов.

В сегодняшней геополитической обстановке возникло повышение спроса на российское программное обеспечение, поскольку многие иностранные поставщики покинули российский рынок. Кроме того, заметно увеличилось число атак на российские компании и государственные организации. Это требует дополнительных мер по обеспечению информационной безопасности.

КАК РАБОТАЕТ UTM МЕЖСЕТЕВОЙ ЭКРАН

Межсетевые экраны выполняют роль фильтра, проверяя весь сетевой трафик, проходящий через них, и блокируя нежелательный или потенциально опасный трафик. Они позволяют определить правила доступа для каждого пользователя или устройства, что позволяет разграничить уровни доступа и обеспечить безопасность системы. Многие межсетевые экраны имеют встроенную поддержку виртуальных частных сетей (VPN), что позволяет обеспечить безопасное удалённое соединение с сетью

компаний. Это особенно важно для сотрудников, работающих из дома или в пути, и позволяет им безопасно и надёжно обмениваться конфиденциальной информацией. Это позволяет предотвратить вторжение злоумышленников в сеть компании и защитить её от вредоносных атак.

UTM работает на сетевом уровне и анализирует каждый пакет данных, проходящий через него. Он использует различные методики фильтрации, такие как контроль состояния, сигнатурное обнаружение, блокировка по IP-адресам и портам, а также белые и чёрные списки. Угрозы в сети могут быть обнаружены с использованием системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). IDS анализирует сетевой трафик и ищет сигнатуры атак, а IPS может принять меры по блокировке или предотвращению этих атак.

ОТКРЫТАЯ ПЕРСПЕКТИВА

Межсетевые экраны являются неотъемлемой частью комплексной стратегии безопасности сети компании. Их правильная настройка и использование помогут надёжно защитить компанию от взлома и утечки данных, обеспечивая сохранность информации и доверие клиентов. В целом развитие межсетевых экранов в России продолжается, и ожидается дальнейший рост спроса на эти средства информационной безопасности. Национальные исследования и статистика свидетельствуют о растущем понимании и значимости обеспечения защиты компьютерных сетей в стране.

мерах по обеспечению информационной безопасности РФ». Этот документ меняет подход к обеспечению кибербезопасности на российских системообразующих и стратегических предприятиях, субъектах информационной инфраструктуры и государственных структурах. Согласно указу, полномочия по обеспечению информационной безопасности должны быть переданы заместителям руководителей организаций, что повышает уровень кибербезопасности в компаниях. Одновременно с этим руководители компаний будут нести личную ответственность за обеспечение информационной безопасности.

МНОГО СТАРТАПОВ

Такой интерес со стороны российских компаний на бесшовный переход увеличил количество стартапов, работающих в области кибербезопасности. Согласно данным MTS StartUp Hub, в

² <https://www.kommersant.ru/doc/6095776>

³ <https://secrets.tinkoff.ru/novosti/v-rossii-rezko-vyroslo-chislo-startapov-v-sfere-kiberbezopasnosti/>

ПЕРЕХОД НА РАМ

ЭКСПЕРТЫ ИБ О ПРИНЯТИИ РЕШЕНИЯ,
ПРЕДПОСЫЛКАХ ДЛЯ НЕГО И МИФАХ О РАМ



Филипп РУЖКОВСКИЙ

руководитель отдела информационной безопасности компании-интегратора, специализирующегося на работе с ГИС



Лев СЕМЁНОВ

руководитель ДИТ
АО «АТК «Ямал»

Актуальность вопроса обеспечения безопасности «чувствительных» данных в компаниях неуклонно растёт. Очень явно эта проблема обозначилась в свете увеличившейся популярности удалённой работы, которая при всём своём удобстве значительно усиливает риск возможных утечек.

Сейчас бизнес всё больше сосредотачивается на защите критически важных данных и применяет для этого разные организационные методы. Один из них — управление доступом сотрудников в корпоративные ИТ-системы и контролем за действиями, которые они в ней совершают.

Ведь часто конфиденциальные сведения «утекают» вовне из-за человеческого фактора, когда специалисты — штатные и особенно внештатные — не следуют простым правилам кибербезопасности: из-за своей невнимательности, некомпетентности или же ввиду спланированных злонамеренных действий.

Для предотвращения таких инцидентов и оперативного реагирования на них компании ищут инструменты, которые не только могут отслеживать действия пользователей, но и позволяют гибко управлять их привилегированными правами доступа. Мониторинг деятельности таких сотрудников — основная задача, которую решают РАМ-системы (Privileged Access Management), способные управлять и контролировать их учётные записи.

Но как бизнесу решиться перейти на такую систему? На каком этапе его развития это становится явной необходимостью? Об этом рассуждают эксперты ИБ: Филипп Ружковский и Лев Семёнов.

НУЖНО ВНЕДРЯТЬ РАМ

— На каком этапе ИБ-зрелости компании решение «можно внедрить РАМ» переходит в «нужно внедрить РАМ»?

Филипп Ружковский. РАМ, как и любое централизованное решение, позволяет автоматизировать тот или иной ИТ-процесс и при необходимости свести к минимуму участие в нём человека.

Когда рутинные операции, связанные с организацией доступа к критически важным данным корпоративных систем, требуют вовлечения в них на постоянной основе более одного ИБ-специалиста, возникает вопрос эффективности работы подразделения в целом. И тут значим не сам факт загрузки отдельно взятого сотрудника. Тут стоит обратить внимание на сами процессы: систематизацию предоставления доступа и контроль действий администраторов целевых систем. Зачастую важно не оценить их масштаб, а предотвратить — сработать на опережение, предугадать. В таких случаях РАМ-система является главным элементом kill chain для блокировки возможных нежелательных действий.

Также не нужно забывать про потенциальные киберриски при работе

с внешними подрядчиками: при передаче на их сопровождение инфраструктуры в целом или отдельных её подсистем. Потому что при расследовании ИБ-инцидентов, которые часто возникают именно по вине контрагентов, не последнюю роль играет то, что те или иные действия просто невозможно доказать. И тогда РАМ становится «судом последней инстанции» с объективной позицией. А в качестве «доказательной базы» приоритет отдаётся журналам сертифицированных средств защиты, поэтому выбор конкретного решения основывается и на этом факторе.

Лев Семёнов. Внедрять РАМ в компании нужно на этапе, когда в результате её роста для администрирования корпоративных систем требуется привлечь более одного сотрудника, зачастую — внешнего подрядчика, или распределять ответственность между несколькими штатными сотрудниками. И тут важен не столько уровень доверия к своему персоналу и подрядчикам, сколько необходимость в обеспечении контроля за его работой, чтобы, с одной стороны, защитить от подозрений, с другой — исключить возможность и желание обходить ИТ-систему. При этом, разумеется, в организации должен быть ИБ-специалист или наделённый его полномочиями сотрудник, иначе функциональность РАМ-системы будет востребована не полностью.

Как итог: внедрение необходимо для всех компаний при совмещении функций по обслуживанию систем

нескольким сотрудниками при наличии службы по информационной безопасности.

НЕОБХОДИМОЕ УСЛОВИЕ

— Есть ли какое-то условие для организации любой формы, некая условная точка в развитии её инфраструктуры, когда можно сказать: теперь вам точно нужен РАМ?

Филипп Ружковский. Конечно: это ИБ-зрелость компании, о которой многократно говорилось. А также — развитие бизнеса, его масштабы, конкретная деятельность, внутренние бизнес-процессы и т.д.

Также существуют и требования регуляторов в области защиты информации, регламентирующие удалённое администрирование компонентов критической информационной инфраструктуры (КИИ). Это особенно важно для крупного (и очень крупного) бизнеса с ориентацией на промышленное производство, госорганизаций. Поэтому для КИИ-субъектов этап «можно», как правило, отсутствует. Доступ к таким данным однозначно должен контролироваться специализированными средствами киберзащиты.

Лев Семёнов. Да, это точка роста критичности той или иной информационной системы, после достижения которой невозможно или сильно осложнено функционирование бизнеса без неё. Соответственно, возрастает степень понимания того, что необходимо обеспечивать «отказоустойчивость» не только в аппаратно-программном обеспечении, но и в отношении сотрудников, обеспечивающих работу системы. Это создаёт условия для размытия или перекладывания ответственности между людьми, даёт предпосылки для злоупотребления доверием, при котором уже нельзя обойтись без применения автоматизированных средств контроля.

ОБРАТИТЕ ВНИМАНИЕ

— На что нужно обратить внимание при выборе РАМ-системы в первую очередь?

Филипп Ружковский. На первом месте однозначно — надёжность решения. И речь тут, разумеется, не

Главный миф о РАМе в том, что можно обойтись в администрировании корпоративной сети без РАМ

столько о качестве аппаратных компонентов с точки зрения «железа», сколько об отказоустойчивости системы в целом, ведь она работает на сверхнагрузках. Также необходимо оценивать, каким образом разработчик реализовал резервирование информации на своём продукте и органично ли «вписывается» всё это в используемую в компании ИТ-архитектуру.

Второе место делят функционал и производительность. Я не могу точно сказать, что именно из этого важнее: всё зависит от сценариев использования РАМ, потому как ИБ-приоритеты бизнеса могут меняться, и это вполне нормально. Функциональные возможности системы, конечно, важны при базовом сравнении решений от различных вендоров, и на это обращают внимание в первую очередь. Однако вероятны ситуации, в которых целесообразно отказаться от условной «красоты интерфейса» в пользу возможности «переварить» лавинообразную нагрузку.

Очевидно одно: РАМ должен работать «на полную катушку» и реализовывать при обеспечении информационной безопасности весь свой функционал в полной мере.

Лев Семёнов. Я скажу про наш конкретный опыт. Когда мы выбирали систему контроля действий привилегированных пользователей, в частности, помимо основных функциональных возможностей РАМ-решений мы ориентировались в первую очередь на возможность автоматизированного анализа сессии, чтобы снизить нагрузку на ИБ-специалистов, проверяющих сотрудников.

МИФЫ О РАМ

— По вашему мнению, какой главный миф о РАМ-системах, ко-

торый сложился сегодня в профессиональной среде?

Филипп Ружковский. Внедрение любой серьёзной (и, безусловно, дорогой!) системы зачастую создаёт у руководства компании и даже профильных сотрудников иллюзию абсолютной защищённости. Однако это не всегда так.

Не открою Америку, если скажу, что любое средство киберзащиты требует в первую очередь грамотной команды экспертов и технических специалистов, которая должна обеспечивать её слаженную и бесперебойную работу. Заплатить интегратору большие деньги за внедрение бывает недостаточно: необходимо развивать внутренние компетенции персонала для совершенствования всего цикла защиты информации в организации.

Лев Семёнов. Что можно обойтись в администрировании корпоративных систем без РАМ.

ДО РАМ

— Какое решение до внедрения РАМа закрывало задачи по организации доступа?

Лев Семёнов. Доверие к администраторам. Всё остальное не про организацию безопасного доступа, а про технологию, а тут, конечно, всё как у всех: VPN, RDP, SSH и прочие. А если говорить про безопасное администрирование систем, то остаются только РАМ или доверие. Сотрудников и подрядчиков, обеспечивающих работу информационных систем, у нас достаточно. Для авиакомпаний ключевым является обеспечение безопасности полётов, вопросы информационно безопасности являются частью этого большого процесса, поэтому мы и приняли для себя решение о внедрении продукта данного класса.



ПЯТЬ ВОПРОСОВ

ПЕРЕД ТЕМ, КАК СФОРМУЛИРОВАТЬ СТРАТЕГИЮ
ОТРАСЛИ ЭП



Дмитрий ДУБЫНИН

директор Департамента развития технологий цифровой идентификации Минцифры России, модератор ключевой дискуссии «21 год законодательству об ЭП»

В 2023 году исполнился 21 год законодательству об электронной подписи (ЭП). За это время многое сделано и участниками рынка, и регуляторами. Отрасль понимает, что эта тема в России будет

развиваться и дальше. Но есть и насущные вопросы, которые необходимо обсуждать и решать. Например, возникла потребность в пересмотре стратегии отрасли: инструментов, сервисов, среды доверия, обеспечения

безопасного и удобного применения электронных документов. О том, из чего бы могла состоять новая стратегия, говорили участники прошедшей в Санкт-Петербурге XXI международной конференции по проблематике инфраструктуры открытых ключей и электронной подписи «PKI-Форум Россия 2023».

При подготовке Ключевой дискуссии «21 год законодательству об ЭП: текущие достижения, направления и стратегия развития», мы понимали, что каждая отрасль имеет свои направления развития, но при этом стратегии как правило универсальны и включают три аспекта:



- ♦ создание безопасной современной инфраструктуры;
- ♦ создание безопасных и доверенных сервисов, которые необходимо внедрять в правоотношения с гражданами;
- ♦ кадровые вопросы.

Но, прежде чем говорить непосредственно о стратегии, участники ключевой дискуссии обсудили вызовы и проблемы, с которыми отрасль сталкивается постоянно. Были сформулированы пять вопросов.

ВОПРОС ПЕРВЫЙ:

Отрасль не понимает тактики и стратегии регулятора. Что с этим делать?

Вячеслав Бражко, начальник Управления режима секретности и безопасности информации, Федеральное казначейство:

— Мы не решили вопросы, прописанные в 63-ФЗ «Об электронной подписи». Наверное, это больше вопрос

к Минцифре, но мы не видим результатов действия этого закона. С точки зрения Федерального казначейства, стратегия есть: увеличено количество действующих сервисов, происходит улучшение их качества и стабилизация работы отдельных сервисов. В настоящее время наблюдается тенденция увеличения как числа цифровых сервисов у государственных органов, так и объёма запрашиваемых сертификатов. Стратегически нужно довести качество сервисов до приемлемого уровня.

Важным направлением будет дальнейший рост числа сервисов, и конечно, возвращение доверия населения. В этом и будет заключаться стратегия Федерального казначейства.

Александр Баранов, действительный член Академии криптографии РФ:

— Главная проблема — это действенность существующих правил. Нужно действовать в соответствии с законами, как они написаны, а не как их можно трактовать.

Вторая проблема — массовая информационная безопасность. Что такое электронная подпись? Тот же паспорт, который используется при подписании электронных документов. При этом ЭП лежит в открытом доступе на компьютере или телефоне и ничем не защищена. Уже были инциденты с незаконным использованием ЭП, их заблокировали, но могут возникнуть новые.

Стратегическая задача должна заключаться в сбалансированности применения ЭП в новых условиях с учетом требований информационной безопасности. Нужно оценить все риски. Это должны сделать и регулятор, и общественность.

Константин Дробаденко, представитель 8 Центра ФСБ России:

— Отсутствие понимания тактики и стратегии регуляторов характерно для всех отраслей во все времена. Положения, которые содержатся в законодательных актах, могут быть выполнены только при существовании механизмов, которые принесут прибыль участникам рынка. При этом последние, выполняя требования, будут развивать рынок дальше.

Мы движемся вперед, пытаемся расширить границы использования ЭП. Для этого нужно выводить на рынок новые сервисы, соблюдая баланс между ними и обеспечением ИБ. Этот баланс всегда находится вручную, конкретно для определенного сервиса.

Есть положения, которые до сих пор не заработали. В частности, институт доверенных лиц третьей стороны. Причина — отсутствие механизмов, стимулирующих развитие этого института.

Реализация законодательства — улица с двусторонним движением. Это и попытки регулятора оформить правилами определенные положения. И широкое информирование общественности, чтобы создать рыночные механизмы саморегулирования, которые позволят реализовывать эти положения. Конечно, есть определенные трудности при создании этих механизмов, но я бы не драматизировал ситуацию в области ЭП — положения приняты, должны появиться процессы, стимулирующие развитие ЭП. Если у регулятора что-то не получается, значит, положения будут меняться.

Фёдор Новиков, начальник управления ЭДО, ФНС России:

— Электронная подпись активно внедряется в различные сферы, в процесс вовлекаются новые люди. Мы даем возможность использовать инструмент в разных отраслях жизни. Обратная задача состоит в том, чтобы отрасль помогла нам ресурсами, знаниями, сервисами. Те решения, которые уже были приняты, необходимо интегрировать в повседневную жизнь граждан с должным уровнем безопасности.

Есть важные, но тяжелые решения, которые не могут быть реализованы простой или квалифицированной ЭП. Именно эти моменты нужно жестко регулировать, использовать более доверенные сервисы и продукты — решения, которые предстоит найти. Эту задачу нужно решать всем вместе, что мы уже и делаем.

Игорь Качалин, генеральный директор АНО «Национальный технологический центр цифровой криптографии»:

— Не всегда отрасль — объединение людей и организаций с разными



Константин Дробаденко (ФСБ России)

технологическими и бизнес-интересами — представляет себе развитие сервисов. Часто они вводятся в эксплуатацию без надлежащей проработки вопросов безопасности.

Этот момент требует законодательного и технического решений, усилий разных людей и организаций. Хотелось бы, чтобы появился некий перспективный план развития сервисов, на основе которого можно было бы заранее отрабатывать вопросы нормативного регулирования и стандартизации в области безопасности, которые легли бы в основу востребованных сервисов.

Дмитрий Гусев, заместитель генерального директора «ИнфоТеКС»:

— Как представитель разработчиков хочу отметить несколько проблем. Первая — отрасль с механизмами и решениями, которые обсуждаются, развиваются и реализуются. В этом движении она обогнала отрасль электронного документооборота, к которой теперь должны быть приложены все усилия.

Известны примеры, когда в простой структурированный документ должны быть внесены атрибуты ЭП, чтобы человек мог оперировать подписью. Эта простая потребность вызвала глобальное замешательство в сообществе. До сих пор не существует

окончательно принятого решения, хотя технически оно готово.

Отсутствие стандартизации структур и данных в большинстве отраслей является стопором развития экономики данных. В ней хорошо разбираются только глубоко погруженные специалисты. Эти сложные вопросы мы не сможем решить здесь и сейчас. Отсюда проистекает вторая проблема — проблема регулирования, определения правил, в рамках которых система может жить и развиваться. Любое предписание будет тормозить развитие системы. И эти две проблемы неотделимы друг от друга.

Необходимо понимание механики того, как исходные бумажные документы должны трансформироваться в электронные машиночитаемые документы, как должно выстраиваться регулирование. По этому вопросу предстоит дискуссия с представителями отраслевых институтов.

На практике мы сталкиваемся с тем, что подписанный регулятором документ порождает вопросы в области безопасности. Чем больше требований по ИБ, тем хуже они структурированы и тем менее детальная модель угроз выстраивается. Прикладная часть задачи перекладывается на плечи специалистов по ИБ, которые превращаются в технологов и расписывают бизнес-процессы предприятия.

ВОПРОС ВТОРОЙ:

Нормативное регулирование отстает от темпов развития технологий и потребностей рынка. Как изменить ситуацию?

Константин Дробаденко. Я бы вернулся в 2011 год, когда был принят 63-ФЗ «Об электронной подписи». Тогда в России было предложено ультралиберальное регулирование использования ЭП. Любой хозяйствующий субъект мог выполнить требования ч. 3 ст. 16 закона и стать аккредитованным центром, создавать и выдавать квалифицированные сертификаты.

Это было рискованное регулирование, но оно принесло больше пользы, чем вреда. Рынок активно развивался. Когда стало понятно, что отрицательные черты преобладают, понадобилось время, чтобы в 2019 году изменить парадигму.

Сейчас мы пытаемся выстроить сбалансированное регулирование. Но многие положения 2019 г. до сих пор не реализованы, например, сроки перехода на машиночитаемые доверенности (МЧД). Рынок воспринял эту идею и движется в нужном направлении. То есть тут нормативное регулирование даже обгоняет технологии: мы выдвинули положения и теперь пытаемся обеспечить их технологическое выполнение.

В целом же нормативное регулирование незначительно отстает от развития технологий и потребностей рынка, а иногда пытается направить развитие технологий для обеспечения интересов личности, общества и государства, что позволит в дальнейшем обеспечивать стабильное развитие ЭДО в стране.

Игорь Качалин. Если говорить про технические аспекты регулирования, то создание новых криптографических механизмов, обоснование их качества, стойкости и соответствия требованиям — сложный трудоемкий и наукоемкий процесс, требующий времени. Опыт ТК-26 показывает, что хорошо выверенный стандарт в области криптографии — это нескольких лет работы.

Даже имея базовые криптографические протоколы и механизмы,

построить на их основе новый протокол — трудоемкая задача, требующая обоснования правильности построения и выбора примитива. Поэтому тут всегда будет отставание от технологий и потребностей рынка.

Что можно сделать? Вовлечь в работу молодых специалистов.

Александр Баранов. Мы наблюдаем технический застой. Задача должна иметь комплексное решение, где главная проблема — увязать одно с другим. Это должно быть принципиально новое решение.

Дмитрий Гусев. Я развернул бы вопрос в другую сторону. Нормативные документы всегда отстают от темпов развития технологий. Если мы в федеральных законах и подзаконных актах уйдём от технических деталей и вынесем их в отдельный стандарт — это выход из ситуации. Но того, что делает ТК 26, мало, чтобы говорить о развитии полноценного ЭДО.

У нас есть технологический задел, но мешает отсутствие стандартов, выпущенных профессиональным сообществом. Стандарты рождаются в спорах между техническими экспертами и компаниями, которые понимают, как устроена начинка. Никакой законодатель или регулятор не сможет погрузиться так глубоко.

Мы знаем, как сделать ЭП, и уже сделали ее, она работает во множестве бизнес-кейсов и госсистем. Но мы ждем требований регулятора. Надо смотреть на эту проблему в другой плоскости и тогда появится решение.

ВОПРОС ТРЕТИЙ:

Длительные сроки оценки сертифицируемых решений. Как на это можно повлиять в текущих условиях? Какого результата ожидать при положительном исходе?

Дмитрий Гусев. Сроки оценки криптографических продуктов выливаются в месяцы, а то и больше года. Когда мы говорим о внедрении криптографических механизмов в прикладные ГИС, жизненные циклы разработки и согласования



Игорь Качалин (НТЦ ЦК)

совпадают. Но бизнес живет в другой парадигме: кто первый вывел решение на рынок, тот и получил прибыль. Бизнес не готов ждать согласования месяцами.

Проблема сроков согласования постоянно обсуждается на профильных конференциях и находит отклик у регулятора. Коллеги готовы рассматривать предложения без снижения или с контролируемым снижением уровня безопасности, чтобы бизнес мог принимать для себя решение, и он готов идти на риск. Каким образом? Оптимизируется существующий линейный порядок проведения оценки. Можно идти параллельным путем и интегрировать один процесс в другой — за процессом разработки СКЗИ и прикладной системы проводить оценку влияния или первичные исследования.

Здесь можно сослаться на опыт ФСТЭК и создания доверенного ядра Линукс на базе ИСП РАН. Эта работа уже ведется, в ней участвуют и компании, и исследователи. Совместными усилиями они создают доверенное ядро доверенного кода и свою базу,

которая может использоваться разработчиками прикладных систем, — чтобы они «с нуля» не проходили все процедуры проверки безопасности своих систем. Аналогично идет работа по программным компонентам, подключаются и разработчики аппаратных платформ, чтобы привнести доверенный драйвер для «железа» в общий список доверенного кода.

Это единственный вариант решения проблемы. Так можно достичь глубокого уровня контроля процессов разработки, решения проблем цепочек поставки и избежать внедрения закладок в OpenSource решения. Так сократится и срок согласования.

Фёдор Новиков. Специфика работы ФНС как госструктуры связана не только со скоростью получения сертифицированных решений, но и с привязкой к бюджетным циклам. Это параллельные проблемы.

Я разделяю мнение коллег, что бизнес страдает от недополучения прибыли. Для ФНС это становится проблемой недополучения налогов в казну. Мы заинтересованы, чтобы



Вячеслав Бражко (Федеральное казначейство)



Дмитрий Гусев (ИнфоТекС)

бизнес активнее внедрял новые решения, оптимизировал затраты и вкладывал средства в развитие.

Константин Дробаденко. Я бы хотел подчеркнуть сложность перехода. Оценка соответствия решений, по итогам которых выдаются сертификаты, — это опыт и требования, написанные поколениями криптографов и инженеров. Это статическая модель безопасности: мы выдвигаем требования и проверяем соответствие им.

Необходима смена парадигмы. Она должна быть проведена в строго определенных областях. Смена парадигмы связана с риск-ориентированным подходом. Можно обратиться к опыту западных стран, которые в области массовой криптографии ориентируются на такие подходы и на динамическую модель противодействия актуальным угрозам.

Это серьезная смена воззрений: должна быть наработана и методика, и опыт, который можно воплотить в методических документах. Это единственный путь, по которому мы можем идти от сертификации решений к сертификации процессов. Быстрого решения вопроса ожидать не стоит.

Александр Баранов. В чем разница требований ФСТЭК и ФСБ? Требования 8 Центра ФСБ техниче-

ские и количественные (вероятностные). А требования ФСТЭК в основном качественные. И попытка заменить качественные на количественные требования приводит к тяжелейшим решениям в оценке. Сертификация будет еще более сложной.

Это пытались сделать почти 20 лет назад, когда мы только начинали разворачивать ИБ. Проблема — ввести количественные характеристики всех требований. Спустя годы, сдвигов на этом направлении не наблюдается. Массовую ИБ надо делать удобной, легкой и масштабируемой, чего нельзя сказать о предлагаемом динамическом подходе.

Вячеслав Бражко. Подводя итоги, отмечу, что в госсекторе все протекает в плановом режиме, но в отдельных случаях хотелось бы сокращения сроков. Иногда госсектор формулирует эксклюзивные решения, требующих быстрых сертификационных мероприятий, часто это напрямую зависит от сформулированных угроз и моделей угроз. И тут важно говорить о сокращении сроков.

Почему я выступаю за идею сертификации производства? Это повысит массовость. Но в определенный момент мы столкнемся с антимонопольным законодательством. Тут нужна осторожность.

Необходимо формирование среды доверия больших платформ, которые позволят по ряду решений отказаться от сертификации определенных элементов. Хороший пример — сертифицированная в определенный момент версия ОС Windows.

ВОПРОС ЧЕТВЕРТЫЙ:

Корреляция между активным регулированием и технологическими возможностями. Пока воплощается замысел, нормы могут измениться. Как найти баланс?

Фёдор Новиков. Да, не всегда проблемы, которые прорабатывались на рабочей группе, на выходе соответствуют замыслу и проделанной работе.

Надо понимать, что государственные институты состоят из разных лиц, которые не всегда общаются с бизнесом. У нас есть практика сопровождения нормативно-правовых актов (НПА) на каждом этапе согласования, это минимизирует процент неожиданностей на выходе. Если со стороны органов власти есть заинтересованность, например, исполнение поручений, то в процессе принятия могут возникнуть сложности, поскольку участники процесса не оценивают все нюансы.

Чтобы в НПА вошли нужные нормы, при выработке решений бизнесу целесообразно создавать экосистему и сообща работать в ней с органами власти. Еще один аспект — участие доверенных лиц при обсуждении НПА, позиционирование бизнеса в госорганах, на мероприятиях, где обсуждаются нормативные акты. Часто в них участвуют одни лица, а претензии после высказывают другие. Необходимо внимательно подходить к тому, кто доносит позицию бизнеса до регулятора.

И делая отсылку ко второму вопросу, скажу, что лучшее регулирование идет после того, как решение сделано. Необходимо идти через механизм экспериментов и пилотных проектов, чтобы максимально комфортно реализовать все при наличии технологической возможности.

Вячеслав Бражко. Нормативные инициативы не могут появляться без технологической возможности. При реализации серьезной задачи сначала стоит вопрос технологической возможности, затем — нормативного регулирования. Иногда это приводит к необоснованному выбору технологических платформ. Но это лучше, чем неисполнение требований.

Как обеспечить корреляцию? Главное, при обсуждении НПА «не выплеснуть ребенка». При появлении технологической возможности необходимо сопровождение НПА, после этого отрасль получает законченное решение.

Регулятор абсолютно открыт, как уже говорили коллеги, есть масса площадок, на которых можно обсуждать. Пример удачного сотрудничества — обсуждение и внесение изменений в Федеральный закон «Об электронной подписи».

Дмитрий Гусев. Необходимо возвращение Госстандартов в рамки НПА и принятие закона «О техническом регулировании». Технологии должны идти впереди регулирования, они должны определять облик будущего законодательства, а не наоборот. Техническое регулирование — вопрос отрасли, а не законодателей.

Это важный момент, на который надо обращать внимание не только в приказах ФСТЭК, но и других регуляторов. Стандарты должны появляться в федеральных законах и подзаконных актах.

ВОПРОС ПЯТЫЙ:

Это вопрос встраивания в глобальное пространство доверия (на уровне стандартов, нормативов, технологий и на организационном уровне). Что мы можем сделать для ускорения этого процесса и повышения его эффективности?

Фёдор Новиков. В чем проблема работы с услугами доверия? По результатам получения услуг необходимо подтвердить деятельность при работе с контрагентами при обращении в суд или в рамках деятельности контрольных органов. В рамках межведомственного и трансграничного взаимодействия мы готовы к тому, что бизнес будет интегрироваться и работать с другими институтами. Мы готовы объяснять всем как работать, почему надо доверять сервисам и услугам. Государство сделало много, теперь бизнесу необходимо применять это на практике.

Константин Дробаденко. Вопрос встраивания в пространство доверия больше политический. А политические течения имеют больше значения, чем вопросы технические. Сегодня по многим направлениям работа ведется в рамках международных контактов, при этом технические вопросы остаются на втором плане. Необходимо выстраивать взаимоприемлемые отношения, разграничивать пространство доверия в рамках действующих договоров. Должна проводиться работа на технологическом уровне. Пример работы ФНС России в этом направлении показывает новые возможности и перспективы развития. Иных универсальных механизмов ускорения процесса нет.

Игорь Качалин. ТК 26 уже более 10 лет занимается международной

стандартизацией и ведет работу по внедрению в международные стандарты российской криптографии. Однако после февраля 2022 г. эта работа была прекращена.

За криптографические стандарты спокоен, но гармонизация стандартов приобрела однобокий характер. Появилась тенденция механического перевода иностранных стандартов, особенно в таких популярных областях как Искусственный интеллект или Интернет вещей, которые внутри содержат отсылки к иностранным стандартам и криптографии, требованиям безопасности без адаптации к российским требованиям. Таких стандартов принимается до сорока в год, очень странно делать их обязательными к применению.

Вячеслав Бражко. Для создания новых путей встраивания в глобальное пространство доверия есть два направления: либо принять чьи-то стандарты, либо заниматься экспансией свободных рынков. Для этого нужно заниматься разработкой и внедрением своих стандартов на свободные рынки, например, на уровне программных продуктов, как это ранее делали иностранные компании. Это можно сделать даже на уровне операционных систем со встроенными российскими криптографическими механизмами.

* * *

Подводя итоги дискуссии, участники отметили, что стратегия развития отрасли всегда есть, даже если она не оформлена на бумаге. Все акторы руководствуются стратегическими соображениями и требованиями регуляторов. При формализации документа необходима стратегия развития сервисов, к которым должны пристраиваться вопросы обеспечения безопасности. При этом стратегия должна быть живой и обсуждаться широким кругом участников. Главное — не возводить ее в ранг догмы, чтобы она не довлела над развитием отрасли.

XX МЕЖДУНАРОДНЫЙ БАНКОВСКИЙ ФОРУМ

СЕССИЯ «КИБЕРБЕЗОПАСНОСТЬ В НОВЫХ РЕАЛИЯХ:
ЗАЩИЩЕННЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ
И КВАНТОВЫЕ ТЕХНОЛОГИИ»

Анна КАТАНКИНА
корреспондент BIS Journal

Деловую часть XX Международного банковского Форума в Сочи открыла сессия «Кибербезопасность в новых реалиях: Защищенный искусственный интеллект и квантовые технологии». Модератор дискуссии Артем Калашников, Газпромбанк, предложил поговорить об опыте использования ИИ в банковской сфере, его перспективах и роли в сфере ИБ.

ИИ ПОМОГАЕТ

Начавший дискуссию руководитель кибербезопасности АО «НСПК» Артём Гутник отметил высокий уровень цифровизации России. Он считает, что сфера применения ИИ также широка. Он зарекомендовал себя в тех системах, где необходимо аккумулировать большое количество разных признаков, в том числе в области ИБ. В целом ИИ это довольно крупная область новых технологий. Элементы ИИ уже не первый год используются в банковской сфере, например, machine learning, что позволяет строить прогнозы и выпускать новые достойные продукты, отметил А. Гутник.

«ИИ помогает правильно выстраивать безопасность. Например, в антифрод ИИ довольно успешно может прогнозировать поведение пользователей и в случае его отклонения от браковывать транзакцию».

При этом, как и любая технология, ИИ может использоваться как во вред, так и во благо. «Например,

использование цифровых двойников, которые совсем недавно появились и всё больше охватывают мир. Злая часть цифрового двойника это deepfake, который тоже существует и его становится всё больше». Поэтому, несмотря на огромную пользу, которую приносят новые технологии, относиться к ним нужно осторожно, подвел итог А. Гутник.

ИИ — ЭТО ПУЗЫРЬ

Эмоциональное выступление президента АО «Крибрум» Игоря Ашманова охватило широкий круг вопросов. Эксперт подробно остановился на рисках использования ИИ. «Искусственный интеллект — новый пузырь со всеми его признаками, третий в моей многолетней практике», заявил спикер. — «Его раздувают журналисты, инвесторы, маркетологи и некоторые банкиры». ИИ — любая программная система, имитирующая когнитивные функции человека. Это не обязательно machine learning, это и алгоритм Т9 и даже калькулятор. Единственный в мире искусственный интеллект — сам человек. В него ИИ заложен учителями и средой.

Игорь Ашманов отметил, что банки активно используют ИИ. Например, технология применяется в работе чат-ботов для снижения нагрузки на контакт-центры, для систем скоринга, систем обнаружения нарушения закона 115-ФЗ и т.д.

«Можно было бы думать, что всё хорошо, банки внедряют ИИ, значит, они инновационные. Но если брать по концовке — всю цепочку — то за последние 2–3 года у граждан украли сотни миллиардов рублей с помощью банков. Поэтому сказать, что там сделана система безопасности, которая это предотвращает,

нельзя», сказал Игорь Ашманов. Он считает, что генеративные системы ИИ, построенные с помощью машинного обучения на больших языковых и графических моделях и внедряемые банками, — дань моде и рациональные соображения.

«Банк, который гонится за статусом инновационного и бешено внедряет ИИ, притворяется ИТ-компанией, превращается в посредственную ИТ-компанию. Банк зависит от лицензии, он ограничен требованиями регулятора, — считает И. Ашманов. — Средний банк, который берется за разработку ИИ, не может конкурировать с зарплатами ИТ-компаний и технологических гигантов. Значит, он нанимает специалистов среднего уровня для разработки посредственных продуктов вместо того, чтобы заниматься финансовыми продуктами». История банка как экосистемы — странная, продолжил докладчик. Он полагает, что для экосистемы нужны другие элементы ДНК, иные подходы к B2C, которых в банке ни у кого нет.

И. Ашманов полагает, что ИИ в России — бутафория, поскольку сборка систем ИИ ведется путем крупноузловой сборки на основе западных движков, а отечественных разработок ИИ практически нет. Причем за основу моделей берутся устаревшие версии ИИ, которые западные технологические компании выкладывают для обучения и привлечения специалистов, а отечественные разработчики лишь активно скачивают их в собственных целях. Эксперт отметил отсутствие реальных компетенций у сборщиков таких систем, которые не понимают всех рисков и угроз, они скачивают чужие обновления и датасеты для обучения, хотя в них



часто заложены ошибки. Скачанные open-source нейронные библиотеки и фреймворки содержат многочисленные вкладки, считает И. Ашманов.

Использование открытого ПО — это высокий риск, включая угрозы нулевого дня, продолжил И. Ашманов. Он напомнил про недавнюю утечку данных из облачного хранилища репозитория AI GitHub компании Майкрософт. «Такие истории будут происходить всегда», напомнил докладчик. Он обратил внимание, что система, построенная на основе глубоких нейронных сетей и больших данных, представляет собой «черный ящик», контроль за которым невозможен. «Мы не знаем, как принимается решение, невозможно пройти в отладчик в отличие от систем, построенных на правилах, — отметил эксперт. — Даже разработчик общается с большой системой как с «черным ящиком»».

Игорь Ашманов подчеркнул, что контроля за ИИ нет, потому что нет критериев, в т.ч. критериев корректности. Например, понятно, что такое хороший чат-бот и что он должен, однако чего он не должен делать — неизвестно. Эксперт отметил, что Технический комитет по стандартизации № 164 «Искусственный интеллект» (ТК 164) занимается разработками стандартов ИИ, безопасности и функциональной корректно-

сти. В июле 2023 г. были приняты 50 стандартов, по большей части они охватывают области медицины и создания БПЛА, вводят термины и понятия. Однако критериев безопасности в них нет.

Эксперт привел многочисленные примеры некорректной работы скоринговых систем или чат-ботов, в результате действий которых нарушаются права человека. Например, он не может выйти на связь с оператором банка или оспорить решение ИИ, на основании которого была отклонена заявка на кредит. «Это риски для репутации и удар по банковской лояльности», считает И. Ашманов, поскольку не прошли годы, чтобы понять верность принятого ИИ решения и накопить нужный опыт. Есть примеры и нового типа сговора, в результате которого корректируются критерии запроса и клиент получает положительный ответ ИИ. Таким образом, снимается и размывается ответственность разработчиков системы, эксплуатантов и сотрудников финансовых организаций.

Завершая выступление, И. Ашманов отметил, что сегодня биометрические данные не защищены должным образом и, в отличие от персональных данных, их невозможно сменить. При этом модели угроз меняются с мошенничества на терроризм. Поэтому любая утечка данных

представляет смертельную угрозу, особенно на фоне отсутствия закона об оборотных штрафах за утечки персональных данных. Эксперт полагает, что перед банками стоит риск выбора неверных приоритетов, сейчас «много пустых обманок и фальшивых целей». «Основной риск — усиленная цифровизация банков, и этот уровень стоит понижать», полагает эксперт.

СВОИХ ТЕХНОЛОГИЙ НЕ ХВАТАЕТ

Константин Панцеров (СПбГУ) во многом согласился с И. Ашмановым. Он отметил, что ИИ — группа технологий, которая способна имитировать действия человека, решать задачи. Бум ИИ начался с 2010-х гг. и связан с глубинным обучением. Многие развивающиеся страны предположили, что с помощью ИИ они способны решить свои проблемы и ускорить социально-экономический рост. Эксперт подчеркнул, что с 2018 г. более 30 стран мира приняли стратегии развития ИИ на государственном уровне и придают его развитию большое значение. Не осталась в стороне и Россия. У нас активно развиваются голосовые чат-боты, кредитный скоринг, ведутся исследования в сфере эмоционального ИИ с целью оценки эмоций клиентов банков. Однако повсеместное применение ИИ создает трудно прогнозируемые

угрозы. Необходимо повышать уровень ИБ, учитывая, что разработки технологий ИИ идут впереди, а после над ними надстраиваются процессы ИБ.

«В основном мы работаем на основе западных фреймворков», отметил К. Панцеров. Отечественные специалисты оттачивают мастерство на западных open source платформах, своих технологий не хватает. Для развития отечественных систем ИИ, укрепления суверенитета, необходимы финансовые средства и технические решения. Нейронные сети требуют мощной материально-технической базы при разработке и обучении ИИ с нуля. Далеко не каждая компания может иметь такое оборудование, полагает эксперт. Нужны ИИ-лаборатории для разработки отечественных решений, расширение и создание собственных датасетов, что скажется на ИБ компаний и России в целом, считает докладчик.

Несмотря на трудности, объем российского рынка ИИ сейчас стабильно растет, в 2022 г. он составил 650 млрд рублей. Планируется, что к 2025 г. ИИ принесет российским компаниям порядка 1 трлн рублей. Правительство России разрабатывает новую стратегию развития ИИ до 2030 г. и планирует вложить в него значительные средства.

ИДЁМ В НОГУ

Вторую тему сессии — квантовые технологии осветил Антон Гугля (QApp) в докладе «Квантово-устойчивая защита данных финансовой отрасли». Он отметил активное развитие квантовых технологий и создание нового класса устройств. Квантовые компьютеры созданы в России и мире. Отечественный 16-кубитный квантовый компьютер сегодня решает неиндустриальные задачи. В мире есть техникакратно мощнее. Квантовые компьютеры могут применяться бизнесом для вычислений, моделирования сложных систем для решения разных задач. Их необязательно покупать — многие компании предлагают облачный доступ для вычислительных экспериментов.

Квантовые угрозы — это новые риски, при которых злоумышленник

будет использовать квантовый компьютер для атаки на традиционные системы защиты данных, в т.ч. для перехвата данных с длительным жизненным циклом и их расшифровкой в будущем.

Эксперт отметил, что ведущие мировые державы включают квантовые угрозы в стратегии ИБ и начинают апробацию квантово-устойчивых решений. В частности, в стратегию нацбезопасности США добавлена квантовая угроза. В России этими вопросами занимается ТК 26 и его профильные подгруппы, поскольку ценные данные требуют защиты новыми инструментами.

Существуют два технологических подхода к вопросу: программный и аппаратный. В России уже есть опыт по апробации квантовых коммуникаций и постквантовых технологий и криптографии, квантово-устойчивой защиты каналов передачи данных. Работу в этих областях ведут и некоторые вендоры. По мнению спикера, «квантовая угроза — фундаментальная история». Банки должны заранее думать и прорабатывать эти риски и включать их в карты угроз.

Отвечая на вопросы, спикер отметил, что по уровню развития квантовых компьютеров и их мощностей, Россия отстает от мировых тенденций на 7–10 лет. «Однако в направлении криптографии и постквантовых решений идем ногу с мировыми разработчиками», — сказал А. Гугля.

ИИ В РОЛИ ОПЕРАТИВНИКА

Никита Преснухин (PlainChain) рассказал о положительном опыте использования технологий ИИ при работе с криптоактивами и ЦФА. Он отметил, что блокчейн технологии перерабатывают огромный массив данных и транзакций. И если компания хочет быть агрегатором данных, ей на помощь приходит ИИ. В частности, технологии искусственного интеллекта активно применяются при анализе данных для противодействия отмывания средств (ALM), идентификации клиентов криптовалютных сервисов (KYC) в соответствии с актуальными требованиями регуляторов. ИИ помогает при обнаружении незаконной деятельности,

на лету считывает IP-адреса и подсети IP-адресов подозрительных кошельков. Также ИИ собирает сопутствующую информацию о владельцах кошельков, которые замечены в неправовом поле. По мнению эксперта, отсутствие регуляторов в вопросах ИИ — важный момент, требующий скорейшего изменения.

ПРО КАДРЫ

Где же взять кадры в области ИИ и квантовых технологий? По мнению участников сессии, кадрового голода в отрасли нет. Игорь Ашманов отметил, что после событий февраля и сентября 2022 г. из страны уехали 3–5% ИТ-специалистов. Однако идет большое сокращение непрофильных проектов в банковских экосистемах. По данным АРПП «Отечественный Софт», вакансии ИТ-специалистов быстро заполняются. Еще один важный аспект для привлечения квалифицированных айтишников — достойный уровень оплаты труда.

По мнению Константина Панцерева, подготовка кадров для ИИ — серьезная проблема, потребуются в 6–8 раз больше специалистов, и спрос на них будет расти. Кадровый голод наблюдается и в отрасли ИБ. При этом эксперт из СПбГУ отметил, что в стране действует 85 программ магистратуры в области ИИ и 21 программа бакалавриата. Многие программы открыты в непрофильных гуманитарных и нетехнических вузах, что должно оказать положительное влияние при подготовке специалистов, понимающих специфику отрасли.

Завершая дискуссию, модератор Артем Калашников отметил, что несмотря на многочисленные риски разработки и применения ИИ в банковской сфере, работы в этом направлении активно ведутся, в т.ч. с применением современных блокчейн- и квантовых технологий, методов криптографии. Применение и развитие ИИ во многом будет зависеть от индивидуальной оценки, а вопросы регулирования ИИ — тема, которая достойна отдельной сессии.

ТОП-10 API SECURITY RISKS 2023

УГРОЗЫ БЕЗОПАСНОСТИ API И МЕРЫ ПО ЕГО ЗАЩИТЕ НА ОСНОВЕ OWASP



Сергей БОРИСОВ
ведущий специалист
отдела стандартов ИБ VK

Цифровизация бизнеса и необходимость постоянной интеграции привели к тому, что API (программные интерфейсы приложений) стали жизненно важным компонентом информационных систем, которые обеспечивают сквозное взаимодействие и обмен данными между различными сервисами. Широкое использование API сделало их одной из основных целей кибератак, подвергая компании рискам утечки данных, несанкционированного доступа и недоступности ключевых систем для клиентов. И по некоторым прогнозам этот тренд будет только усиливаться: API Statistics (Statista) предсказывает в ближайшие 4 года увеличение количества вызовов в 5 раз.

В 2019 году в целях повышения осведомлённости по вопросам безопасности API-проект Open Web Application Security Project (OWASP) определил в документе перечень наиболее опасных угроз (Top 10 API Security Risks). На основе анализа данных с различных площадок Bug Bounty и публичных инцидентов в 2023 году был существенно обновлён перечень наиболее актуальных трендов и угроз. Изменения коснулись популярности некоторых протоколов API,

появления новых методов и техник их компрометации, а также новых способов защиты.

ЧТО ПОМЕНЯЛОСЬ В 2023 ГОДУ

Самой значимой проблемой остаётся авторизация. Три пункта наиболее опасных угроз связаны именно с уязвимостями механизмов авторизации и управлением доступом. Современные приложения на основе API становятся всё более сложными — с тысячами конечных точек и бесчисленным количеством параметров. Когда в эту запутанную сеть добавляется иерархия пользователей и организаций, то становится сложно понять, кто и к чему в действительности имеет доступ.

Также стоит отметить появление новой угрозы Unrestricted Access to Sensitive Business Flows, реализация которой из-за недостаточной проработки или ошибок в логике критических технологических цепочек бизнес-процессов приводит к возможности выполнения мошеннических операций. Это в очередной раз подчёркивает важность не только безопасного кодирования, но и планирования и проектирования безопасной архитектуры приложений. Поскольку API-интерфейсы обеспечивают лёгкий доступ для ботов, крайне важно определить критичные потоки данных и выбрать соответствующие меры защиты для них.

Подделка запросов на стороне сервера (SSRF) также была добавлена в список актуальных угроз. Хотя SSRF не является новой уязвимостью, в настоящее время она стала более распространённой именно в приложениях на основе API. Популярность веб-хуков упростила

хакерам использование уязвимостей SSRF. Кроме того, REST API-интерфейсы для управления и контроля облачных сервисов, K8S и Docker также упрощают эксплуатацию уязвимостей.

ТОП-10

Общий же перечень OWASP Top-10 API Security Risks 2023 выглядит так:

API 1: 2023

Broken Object Level Authorization

API обычно представляют конечные точки, которые обрабатывают идентификаторы объектов, создавая широкую поверхность атаки на контроль доступа на уровне объектов. Проверки авторизации на уровне объектов должны быть предусмотрены в каждой функции, которая получает доступ к источникам данных, используя идентификатор пользователя.

API 2: 2023

Broken Authentication

Механизмы аутентификации часто реализуются некорректно, что позволяет злоумышленникам компрометировать токены аутентификации или использовать ошибки реализации, чтобы временно или постоянно выдавать себя за другого пользователя. Компрометация способности системы идентифицировать клиента/пользователя подрывает безопасность API в общем случае.

API 3: 2023

Broken Object Property Level Authorization

Эта категория объединяет API3:2019 Excessive Data Exposure и API6:2019 — Mass Assignment, фокусируясь на первопричине — отсутствии или неправильной проверке авторизации на

уровне свойства объекта. Это приводит к раскрытию информации или несанкционированным манипуляциям ею.

API 4 : 2023

Unrestricted Resource Consumption

Обработка API-запросов требует ресурсов на уровне сети, вычислительных мощностей, оперативной памяти и места для хранения данных. Эти и другие ресурсы системы, например, отправленная электронная почта / SMS / телефонные звонки или выполненные проверки биометрических данных, предоставляются поставщиками и оплачиваются за каждый запрос. Успешные атаки могут привести к отказу в обслуживании или увеличению операционных затрат.

API 5 : 2023

Broken Function Level Authorization

Сложные политики контроля доступа со сложной иерархией, структурой групп и ролей, а также неясным разделением между привилегированными и обычными функциями часто приводят к ошибкам авторизации. Злоумышленники могут получить доступ к ресурсам других пользователей и/или административным функциям, эксплуатируя эти недостатки.

API 6 : 2023

Unrestricted Access to Sensitive Business Flows

API, уязвимые для этого риска, задействованы в критических технологических цепочках, обеспечивающих бизнес-процессы продукта. Они предполагают возможность фрода, например, при покупке билета или публикации комментария, без учёта того, как злоумышленники могут использовать эти функции в автоматическом режиме для извлечения прибыли и нанесения вреда бизнесу. Это может происходить не только из-за ошибок в реализации, но и из-за ошибок в логике. Также сюда можно отнести ситуации, когда разработчики рассчитывают, что пользователь пойдёт по цепочке API1 > API2 > API3 > API4, но не объединяют это в одну

целостную транзакцию. В итоге это может привести к тому, что злоумышленник может сразу прийти в API4, чтобы получить тот же результат.

API 7 : 2023

Server-Side Request Forgery

Угрозы подделки запросов на стороне сервера (SSRF) могут возникать, когда API запрашивает удалённый ресурс URI, предоставленный пользователем без проверки безопасности. Это позволяет злоумышленнику заставить приложение отправить специально подготовленный запрос на внешний сервер, даже если этот трафик запрещён на межсетевом экране.

API 8 : 2023

Security Misconfiguration

API и системы, обеспечивающие их, обычно содержат большое количество настроек, предназначенных для увеличения гибкости. Разработчики и DevOps-инженеры могут допустить ошибки в этих конфигурациях или не учесть лучшие практики безопасности при их конфигурировании, оставляя возможность для дальнейших атак.

API 9 : 2023

Improper Inventory Management

API обычно публикуется на большем количестве конечных точек, чем традиционные веб-приложения, поэтому корректная и актуальная документация является крайне важной. Также важна инвентаризация конечных точек и развёрнутых на них версий API для своевременного обнаружения недостатков, связанных с устаревшими версиями API или раскрытием отладочной информации.

API 10 : 2023

Unsafe Consumption of APIs

Разработчики склонны доверять данным, полученным из сторонних API, больше, чем пользовательскому вводу, и поэтому, как правило, применяют менее строгие контроли. Чтобы скомпрометировать API, злоумышленники могут атаковать сторонние сервисы вместо того, чтобы пытаться напрямую скомпрометировать целевой API.

ЗАЩИТА API

ГЛАЗАМИ OWASP

Фреймворк Top 10 API Security Risk не только перечень актуальных рисков для API компании, но и методологическая основа для их анализа, митигации и внедрения риск-ориентированного подхода. У каждого риска присутствует ряд важных атрибутов.

- ◆ Threat agents/Attack vectors — определение источника угрозы или вектора атаки.

- ◆ Security Weakness — описание недостатков, которые могут быть использованы.

- ◆ Impacts — предположения о возможном вреде, который может быть нанесён организации в результате реализации риска.

- ◆ Is the API Vulnerable? — описание признаков, которые позволяют определить, уязвимо ли API.

- ◆ Example Attack Scenarios — детальные примеры сценариев атак, основанные на реальных кейсах.

- ◆ How To Prevent — практики и меры безопасности, которые помогают предотвращать атаки и митигировать риски.

- ◆ References — ссылки на подобные уязвимости, утечки и рекомендации по защите.

Идентификация рисков является лишь первым шагом, после которого экспертная команда безопасности должна определить уязвимые API и приоритетные меры по их защите. Фреймворк имеет потенциал использования в качестве доверенного источника знаний для команды разработки, администрирования, мониторинга и реагирования на инциденты. Они могут использовать его, например, в качестве чек-листа по защите.

OWASP предлагает следующие практики — рис. 1.

Но самым важным результатом использования данного фреймворка стоит считать повышение осведомлённости в области защиты веб-приложений. Полноценная митигация угроз API невозможна без повышения уровня зрелости процессов безопасной разработки приложений, а также общей культуры ИБ в организации.

Конечно, фреймворки OWASP никогда не были пошаговой инструкци-

Практика	Описание
Authentication	Проверка подлинности пользователей, обращающихся к API
Authorization	Определение прав и полномочий пользователей
Data Redaction	Скрытие, маскировка или обезличивание конфиденциальных данных
Encryption	Шифрование данных и контроль прав при расшифровке
Error Handling	Безопасное управление ответами об ошибках или проблемах, позволяющее избежать раскрытия конфиденциальных данных
Input Validation & Data Sanitization	Проверка входных данных от пользователей и удаление вредоносных частей
Intrusion Detection Systems	Мониторинг аномальной сетевой активности
IP Whitelisting	Формирование перечня доверенных IP-адресов, с которых возможно обращение к API
Logging and Monitoring	Постоянный мониторинг и детальное логирование обращений к API
Rate Limiting	Ограничение частоты обращений пользователей и объёма передаваемых данных для предотвращения отказа в обслуживании
Secure Dependencies	Проверка отсутствия уязвимостей в используемом стороннем коде
Security Headers	Повышение безопасности front-сервисов против таких типов атак, как XSS
Token Expiry	Ограничение жизни токенов доступа и их регулярное обновление
Use of Security Standards and Frameworks	Определение и совершенствование стратегии безопасности API
Web Application Firewall	Защита веб-приложений от специфических атак на прикладном уровне
API Versioning	Одновременная поддержка нескольких версий API для возможности их непрерывного обновления

Рисунок 1. OWASP предлагает следующие практики

ей для построения безопасного продукта или API. OWASP агрегирует актуальную информацию и подаёт её в виде удобных справочников, поэтому он так популярен в ИТ-сообществе. За каждой приведённой практикой стоит множество нюансов, о многих из которых не получится узнать из открытых источников. Это обуславливает ценность именно опытных специалистов в области ИБ, кото-

рые могут вовремя отследить риски безопасности и грамотно применить необходимые инструменты и практики.

Надёжная безопасность API – это уже фундаментальная необходимость, тренд, к которому должны быть готовы специалисты

ИТ- и ИБ-индустрии. Проблемы с безопасностью API могут иметь далеко идущие последствия, оказывая негативное влияние не только на прибыль, но и клиентскую лояльность. Поэтому организации должны применять проактивный подход к отслеживанию угроз и поиску новых инструментов защиты, проводить регулярные аудиты и тестирования.

ПОД НАЗВАНИЕМ NGFW...

ЗАХВАТЫВАЮЩИЙ СЮЖЕТ НА ОТЕЧЕСТВЕННОМ РЫНКЕ ИБ



**Марина
БРОДСКАЯ**
обозреватель
BIS Journal

Тема межсетевых экранов нового поколения, поднятая Денисом Батранковым в статье «Что такое NGFW. Недавние конкуренты вместе создают новые продукты для защиты страны»¹ неожиданно, но в то же время и ожидаемо стала лейтмотивом в отечественной ИБ 2023 года. По крайней мере, в части развития новых программно-аппаратных комплексов (ПАК). И если одни производители смело вышли к потребителям с рассказом «да у нас такое есть давно, мы просто называли его иначе», другие аккуратно назвали продукцию «межсетевым экраном или универсальным шлюзом безопасности» с или без уточнения версии поколения, а кто-то объявил, что начал разработку собственно NGFW на базе ранее созданных продуктов. Не остались равнодушными к популярной у производителей и потребителей теме фаерволов и регуляторы. Но по порядку...

РЕГУЛЯТОР

Есть ли у нас свои NGFW? Отвечая на этот вопрос в мае на PHDays 2023, представитель ФСТЭК Рос-

сии В. С. Лютиков уклончиво ответил, что выйдут требования, там и увидим.

В июле (информационное сообщение ФСТЭК от 19.07.2023 г. № 240/24/3584) ФСТЭК выпустил «Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети», утвержденные приказом ФСТЭК России от 7 марта 2023 г. № 44. Указанный документ предназначен для организаций, осуществляющих разработку и (или) производство многофункциональных межсетевых экранов уровня сети (МЭ), заявителей на осуществление сертификации, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств защиты информации на соответствие обязательным требованиям по безопасности информации.

По этим требованиям МЭ должен соответствовать также и «Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76 (с изменениями). В них к МЭ устанавливаются три класса защиты.

В соответствии с классами защиты к управлению доступом в МЭ предъявляются минимально необходимые требования по безопасности информации, предъявляемые к уровню доверия МЭ, управлению доступом в МЭ, идентификации и аутентификации пользователей, фильтрации сетевого трафика, обнаружению и блокированию компьютерных атак, обнаружению и блокированию вредоносного ПО, доверенной загрузке МЭ, тестированию и контролю целостности

МЭ, производительности, аппаратной платформе, режимам работы, регистрации событий безопасности, обеспечению бесперебойного функционирования и восстановления МЭ, взаимодействию с иными средствами защиты информации, а также к централизованному и удаленному управлению многофункциональным межсетевым экраном уровня сети.

При включении в МЭ дополнительных функций безопасности, требования к таким функциям должны быть заданы в технических условиях или техническом задании, а полнота и корректность их реализации оценены при проведении сертификации МЭ.

Сертификация МЭ на соответствие Требованиям осуществляется с 14 июня 2023 г. В соответствии с приказом ФСТЭК России от 7 марта 2023 г. № 44 пункт 15 документа (требования к аппаратной платформе) вступает в силу с 1 января 2025 г.

Согласно данным Государственного реестра сертифицированных средств защиты информации, по состоянию на конец сентября сертификацию на полное соответствие новым требованиям не прошел ни один МЭ. На большинство действующих изделий подобного типа были переоформлены действующие сертификаты с учетом соответствия классам защиты МЭ, поэтому называть их полноценными «многофункциональными межсетевыми экранами уровня сети» не совсем корректно. Впрочем, для включения свежих решений МЭ в реестр новых ПАК прошло слишком мало времени.

ПОД НАЗВАНИЕМ NGFW...

Согласно классификации Gartner, термин NGFW (New Generation Firewall)

¹ BIS Journal № 1/2023

Тема использования отечественных межсетевых экранов нового поколения многими производителями и потребителями была воспринята как панацея от всех бед в ИБ

появился в 2008 г. для описания фаервола от компании Palo Alto Networks, который контролировал доступ пользователя к приложениям и обрабатывал трафик на нескольких процессорах одновременно. Считается, что современный NGFW — программно-аппаратный комплекс с большим количеством функций, обеспечивающих централизованное управление и комплексную защиту масштабных IT-инфраструктур. Он реализует технологии SPI (stateful packet inspection), встроенной системы предотвращения вторжений IPS (Intrusion Prevention System) и IDS (Intrusion Detection System), обладает возможностью контролировать и блокировать трафик на уровне приложений и предоставляет дополнительные возможности брандмауэра (Extra Firewall Intelligence), что обеспечивает постоянную актуализацию механизмов защиты.

По данным все того же Gartner, в 2023 г. потребители в мире отдадут предпочтение NGFW от американских компаний Palo Alto Networks и Fortinet. Однако после февраля 2022 г. эти решения недоступны на российском рынке и не поддерживаются производителями. В соответствии с Указами Президента России №166 и №250, постановлениями правительства и требованиями регуляторов после 01.01.2025 г. обязателен переход на доверенные отечественные ПАК на объектах КИИ.

Тема импортозамещения и, в частности, использования отечественных межсетевых экранов нового поколения многими производителями и потребителями была воспринята как панацея от всех бед в информационной безопасности. И если первые видят в ней способ получения прибыли в непростых экономических условиях, то вторые часто ведутся на красивые слова маркетологов и полагают, что NGFW станет универсальным выходом из сложной ситуации с учетом ухода иностранных вендоров и ужесточением требований регуляторов.

Рынок производителей МЭ условно можно поделить на три категории:

- ◆ ведущих агрессивное продвижение модельного ряда продуктов под названием NGFW;
- ◆ продолжающих разработку ПАК и без лишней помпы представляющих новые продукты класса МЭ клиентам;
- ◆ новичков, которые ведут активные разработки NGFW на основе своих старых продуктов.

ПРОИЗВОДИТЕЛИ

Позиция первой категории производителей проста: мы давно предвидели такую ситуацию и занялись разработками МЭ еще во второй половине 2010-х гг. «Мы давно выпускаем доверенную продукцию, удовлетворяющую требованиям заказчиков без оглядки на классификацию Gartner,

рост компании составляет 20–30% в год. Тем, кто только пришел на рынок МЭ, не стоит изобретать велосипед — он давно уже ездит», — примерно такой посыл звучит на многочисленных пресс-конференциях и презентациях продуктов ряда компаний.

Весной этого года на IV ежегодной конференции UserGate Александр Левченко, сооснователь и директор компании, отмечал, что вокруг только и говорили, что про NGFW. На начало 2023 г. появилось пять или шесть решений межсетевого экрана нового поколения, к середине года их число приблизилось к двум десяткам. Презентуя потребителям новую линейку продукции сезона 2023, представители UserGate сообщили, что извлекли уроки прошлого года, когда запасы устройств на складах компании быстро иссякли, и возникли проблемы с логистикой и получением компонентов ПАК. Менеджеры подчеркивали, что на складах покупателей ждут несколько тысяч серийных платформ, часть решений находится в предсерийной разработке или в виде прототипов и будет представлена на тестирование постоянным клиентам позже.

По оптимистичным оценкам коммерческого директора компании «Код безопасности» Федора Дбара, «на начало 2023 года отечественными NGFW пользовалось примерно 30% заказчиков». «За 2023 год количество

заказчиков, которые будут иметь отечественные NGFW, составит около 50% от всего рынка», — считает эксперт. — «Общий процент компаний, которые мигрируют на российские NGFW, к 1 января 2025 года (когда вступит в силу указ президента РФ № 250) достигнет 75%. Оставшиеся 25% будут пользоваться доступными иностранными продуктами, поскольку не подпадают под требования Указа» (цитаты из сообщений ТАСС). Напомним, что компания продвигает на российском рынке многофункциональный межсетевой экран (NGFW/UTM) с поддержкой алгоритмов ГОСТ «Континент 4». Модельный ряд включает 11 вариантов ПАК разной производительности и три МЭ в виртуальном исполнении.

КОММЕНТАРИЙ ЛУКАЦКОГО

Как отметил в своем телеграм-канале Алексей Лукацкий, арифметика у коллег не сходится: на 2,77 млн коммерческих компаний до конца года нужно почти 1,5 млн NGFW. «Если предположить, что у кого-то эти решения уже стояли и были отечественного производства, то по оценкам заказчикам до конца года должно быть поставлено около 500–700 тысяч устройств, — пишет А. Лукацкий. — Если предположить, что средний ценник на NGFW у нас порядка 200 тыс. рублей, то до конца года будет продано железок на 100–140 млрд рублей, что составляет больше половины всего рынка ИБ в 2023-м году по оценкам ЦСР (отчет «Прогноз развития рынка кибербезопасности в РФ на 2023–2027 годы», — прим. ред.). А ведь у ЦСР на всю сетевую ИБ приходится всего 40% рынка. А это далеко не только NGFW, но и NTA, песочницы, VPN и т.д. В общем, не сходится у меня пазл». Продолжая мысль эксперта, можно напомнить, что совокупные возможности отечественных вендоров ограничены производством десятков тысяч, но никак не сотен тысяч устройств.

А КОГО СЕРТИФИЦИРОВАЛИ?

На сегодня сертифицирована ФСТЭК России в части соблюдения требо-

ваний профиля защиты МЭ продукция 45 организаций, реестр регулятора охватывает 123 устройства, в т.ч. российских компаний АО «ИнфоТеКС», АО «Позитив Текнолоджиз», ООО «БИЗон», ООО «ИнфоВотч АРМА», ООО «Код Безопасности», ООО «Юзергейт». Сертифицированы в России до 2027 г. ПАК шлюз безопасности «Check Point Security Gateway R80.XX» (Израиль), функционирующий на аппаратной платформе семейства SG15XX (заявитель — ООО «Сертифицированные информационные системы групп»), и китайские межсетевые экраны HUAWEI различных серий (ООО «Техкомпания Хуавэй»). Среди других обладателей сертификатов — компании, работающие с госструктурами, предприятиями оборонного комплекса, ТЭК и промышленностью, телекоммуникационными и финансовыми организациями и часто использующие в своих решениях СКЗИ. В процессе разработки и подготовки к сертификации в 2024 г. находятся решения Solar NGFW от компании «Солар».

ТЕХНИЧЕСКИЕ УСПЕХИ

Один из главных вопросов, который волнует всех производителей МЭ, — пропускная способность на различных режимах работы. В ~10 раз планируют повысить скорость обработки запросов разработчики VipNet xFirewall («ИнфоТеКС»). Сегодня тесты оборудования по стандарту RFC2544 показывают скорости от 800 Мбит/с (решения для малого и среднего бизнеса) до 7600 Мбит/с (крупные предприятия) и 45 000 Мбит/с для ЦОД (по данным презентации компании, представленной на практической конференции ИнфоТеКС ТехноФест).

О том, что 40 ГБ/с — не предел, который может выжать центральный процессор аппаратных платформ, используемых в России, рассказывали и представители UserGate в рамках фестиваля кибербезопасности Positive Hack Days, который прошел в мае 2023 г. Им удалось обойти аппаратное ограничение и ускорить UserGate FG более чем в четыре раза.

Фактически в прямом эфире ведут разработку РТ NGFW специалисты АО «Позитив Текнолоджиз». И если

в начале одной из презентаций описание возможностей новой системы вызывало ухмылку конкурентов, присутствовавших в зале, то к концу мероприятия смешки сменились глубокой задумчивостью и погружением в тему. По утверждениям РТ, новый МЭ может работать на оборудовании различной производительности и форм-фактора: от настольных устройств для передачи данных на скоростях до 100 Мбит/с до высокопроизводительных серверов с пропускной способностью до 100 Гбит/с. Очередной этап представления возможностей РТ NGFW запланирован на ноябрь 2023 г.

СВЕТ И ТЕНИ КОНКУРЕНЦИИ

Конкуренция — один из двигателей рынка производителей. И хотя пока отечественным решениям по многим показателям далеко до продуктов ушедших иностранных компаний, активные разработки и поиски новых решений идут на пользу развитию российских технологий. Многие NGFW создаются как на базе проприетарных решений, так и на базе OPNsense решений для малого, среднего, крупного бизнеса и госструктур. Однако упор производителей на создание МЭ как «универсального решения с широкими функциональными возможностями» (и весьма дорогостоящего для компаний малого и среднего бизнеса) и усилия маркетологов по продвижению «страшного» и потому привлекательного звена NGFW среди не сильно сведущих в вопросах кибербезопасности потребителей может сыграть дурную шутку с рынком ИБ. Ведь помимо МЭ есть иные средства и технологии ИБ, которые выполняют защитные функции, достойны развития и внимания потребителей.

Завершим краткий обзор цитатой из уже упомянутого А. Лукацкого: «...видя результаты пентестов, я бы с точки зрения продуктов фокусировался не на NGFW, а на тех же NDR, EDR, WAF и VM. Они ловят и предотвращают то, что NGFW в принципе не видит».

Порядок потребен лишь глупцу,
гений властвует над хаосом.
Альберт Эйнштейн

О ТЕОРИИ ОТНОСИТЕЛЬНОСТИ В СЕТИ

КАК СОС И НОС КАЖДЫЙ ДЕНЬ СПАСАЮТ БИЗНЕС



Олег ХНЫКОВ
руководитель
продвижения
продуктов
сетевой
безопасности
Positive
Technologies

Иногда кажется, что проблемы взаимодействия ИБ и ИТ в инфраструктуре поможет решить только магия. Но если заменить магию на теорию, например, теорию относительности и приложить воображение, то эти проблемы станут гораздо понятнее. Предлагаю поднять фундаментальные вопросы задач ИБ и ИТ в защите сети, найти точки пересечения обязанностей каждого, устранить теневую инфраструктуру и выбрать подходящие инструменты.

ВВЕДЕНИЕ В СИТУАЦИЮ

Покой — состояние, которого не существует. Альберт Эйнштейн обозначил это ещё в 20 веке. Все объекты находятся в непрерывном движении относительно друг друга. В бизнесе, например, теория относительности отлично работает. Ни одна компания не абсолютна и не находится в состоянии покоя. На её способность зарабатывать, быть конкурентной, приносить пользу обществу и окружающему миру влияет всё. Потому что всё относительно!

Тем не менее что-то стабильное, абсолютное все-таки есть. Например, цифровые рельсы. Бизнес в России уже встал на них и довольно уверенно движется вперед. Например, финтех-корпорации не могут существовать без Big Data, Data Science, Machine Learning. Вся экосистема компаний построена на них, и пользователи привыкли к удобному технологичному сервису. В промышленности по цифровым рельсам, можно сказать, несётся целый исторический локомотив. Индустриальные компании наращивают цифровые активы, внедряют новые технологии, вводят процессы и процедуры... Но и внутри локомотива нет покоя: чтобы оставаться прибыльным для страны и акционеров, будь готов к модернизации. Кстати, государственные регуляторы этому неплохо способствуют. Вводят новые нормативные акты, подталкивающие важные сегменты экономики страны к обновлению. Тот же Указ № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ» предлагает компаниям пищу для размышлений и руководство к действию.

В целом вектор развития понятен, в условиях конкурентного рынка большим и малым игрокам не обойтись без современных систем автоматизации и информатизации. А поскольку абсолютного покоя нет, то информационные ресурсы постоянно изменяются, оптимизируются и добавляются. Бизнесу же важно, чтобы эти ресурсы оставались надежными, стабильными и производительными. По-другому не может быть. Поэтому

высоконагруженный сервис всегда нуждается в ресурсах, а еще в отказоустойчивой архитектуре систем и, разумеется, резервировании данных. Для решения этих задач в любом интерпрайзе есть целая бригада штатных ИТ-специалистов.

Так же обязательна и безопасность систем. Под безопасностью я подразумеваю недопущение неприемлемых для бизнеса событий на трех уровнях: сетевом, системном и прикладном.

Получается, что ИБ и ИТ — это два важных звена для бизнеса, их задачи сильно переплетены.

ЗАДАЧИ ИБ И ИТ. КАК ПРОВЕСТИ ЧЕРТУ

И вновь обращаюсь к Альберту Эйнштейну. Мысль, положенная в основу теории относительности, посетила его, когда он ехал в трамвае. Глядя на фонарные часы, ученый предположил, что если бы он смог разогнаться до скорости света, то для него время на этих часах остановилось бы и перестало существовать. Вот вам пример того, как решение задачи может основываться не только на знаниях и опыте, но и на воображении.

Но вернемся к ИБ и ИТ. Как известно, практически весь интерпрайз имеет in-house службы ИБ и ИТ, но не ограничивается ими. Вместе они обеспечивают достижение трех важных условий функционирования бизнеса (рис. 1):

- ◆ целостность цифровых ресурсов компании;
- ◆ доступность приложений, услуг и сервисов для внешних и внутренних пользователей;

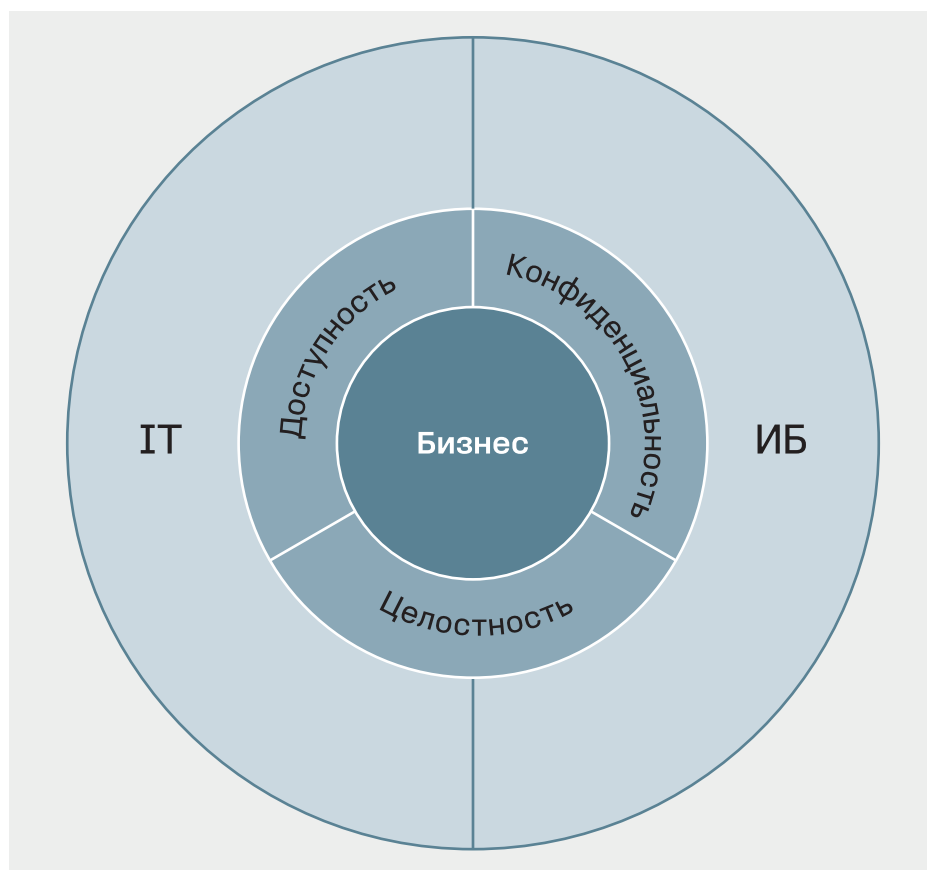


Рисунок 1. ИТ и ИБ являются основой для бизнеса

♦ конфиденциальность передаваемой и используемой информации.

Наверняка читатель помнит, что любая из служб ИБ или ИТ отвечает за множество доменов и поддоменов. Раз уж мы говорим про относительность, то применительно к сети ИТ-департамент представляет собой NOC (Network Operation Center). Он отвечает за сетевой доступ к бизнес-приложениям и сервисам для всех пользователей, контролирует целостность сети и управляет ей.

ИБ относительно сети представляет собой SOC (Security Operations Center) эксперты центра реагирования могут фокусироваться на защите периметра, каналов связи и в целом всей сетевой инфраструктуры.

Рассмотрю каждую службу поближе.

ЗАДАЧИ NOC

Как вы думаете, сколько стоит простой сервиса для бизнеса? Например, остановка важного сервиса финансовой организации в течение 30 минут обойдется минимум в 4 млн рублей. Сумма может только увеличиваться

в зависимости от числа пользователей, специалистов в NOCе и времени на восстановление доступа. Если такой простой будет регулярно повторяться, то существование бизнеса уже под угрозой. NOC делает все, чтобы этого не произошло, и решает семь задач (рис. 2):

- ♦ анализ сетевого трафика;
- ♦ управление сетевыми событиями;
- ♦ контроль конфигураций сетевого оборудования и ПО;
- ♦ обнаружение неисправности сети;
- ♦ диагностика и устранение неисправностей в оборудовании и ПО;
- ♦ поддержка сетевой инфраструктуры.

♦ мониторинг сети.

NOC отлично знает корпоративную сеть, вносит в нее изменения и актуализирует данные. Все это позволяет быстро решать проблемы с доступом к бизнес-приложениям и сервисам, устранять неполадки и строить отказоустойчивую и производительную сеть. Разумеется, для этих задач специалисты используют разный набор инструментов.

Например, CMDB позволяет собирать данные об устройствах и оборудовании, проводить детальную инвентаризацию активов и управлять этими данными. Система мониторинга, например, Zabbix обеспечивает данными о доступности сервисов, серверов и сетевого оборудования и помогает вовремя обнаружить неисправность и среагировать на нее. Ну и как же без анализа трафика, всем известного Wireshark. Инструментов много, как платных, так и бесплатных. Каждый специалист выбирает то, что ему удобно.

ЗАДАЧИ SOC

Простой сервиса из-за ошибки оборудования или ПО понятен. А сколько будет стоить бизнесу взлом этого сервиса, утечка данных и компрометация всей инфраструктуры? Скажем, 87 млн рублей. Эта сумма будет зависеть от количества узлов в сети, стоимости каждого актива и информации в нем, включая цену оборудования и ПО. Чем больше инфраструктура, тем стоимость компрометации будет выше. Если компрометация сервиса и, как следствие, всей инфраструктуры будет повторяться, значит стоимость такого взлома нужно умножать на его количество. В организации может быть несколько доменов, которые нужно защищать и обеспечивать в них:

- ♦ безопасность и мониторинг сетей;
- ♦ контроль мобильных устройств;
- ♦ контроль узлов;
- ♦ безопасность ОС и ПО;
- ♦ защита данных;
- ♦ безопасность виртуальных сред;
- ♦ безопасность облаков;
- ♦ безопасность приложений;
- ♦ управление уязвимостями.

А какие из них связаны в сети? Декомпозируем и получим (рис. 4):

- ♦ организацию межсетевого экранирования и формирование периметра;
- ♦ контроль каналов связи;
- ♦ мониторинг внутренней сети и угроз;
- ♦ мониторинг облачных сетей.

Читатель наверняка заметил, что есть явное пересечение зон ответственности NOC и SOC. Оба подраз-

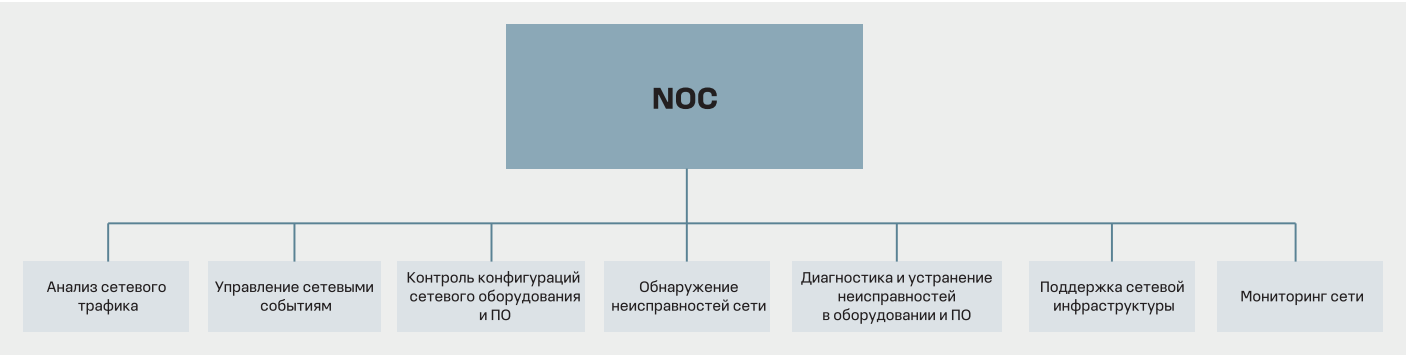


Рисунок 2. Задачи, решаемые с помощью NOC

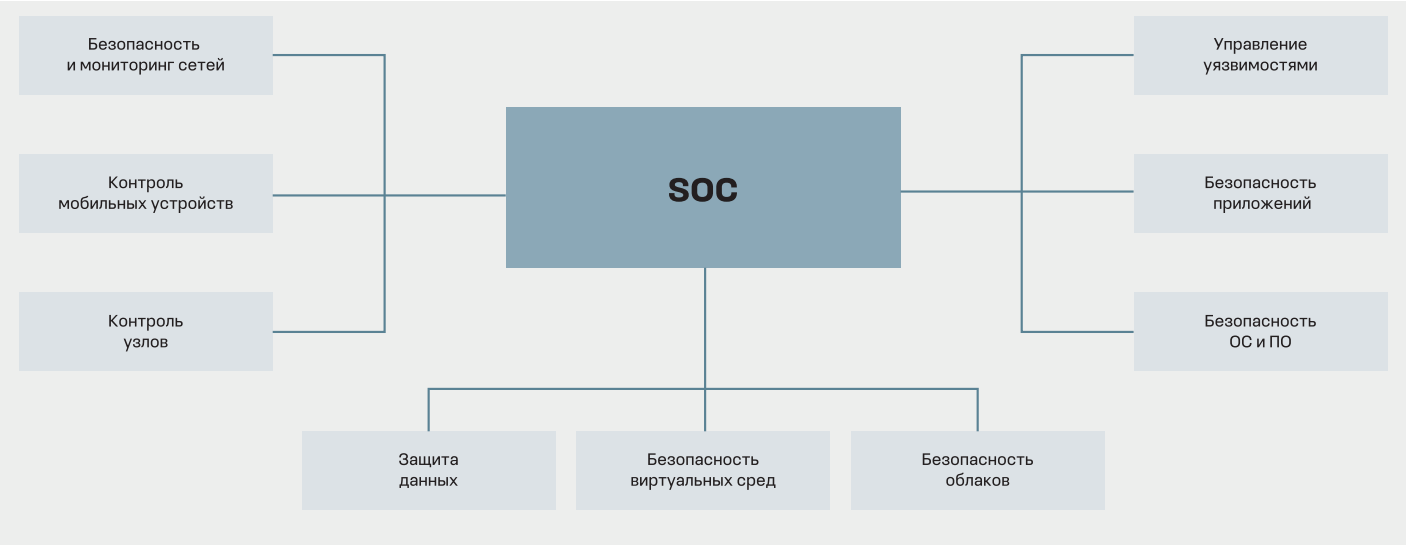


Рисунок 3. Задачи, решаемые SOC

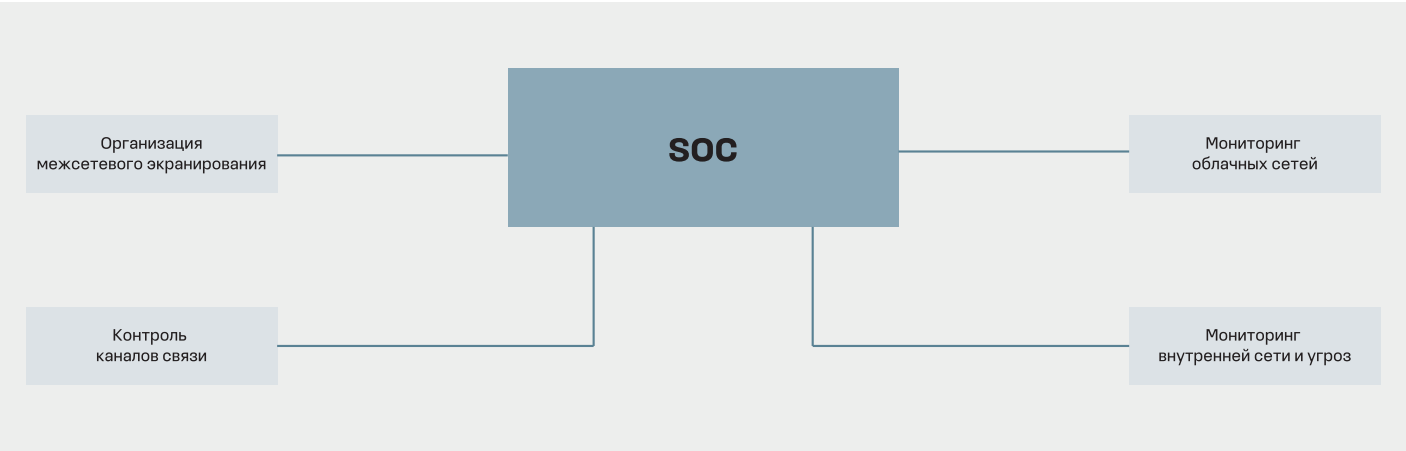


Рисунок 4. Сетевые задачи, решаемые SOC

деления контролируют сеть. Задача у них одна, а результаты разные.

ЦЕЛЬ ОБЩАЯ, РЕЗУЛЬТАТЫ — РАЗНЫЕ

Мониторинг сети — общая задача для NOC и SOC, но есть нюансы. **Первый нюанс** связан с исходными данными, полученными из сети для выполнения задачи.

NOCу достаточно получать сетевую статистику (NetFlow, sFlow, NetStream и проч.), записывать трафик по настроиваемому правилу и собирать метрики устройств с помощью SNMP, WMI, CLI, API или логов. Эта информация дает контекст сетевой проблемы, позволяет найти источник неисправности и решить возникшую аварию. Для этого даже существует

отдельный класс продуктов сетевого мониторинга — NPM (Network Performance Monitoring).

SOCу нужна глубина. Тут недостаточно только сетевой статистики и поверхностных данных. Чем больше информации можно получить из сети, тем лучше. Поэтому предпочтение отдается анализу копии сырого трафика, запись его в хранилище,

извлечение метаданных и автоматический ретроспективный анализ по ним. Для этого тоже существует отдельный класс решений NTA (Network Traffic Analysis) для мониторинга сети и обнаружения угроз.

Второй нюанс в решении задач подразделениями SOC и NOC заключается в отсутствии налаженного взаимодействия между ними. Это чревато «раздуванием» бюджетов каждого департамента, отсутствием единой базы данных о сетевом устройстве сети и нерегулярным обновлением данных. Например, IT-департамент вводит новый сервис для тестов. Работает с ним на протяжении нескольких недель, перестраивает часть инфраструктуры, разрешает доступы пользователям, не предупредив специалистов по ИБ. Протестировав, специалисты решают оставить ресурс без каких-либо изменений на какое-то время. Тем временем специалисты по ИБ даже не подозревают о появлении нового сервиса в инфраструктуре. Агентов (EPP/EDR) на них нет, журналы не заведены в SIEM-системы.

Другой пример. Случился инцидент, специалисты по ИБ провели сбор артефактов и принялись реагировать. Часть задач можно выполнить через имеющийся ИБ-инструментарий (EDR, NGFW), но учетную запись, например, уже не заблокировать на уровне инфраструктуры без участия IT. Поэтому ИБшникам в такой ситуации нужно собрать все артефакты и попросить специалистов NOC сделать блокировку. Результат получится быстрым, если NOC поверит им на слово. Но на практике айтишники предложат подождать, пока они сами разберутся, кого и почему нужно заблокировать, на какой срок, а главное, когда возвращать доступ.

Третий нюанс в совместной работе ИБ и IT — это теневая инфраструктура. Администраторы сети меняют место работы, пользователи устанавливают новые приложения, которые взаимодействуют с интернетом, приносят в офис собственные мобильные устройства. Это все приводит к появлению активов, про которые никто не знает и не может их контролировать. Сочетание теневой

инфраструктуры и отсутствие взаимодействия между подразделениями дают атакующим преимущество для проникновения в инфраструктуру и осуществления неприемлемых для бизнеса событий.

В итоге, получаем, что абсолютного покоя нет даже внутри казалось бы стабильной инфраструктуры компании, а каждая сеть относительно другой уникальна. Проблема же повторяется от компании к компании. Возьмем этот тезис за аксиому и попробуем решить проблему теневой инфраструктуры и отсутствие взаимодействия между IT и ИБ с помощью одного инструмента. Например, NTA.

КАК SOC И NOC ПОДРУЖИЛИСЬ... В NTA-СИСТЕМЕ

Мир не идеален. В ИБ, например, для решения конкретной задачи нужно использовать отдельный инструмент, который хорошо делает свою работу. На практике все, конечно, получается совсем не просто. Один и тот же инструмент часто применяют для решения смежных задач. Лучшим выходом из такой ситуации будет обозначить пересекающиеся задачи и выработать критерии для выбора подходящей системы.

Для начала обозначим четыре шага, которые важно пройти, чтобы избежать появления теневой инфраструктуры:

1. Получить полную видимость сети.
2. Разделить обнаруженные приложения, сервисы и узлы на категории: разрешенные, подозрительные, запрещенные.
3. Оценить уровни риска обнаруженных приложений, сервисов и узлов.

4. Получить полный контроль над выявленными активами.

5. Вывести из эксплуатации ненужные или запрещенные активы.

Первый, второй, четвертый и пятый шаги — это в чистом виде задачи для NOC. Все, кроме пятого, находится в поле зрения SOC. Перейдем к требованиям, предъявляемым к системам NTA.

К обязательным можно отнести:

♦ **Гибкие варианты сбора трафика в инфраструктуре.** Чем больше вариантов получения зеркалированного трафика из инфраструктуры поддерживает система, тем проще начать работать с инструментом. Идеально, если система поддерживает технологии SPAN, RSPAN, ERSPAN, GRE. Немаловажным преимуществом является поддержка аппаратных TAP-устройств и возможность работы с брокерами сетевых пакетов.

♦ **Пропускная способность.** Внутри сети широкие каналы, а значит система должна обрабатывать весь поток без ошибок. Потоки могут достигать 10 Гбит/с и выше.

♦ **Хранение сырых данных и метаданных.** Система должна иметь несколько хранилищ. Хранилище сырых данных нужно для ИБ, хранилище метаданных — для IT. Здесь важно соблюсти баланс между временем хранения данных и ресурсами на оборудование. На практике рекомендованное время хранения сырого трафика достигает 7 дней, а хранение метаданных — до 2-х недель.

♦ **Легкость внедрения.** Наличие конфигуратора и инсталлятора существенно упрощают внедрение в инфраструктуру и настройку системы.

♦ **Гибкость внедрения.** Двухуровневая архитектура системы позволяет горизонтально масштабироваться на всю компанию. Установка системы в виртуальную инфраструктуру, включая отечественные, актуально после ухода иностранных вендоров с российского рынка. Напомню, что в виртуальных средах возможны ограничения по обработке потока данных.

♦ **Количество обрабатываемых сетевых протоколов.** Количество поддерживаемых протоколов не означает их детальный разбор. Например, система может обнаружить 40 протоколов, а разбирать всего 5. Нужно находить баланс между количеством и качеством. И не стоит забывать про вложенные друг в друга протоколы. Хороший инструмент умеет определять инкапсуляцию и разбирает весь трафик внутри туннелей.

♦ **Визуализация накопленных данных.** Возможность строить виджеты и дашборды на основе полученных данных.

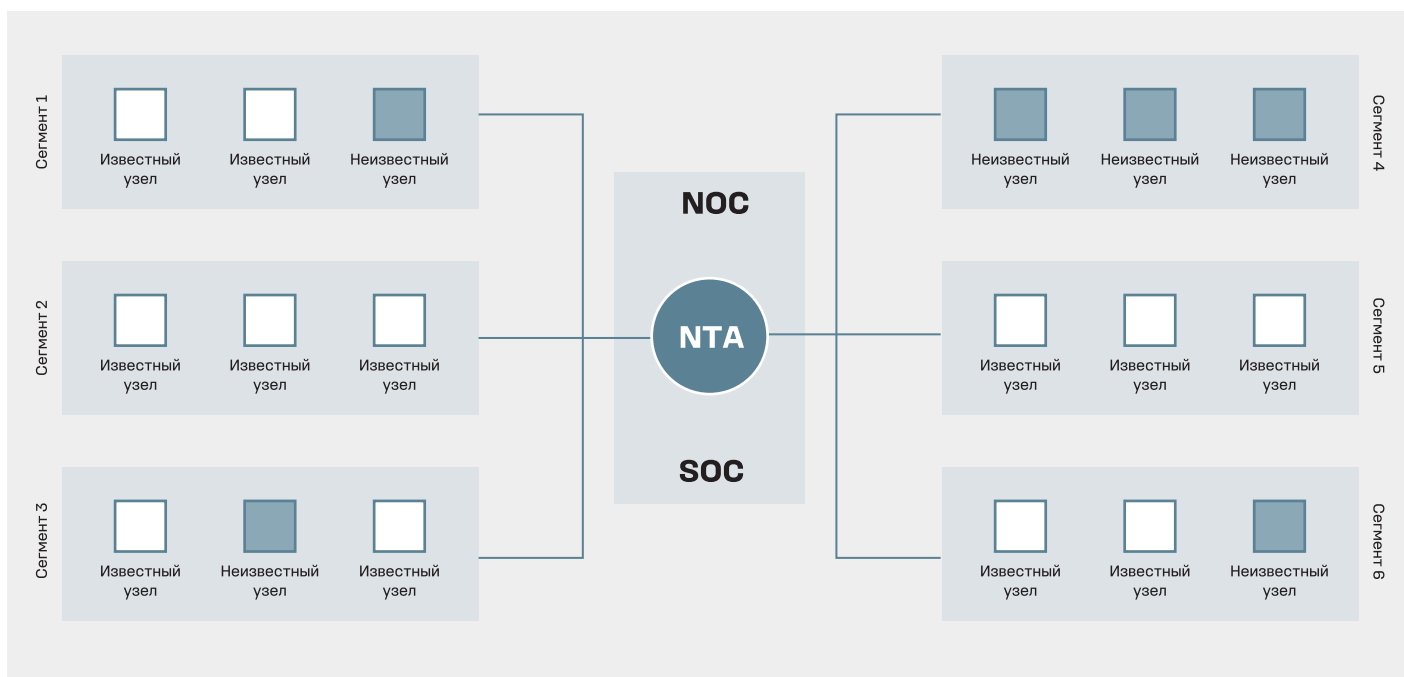


Рисунок 5. Обнаружение теневой инфраструктуры с помощью NTA

♦ **Система поиска.** Гибкий поиск по всем индексируемым данным. Возможность сохранить фильтры и делиться ими с коллегами.

♦ **Экспертиза.** Важный пункт для ИБ и не менее важный для ИТ. Система должна уметь определять приложения, операционные системы, типы и роли устройств, и используемые учетные записи.

Список требований не конечный и каждый для себя добавит, что ему необходимо.

Итак, мы разобрались с требованиями, выбрали инструмент, внедрили его и используем. А что делать с регламентами и взаимодействием департаментов? Регламент лежит на поверхности. Общая система анализа трафика дает ИБ и ИТ общую карту сети, информацию обо всех узлах, подключенных к ЛВС (локальной вычислительной сети); об учетных записях, паролях, ролях и типах устройств. Теперь ИБ не нужно постоянно запрашивать актуальные данные у ИТ, достаточно обратиться к NTA-системе. У ИТ исчезает часть рутинных задач. Теперь им не нужно собирать данные для специалистов по ИБ. Внедрение единой системы поможет построить взаимовыгодные отношения между подразделениями.

Отлично, а что дальше? Эффективность процесса будет зависеть

от принятых в компании регламентов. Возьму базовый сценарий. Например, ИБ обнаруживает новый узел с помощью NTA. Оператор обращается к системе и смотрит детали по обнаруженному узлу. При необходимости может перейти в сетевой граф и оценить насколько узел:

♦ **Легитимный.** Специалист формирует фильтр и ставит задачу в ИТ по установке систем защиты конечных точек и заведению журналов и событий с узла в SIEM-систему.

♦ **Подозрительный.** Оператор помечает узел как подозрительный и продолжает наблюдать за его активностью в сети. Эксперту предстоит понять, с кем этот узел уже взаимодействовал и продолжает общаться, нет ли обращений к доменному контроллеру или к критическим сегментам сети, какие протоколы используются для передачи данных, какой используется User-Agent и т.п.

♦ **Нежелательный.** Оператор формирует фильтр и задачу на деактивацию узла. ИТ получает задание, использует полученный фильтр с нужными деталями и выключает нежелательный хост.

Получается, все подразделения уже в курсе появления нового узла, определили его опасность, вовремя приняли соответствующие меры и

закрыли потенциальный вектор для атаки. Система NTA однозначно знает, что происходит и вовремя сообщает об этом специалистам SOC и NOC (рис. 5).

«Так причем здесь теория относительности?», — спросите вы, и будете правы. Очень важно не прекращать задавать вопросы и искать ответы даже там, где все кажется очевидным.

Все в нашем мире меняется: окружение, люди, бизнес. При этом, как мы выяснили, инфраструктура бизнеса подчиняется тем же законам физики. И дело не в том, что изменения происходят, а в том, что они происходят непрерывно и часто незаметно. Невидимые и неконтролируемые системы в инфраструктуре компании — общая проблема для ИБ и ИТ, и она обостряет необходимость менять процессы, регламенты и суть взаимодействия между экспертами из разных отраслей. Решить задачу комплексно и получить при этом новый качественный результат, поможет только нестандартный подход, и главный инструмент тут — воображение!

PEOPLE AS CODE

КАК СДЕЛАТЬ, ЧТОБЫ ЛИНГВИСТИЧЕСКАЯ
ОТНОСИТЕЛЬНОСТЬ НЕ МЕШАЛА ЗАЩИЩАТЬ ИБ-АКТИВЫ



Андрей ЖАРКЕВИЧ
ведущий рубрики,
эксперт «Антифишинг»

Многочисленные исследования год за годом демонстрируют странное явление: люди являются причиной примерно 80% всех инцидентов, однако на защиту от угроз, связанных с человеческим фактором, приходится менее 3% ИБ-бюджетов. Всё остальное уходит на технические средства. В статье разберёмся в причине такой несправедливости, выясним, к чему это приводит в реальной жизни и как можно решить проблему.

КАРТИНА МАСЛОМ

По данным отчёта за 2022 год, подготовленного телекоммуникационным гигантом Verizon, человеческий фактор остаётся главной причиной всех ИБ-инцидентов.

Он присутствует в 82% киберпроисшествий, будь то использование украденных учётных данных, фишинг, злоупотребление или просто ошибка конфигурации. Люди продолжают играть главную роль в инцидентах и нарушениях. Об этом говорит не только Verizon. Важность поведения сотрудников для безопасности признают практически все крупные компании.

Но если проанализировать структуру затрат на различные системы защиты, то создаётся впечатление, что ИБ-подразделения во всём мире дружно не замечают очевидного и продолжают вкладываться в защиту сети, серверов и веб-приложений, игнорируя сотрудников (рис. 1).

На долю продуктов, снижающих риски, связанные с человеческим фактором, приходится меньше 3% затрат.

В чём же причина такого нелогичного поведения? Дело в том, что всё, что связано с человеческим фактором, крайне сложно поддётся учёту. Вот и получается, что то, что не учтено, остаётся не защищено.

С ЧЕГО НАЧИНАЕТСЯ ПОРЯДОК В ИБ

Вряд ли у коллег по ИБ возникнет вопрос, о каком учёте речь, однако на всякий случай

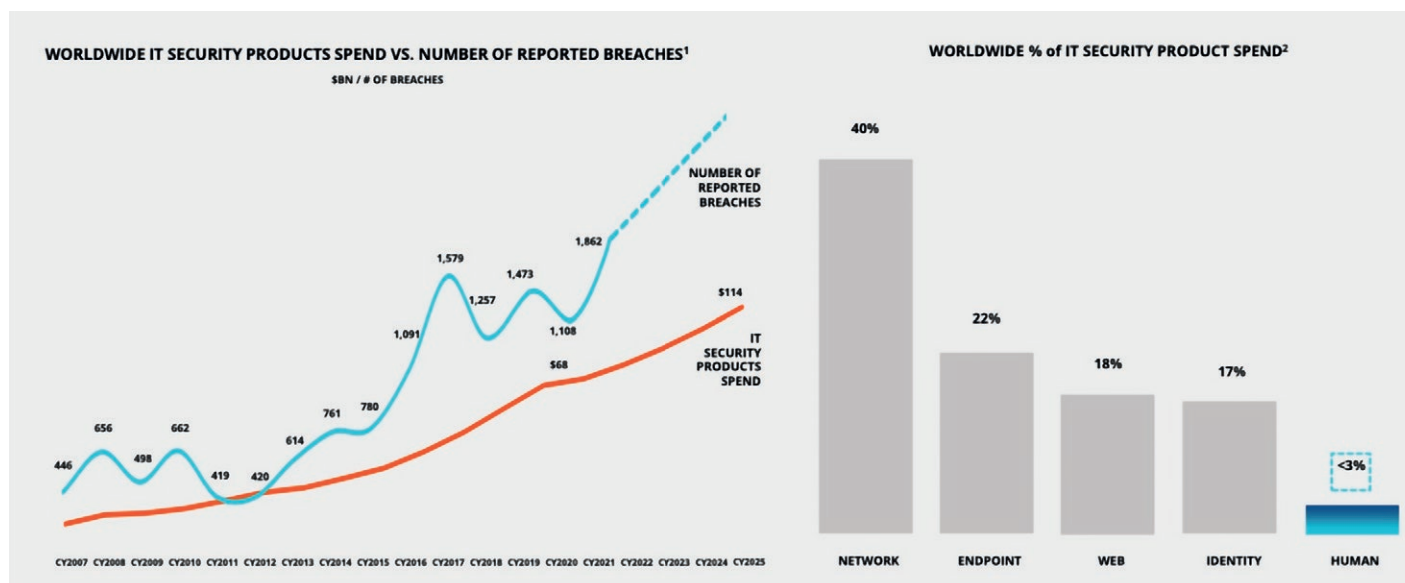


Рисунок 1. Затраты на ИБ, количество происшествий и структура расходов на ИБ-решения

стоит уточнить, что мы говорим про учёт активов, без которого организация полноценной защиты невозможна. Порядок в ИБ начинается с порядка в ИТ-процессах. Между тем, по данным опросов, уровень удовлетворённости в ИБ хуже всего именно от управления активами.

В идеальном мире, где царит ITSM, а инфраструктура реализована в полном соответствии с рекомендациями ITIL, проблем с учётом нет. Всё классифицировано, учтено и защищено. Однако большинству организаций до такого состояния очень далеко. Журналы SIEM переполнены алертами, но при этом часть активов выпадает из поля зрения систем мониторинга, потому что при инвентаризации о них не вспомнили.

С техническими средствами ситуация более-менее понятна. Специалисты по ИБ вполне квалифицированно научились работать с серверами, сетевым оборудованием, шлюзами, системами IPS/IDS и прочим. Налаженный учёт активов обеспечивает качественное управление и защиту. И вроде бы картинка выглядит правильной, так что беспокоиться не о чем. До тех пор, пока не вспоминаем про поведение людей как фактор успеха 82% инцидентов.

А ГДЕ ЖЕ ЛЮДИ?

Если посмотреть на перечень активов, которые мы защищаем от кибератак, то там найдётся всё что угодно. Кроме людей. EDR и SIEM-системы рисуют красивые цепочки заражения, на которых детально разобрано, как вредоносное ПО проникло в систему и к чему это привело. Но если присмотреться, на схеме (рис. 2) не хватает одного ключевого элемента, который расположен ровно между получением письма и запуском вложенного.LNK-файла.

Почему ярлык запустился и произошло заражение? Кто нажал кнопку?

А кнопку нажал конкретный человек, в ящик которого пришло это письмо. Это человек принял решение, которое привело к проникновению вредоноса в систему и краже информации. Поэтому реальная схема должна выглядеть как на рис. 3.

На этой схеме присутствует человек, действия которого привели к инциденту. Или не привели, если он не стал запускать вложенный в письмо ярлык.

Если всё зависит от поведения людей, то почему мы не встречаем их на схемах с цепочками заражений? Куда подевались сотрудники, администраторы и разработчики, из-за которых происходят ИБ-инциденты?

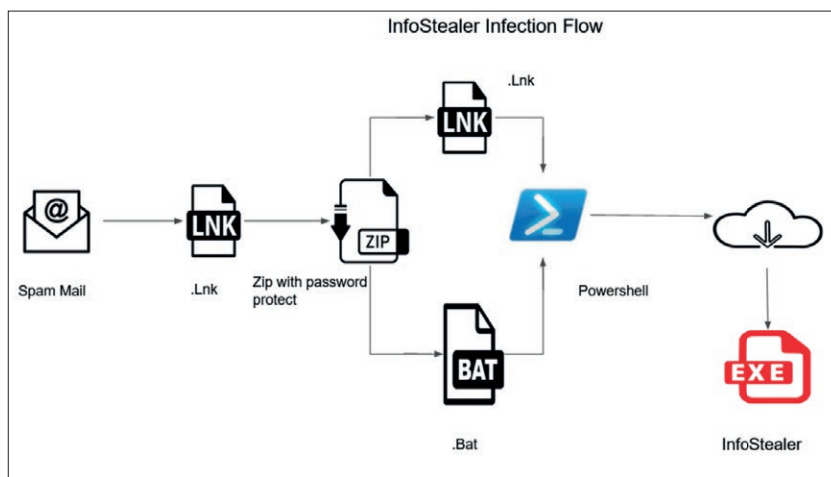


Рисунок 2. Цепочка заражения инфостилером с помощью фишингового письма

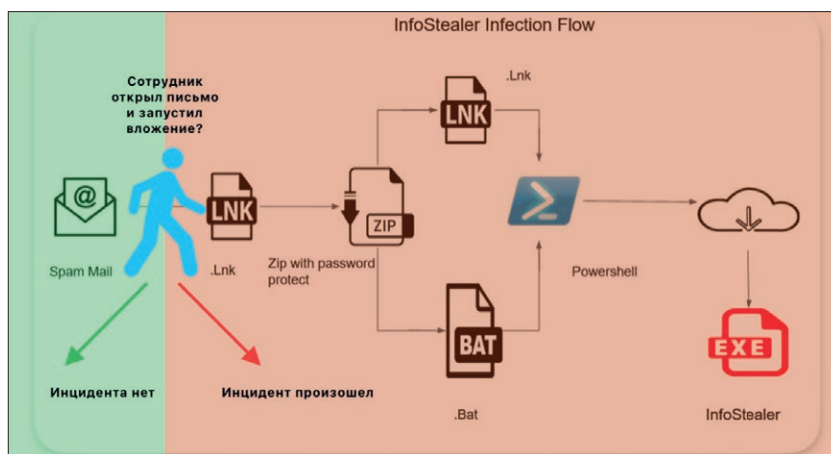


Рисунок 3. Реальная цепочка заражения. Человек — ключевой элемент

Всё просто. Возвращаемся к учёту активов и вспоминаем, что мы привыкли работать с техникой, технологиями, понятными цифровыми и физическими активами. Нам нужна детерминированная среда и логичные модели угроз в этой среде, а люди и их действия — это элемент неопределённости. В результате человеческий фактор отсутствует как класс в семантике языка, который используется в ИБ.

Есть сомнения? Тогда давайте посмотрим на базу данных угроз ФСТЭК. Чтобы не рисовать новые цепочки заражения, обратимся к разделу «Внедрение вредоносного ПО через электронную почту» (рис. 4).

Внедрение вредоносного ПО через электронную почту невозможно без участия человека. Может показаться, что люди спрятались где-то среди «Компонентов объектов воздействия», но это не так. Там есть ОС, браузер, клиент электронной почты и многое другое, а вот сотрудника, который открыл вредоносное письмо и запустил вредоноса в систему, нет.

← СП.4.1 Внедрение вредоносного программного обеспечения через электронную почту ⓘ	
Группа способов:	СП.4 Внедрение вредоносного программного обеспечения
Способ реализации:	СП.4.1 Внедрение вредоносного программного обеспечения через электронную почту
Уровень возможностей нарушителя:	В.1
Возможные реализуемые угрозы:	УБИ.1, УБИ.2, УБИ.3, УБИ.4, УБИ.5, УБИ.6, УБИ.7, УБИ.8, УБИ.9, УБИ.10, УБИ.11
Компоненты объектов воздействия:	К.1.2.1, К.1.2.2, К.1.5.1, К.1.5.15, К.1.7.2
Возможные меры защиты:	АВЗ.1.1, АВЗ.1.5, АВЗ.2.1, ЗИС.15.1, ЗИС.16.1, ЗИС.17.1, ЗИС.28.1, ЗИС.29.1

Рисунок 4. База данных угроз ФСТЭК. Раздел «Способы реализации»

Люди остаются за скобками любых инцидентов ИБ, и это системная проблема всей отрасли. Атаки описываются так, словно человеческого фактора в них нет. Пример на рис. 5.

Почему же мы так старательно избегаем упоминания о людях при описании киберпроешествий? Дело совершенно не в злом умысле, а в лингвистической относительности.

ЧТО НА УМЕ — ТО НА ЯЗЫКЕ. ИЛИ НЕТ?

Гипотеза лингвистической относительности предполагает, что структура языка влияет на мировоззрение и мировосприятие носителей языка, а также на их когнитивные процессы. Таким образом, мышление определяется языком, а значит, когнитивные категории определяются и ограничиваются лингвистическими категориями.

В соответствии с гипотезой структура языка формирует мышление человека и то, как он познаёт окружающий мир. Получается, что народы, которые говорят на различных языках, по-разному воспринимают основные категории окружающего мира, оценивают события и явления.

Таким образом, ИБ-специалисты действуют в соответствии с набором понятий, который присутствует в их языке для описания инцидентов. И раз люди как актив в этом наборе понятий отсутствуют, то и причин рассматривать их, рассказывая о происшествии, не имеется. Ментальные ограничения в действии. Как быть?

ВСЁ КАК КОД

Чтобы работать с людьми и их поведением так же удобно и прозрачно, как с другими активами, нужно ввести их в ИБ-язык как целостное понятие, формализовать. Реализовать это на практике можно с помощью концепции «Всё как код».

Концепция «Всё как код» родилась как решение проблемы администрирования сложных инфраструктур, включающих множество разнородных серверов, сервисов и систем. Сложность таких систем при ручном администрировании растёт с каждым дополнительным компонентом, особенно если этот компонент отличается от других.

Упростить администрирование можно путём унификации компонентов и средств их администрирования. Тогда недетерминированный инфраструктурный бардак превратится в структурированную ИТ-среду с чётко определёнными задачами и средствами управления.

Таким образом, чтобы превратить людей в детерминированный цифровой актив, которым можно удобно управлять, нужно превратить его в код.

ОЦИФРОВЫВАЕМ ЛЮДЕЙ — PEOPLE AS CODE

Для оцифровки людей мы воспользовались поведенческой моделью профессора Стэнфордского университета Брайана Джеффри Фогга. В соответствии с ней любые человеческие действия складываются из мотивации и возможностей. Чтобы действие было выполнено, требуется, чтобы один из

Описание инцидента

В сеть проник вирус, который зашифровал несколько тысяч рабочих станций и остановил работу завода ИТ-службе пришлось восстанавливать данные и системы из резервных копий

Компрометация учётной записи позволила злоумышленнику получить доступ к внутреннему веб-порталу организации, а оттуда переместиться на внутренние сервера и похитить конфиденциальную информацию

Что произошло на самом деле

Менеджер по продажам открыл письмо и запустил файл из вложения, потому что думал, что это выгодный договор с крупным заказчиком

Финдиректор получил сообщение в мессенджер от мошенника, который представился системным администратором. По указанию мошенника он перешёл по ссылке и два раза ввёл свой пароль, а затем уехал в банк

Рисунок 5. Атаки описываются так, словно человеческого фактора в них нет

этих показателей или оба были достаточно высоки (рис. 6).

Например, даже если желание не особенно сильное, но выполнить действие просто и быстро, оно, скорее всего, будет выполнено. Точно так же, когда очень хочется, даже очень сложное действие будет выполнено.

Интеграцию человека в организацию можно описать набором свойств: мотивацией, включающей его убеждения, и возможностями — оборудованием, ПО, доступами, знаниями, навыками.

Когда мотивация и возможности человека описаны, их можно добавить в систему информационной безопасности и получить решение нового поколения, в котором учитывается человеческий фактор. Этот подход мы использовали при создании концепции People as Code и базы данных People CMDB.

People CMDB — это open-source-продукт, реализованный в виде базы данных управления конфигурациями сотрудников. Он представлен в виде репозитория, содержащего информацию о ролях, свойствах сотрудников (знания, навыки, мотивация, убеждения), их уровнях защищённости и других параметрах согласно методологии антифишинга. С помощью People CMDB сотрудников можно превратить из угрозы безопасности в сильный и надёжный цифровой актив.

В рамках концепции People as Code роли людей, их доступы и возможность влиять на недопустимые события описываются в виде структуры данных (JSON-файла). Критически важно наличие следующих пунктов:

- ◆ бизнес-цели,
- ◆ недопустимые события,
- ◆ сценарии недопустимых событий,
- ◆ опасные действия,
- ◆ безопасные действия,
- ◆ сотрудники,
- ◆ роли,
- ◆ курсы,
- ◆ имитированные атаки.

От каждого из этих пунктов будет зависеть информационная безопасность компании.

Более детально с концепцией можно познакомиться на гитхабе антифишинга¹. Там приведены примеры на специфичном DSL-языке для интеграции People CMDB со средствами защиты и реализации концепции People as Code в ключевых процессах управления безопасностью.

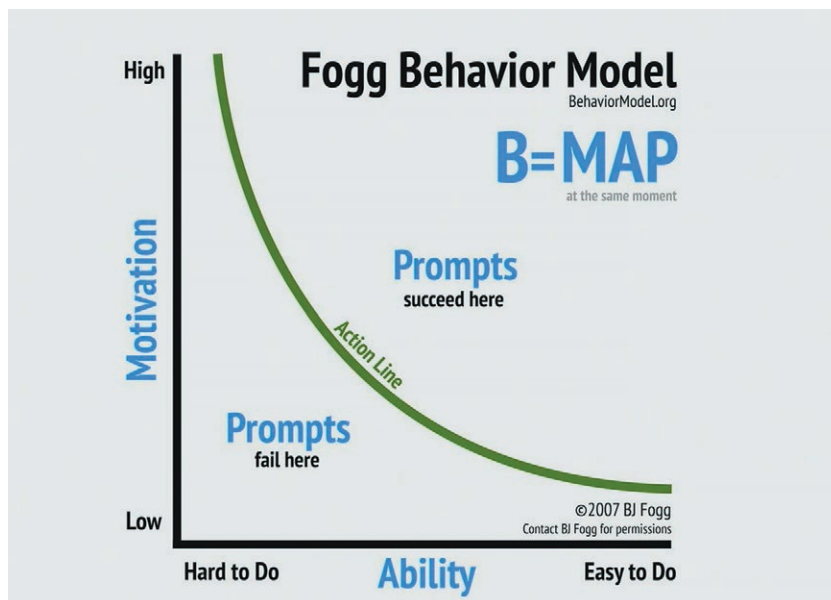


Рисунок 6. Модель Фогга. Высокая мотивация и/или возможность = высокая вероятность действия

ЗАКЛЮЧЕНИЕ.

НОМО DIGITALIS КАК ИБ-АКТИВ

Специалисты по ИБ воспринимают людей как неуправляемый и непредсказуемый аналоговый актив. Им проще работать с привычными цифровыми и техническими компонентами, поэтому проблема человеческого фактора игнорируется и замалчивается как что-то несущественное.

Причина такого явления — ментальные ограничения, описанные в гипотезе лингвистической относительности: в ИБ-языке отсутствуют понятия, с помощью которых можно унифицированным образом описать поведение людей и проблемы, связанные с ним.

Чтобы превратить людей в управляемый и понятный актив, нужно оцифровать их, используя подход «Всё как код» (Everything as Code). По аналогии с системами Documents as code, Governance as code и Infrastructure as code мы создали систему People as code и назвали нашу разработку People CMDB. Она позволяет мотивировать сотрудников обходить угрозы и объясняет, как это сделать.

Внедрение People CMDB в организации избавит ИБ-специалистов от составления бесконечных регламентов, которые никто не читает, и позволит полноценно управлять рисками, вовлечённостью, мотивацией и производительностью людей.

В результате все объекты защиты окажутся покрыты вниманием команды безопасности и соответствующими процессами и в них не останется «белых пятен», занимающих 82% площади.

¹ <https://github.com/PeopleCMDB>

УГРОЗЫ СНАТСРТ МНИМЫЕ И РЕАЛЬНЫЕ: НЕ СВЕРХРАЗУМ, А ЛЖИВЫЙ ИНОАГЕНТ

ГЕНЕРАТИВНЫЕ МОДЕЛИ ЕСТЕСТВЕННЫХ ЯЗЫКОВ
НЕ БОЛЕЕ ЧЕМ ЭЛЕКТРОННЫЕ СПРАВОЧНИКИ,
АВТОМАТИЗИРОВАННЫЕ ИЗВЕСТНО КЕМ



Павел БЫЛЕВСКИЙ
шеф-редактор
BIS Journal, кандидат
философских наук,
доцент

Появление новых версий ChatGPT (4.0 в марте 2023 года), наиболее известного и продвигаемого компьютерного генератора текстовых ответов, имитирующих диалог, порождает всплески общественного и научного интереса. Наблюдается значительный разброс мечтаний и страхов, оценок соотношения преимуществ и угроз ChatGPT как генеративной языковой модели на основе «машинного обучения». Объясним, что многие ожидания выглядят завышенными: ChatGPT как очередная компьютерная автоматизация справочно-библиографической деятельности относится к группе «сквозных» технологий «искусственного интеллекта», роль которых существенно возросла в результате цифровой трансформации, начавшейся в 2010-е годы. Каковы же мнимые и реальные угрозы ChatGPT российским гражданам?

ПОСТЫДНАЯ ТАЙНА ТЕСТА ТЬЮРИНГА

Новейшим компьютерным технологиям сопутствуют неизвестные прежде не только преимущества, но и угрозы информационной

безопасности. Фактором, обостряющим внимание к аспектам безопасности таких сервисов для российских граждан, является осложнение международных отношений, в том числе с глобальными цифровыми платформами, базирующимися в США, в связи с началом в 2022 году Специальной военной операции на Украине. Преувеличенные оценки возможностей ChatGPT, от утопии (высокой автоматизации, «замены» авторского труда) до антиутопии (сверхоружие в психологической войне), маскируют реальные риски. Чем же реально угрожает российским гражданам использование ChatGPT как публично-зарубежного массового цифрового сервиса и какие меры безопасности востребованы?

Декларации разработчиков нуждаются в сдержанно-критическом осмыслении: история «вёсен и зим» «искусственного интеллекта» с 1950-х годов свидетельствует, что они зачастую были сильно преувеличены в целях агрессивного маркетинга для привлечения инвестиций. Полюсами таких завышенных оценок являются утопия (машины будут за всех работать и всё решать) и антиутопия (машины поработят, уничтожат людей), грань между которыми не безусловна: если машины смогут делать всё лучше, то в чём смысл существования человека?

С точки зрения теории культуры, её единственным субъектом является человек, коллективы людей (общество). Наскальный рисунок, библиотека глиняных табличек с клинописью, бумага и карандаш, книга и статуя, кисть и полотно, библиотека и музей, телефон и телевизор, социальная сеть, интернет-мессенджер, «машинная живопись» и ChatGPT — всё это в равной степени, хотя и на разных стадиях исторического развития,

технические средства совместной деятельности людей. Создание топора позволяет человеку срубить дерево, но рубит не сам топор, а человек, и не всякий, а дровосек, умеющий правильно рубить топором. Этот пример верен для инструментов любых степеней сложности, автономности и автоматизации (в том числе технологий «искусственного интеллекта»): их умелое применение позволяет расширить способности человека.

Можно предложить продуктивную культурологическую версию классического теста Тьюринга, призванного определить «разумность» машины. Постыдной тайной этого теста, схоластической абстракцией выглядит сама постановка задачи «отличить человека от машины» вне критериев истинности и ценности: критерием служит мнение проводящего тест, к тому же в специально подобранных лабораторных, а не в практических полевых условиях. Задача теста компьютерных технологий должна ставиться по-другому: выявить ценность применения, её характер и значимость (или, напротив, ущерб); а затем определяющие роли социально-культурных субъектов — пользователя, создателя и разработчика. Такой метод может быть применён и для оценки преимуществ и рисков использования ChatGPT российскими гражданами. Компьютерное оборудование и программное обеспечение, независимо от сложности, уровня автоматизации и «человекоподобия» (включая решения класса ChatGPT), характеризуются не как субъекты, но как технические средства нарушения информационной безопасности, совершения преступления.

ТИХО САМ С СОБОЮ

Технические инструменты, расширяющие возможности человека, могут выглядеть более или менее самостоятельными в зависимости от степени автономности, уровня и масштабов автоматизации операций, выполняемых с их помощью, от отдалённости результатов во времени и пространстве. Однако люди, ответственные за противоправное нанесение ущерба другим с помощью сколько угодно высокотехнологичных средств, а также виновные в техногенных авариях, выявляются расследованием и привлекаются к ответственности без оглядки на имитационные иллюзии, порождаемые «искусственным интеллектом». В расследованиях инцидентов и преступлений, в том числе связанных с информационной безопасностью, определяются персональные роли и участие, степень вины в причинении ущерба каждого фигуранта.

ChatGPT как технология «искусственного интеллекта» не является ни интеллектом, ни даже чатом, поскольку данный цифровой сервис лишь имитирует человеческое общение и любую личность воображаемого «собеседника». У пользователя ChatGPT, задающего набором текста вопросы, отсутствует собеседник, в качестве такого он воспринимает... автоматизированный сервис самообслуживания. На деле происходит общение пользователя «тихо с самим собою»: «разговор» посредством текстового набора, пользователь сам же и отвечает на свои вопросы, предварительно подыскивая подходящие ответы в электронном справочнике. Генерируемые текстовые результаты, выдаваемые по запросам пользователя, не являются ответами, носят не субъектное происхождение, а исключительно техническо-вещный характер, наподобие маршрутов, автоматически прокладываемых навигационными интернет-сервисами, или изготовления торговым автоматом выбранного оплаченного коктейля.

В мировой культуре создана целая галерея иронично-сатирических образов подобных решений, от машины для комбинирования книг из слов в Академии прожекторов на летающем острове Лапута Дж. Свифта до компьютерного стихотворца «Электрибальда Трурля» Ст. Лема. В 1990-е первые подобные компьютерные программы их российские разработчики честно называли «бредогенераторами». Однако в определённых условиях и наркотический бред (например, жриц-пифий храма Аполлона в Древней Греции) может быть успешно выдан за божественное пророчество со скрытым глубоким смыслом.

Иллюзия «общения» возникает за счёт комплексного психологического фокуса: некритического восприятия названия «чат» и понятия «искусственный интеллект»; агрессивной рекламы разработчиков, транслируемой массовой прессой, а также имитационной словесной оболочки, выдающей пользователю результаты запросов от лица некоего иллюзорного «я» ChatGPT. С таким же успехом можно создать словесную или озвучиваемую сгенерированным тембром голоса «чат»-надстройку над любым автоматизированным цифровым сервисом, включая поисковые и навигационные. Психологическая иллюзия «общения» пропадает даже для самых впечатлительных и доверчивых пользователей, если выдачу результатов запросов производить не от имени «личности» ChatGPT, а сопровождать выполненным крупным ярким шрифтом уведомлением о том, что это автоматизированный электронный справочный

сервис, со ссылкой на подробное описание принципов работы. Также уместна маркировка «18+», учитывая для несовершеннолетних необходимость сопровождения использования ChatGPT опытным взрослым, педагогом, наподобие случаев обязательных по закону упоминаний «запрещённая в РФ организация», «иноагент» и т.п.

ОТКРОВЕНИЯ ЛЖИВОГО ИНОАГЕНТА

Содержание текстовых «ответов» по запросам пользователей, генерируемых компьютерными решениями, включая ChatGPT, определяется следующими тремя основными элементами сервиса:

- 1) «библиотекой», структурированной базой размеченных (формализованных по ключевым параметрам) текстов (созданных людьми или автоматически обработанных тем или иным способом), отобранных по правилам, сформулированным разработчиками;
- 2) параметрами «обучения», а по сути автоматизированной отработкой алгоритмов поиска и отбора фрагментов, формально наиболее соответствующих запросу (критерии и степень соответствия задаются разработчиками, контролирующими результаты обработки);
- 3) алгоритмами компиляции отобранных фрагментов в связный текст в соответствии с правилами «естественного языка».

Первые два элемента целиком и полностью зависят от разработчиков, в том числе от их политики предпочтений и проводимой цензуры, избирательного применения критериев «языка ненависти» и др. Технические задания утверждаются в соответствии с интересами собственника, инвесторов сервиса и государства, резидентами которого они являются, в том числе «групп влияния». Компания OpenAI, разработчик ChatGPT, базируется в США, как и один из крупнейших инвесторов и партнёров проекта, компания Microsoft. Соответственно, принципы подбора (и отсеивания) текстов для «библиотеки», а также критерии соответствия их фрагментов запросу пользователя, используемых для компиляции «ответа», должны полностью соответствовать корпоративным интересам OpenAI и законодательству США.

Крайне важно обстоятельство, что, в отличие от поисковых интернет-сервисов, «ответы» ChatGPT, точнее, результаты машинной обработки имеющейся «библиотеки» текстов на основе запроса пользователя... не содержат ссылки на источники. Отсутствуют и другие встроены инструменты проверки

(«фактчекинга»); разработчики гарантируют пользователям лишь некоторую степень правдоподобности, но не достоверность, не истинность «ответов». Если относить современные версии ChatGPT к «искусственному интеллекту», то перед нами модель генерации «фейк-новостей» и фальсификации истории в стиле среднего журналиста «жёлтой прессы» США, сильно политически ангажированной.

«Этические» риски фальсификации авторства в результате не декларируемого использования ChatGPT журналистами, учёными, студентами и т.п. являются завышенными. Роль ChatGPT в создании авторских текстов принципиально не отличается от любых других технических средств культуры: гусиного пера с чернилами, карандаша, перьевой или шариковой авторучки, источников рукописных и печатных, электронных документов, библиотек с каталогами, поисковых интернет-сервисов и т.д. ChatGPT представляет собой не более чем жёстко цензурируемую цифровую библиотеку с алгоритмами выдачи результатов по запросам без ссылок на источники и проверки на истинность («фактчекинга»). Гарантируется лишь высокая оригинальность, но не достоверность и не смысловое качество генерируемого по запросу текста. Проверка и оценка качества, а также ответственность остаются на долю автора, пользующегося сервисом, а также специалистов, оценивающих создаваемые таким образом тексты (редакторов и т.п.). Гонорар за публикацию, созданную с использованием ChatGPT, по праву будет принадлежать человеку-автору, как и ответственность вплоть до уголовной в случае, если при этом будет нарушен закон.

ГРУБЫЙ АМЕРИКАНСКИЙ АКЦЕНТ

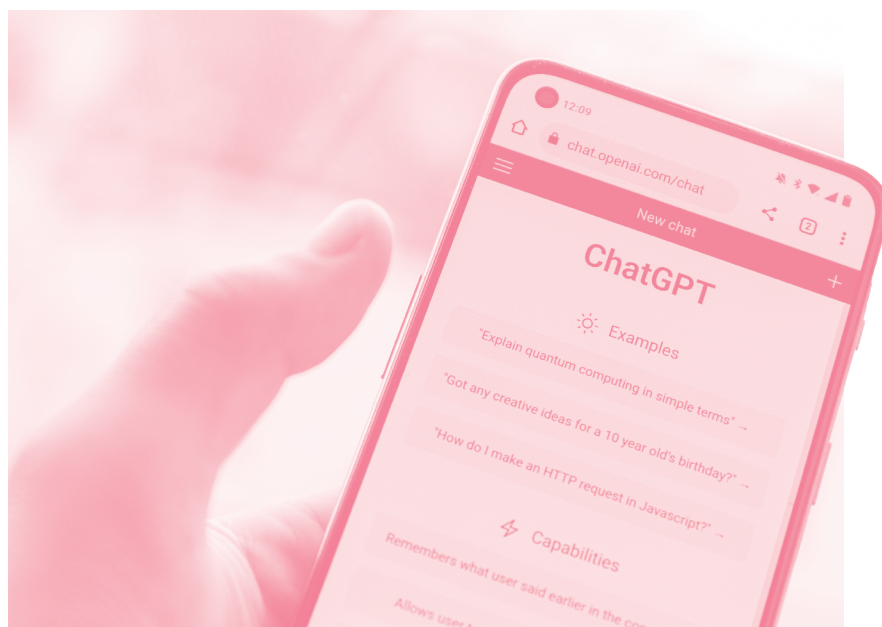
Таким образом, можно признать лишь гипотетическими и завышенными риски использования ChatGPT в качестве «сверхоружия» антироссийской психологической войны, фальсификации авторства, массовой безработицы журналистов и других создателей текстов. Зато уже сейчас ChatGPT реально используют злоумышленники для маскировки вредоносных кодов, внедряемых в программные продукты. Происходят инциденты утечки и публикации конфиденциальной информации, вводимой пользователями в запросах без учёта того, что это частный трансграничный сервис, способный публиковать вводимые сведения. Так, весной 2023 года корпорация Samsung из-за применения сотрудниками в работе ChatGPT понесла значительный ущерб от утечек, содержащих

корпоративную коммерческую тайну. Одна из главных причин подобных инцидентов — недостаточная культура информационной безопасности, профессиональной и массовой пользовательской.

К рискам, усилившимся в результате анти-российских технологических санкций недружественных стран, следует отнести дискриминационные действия глобальных цифровых платформ, базирующихся в США, в отношении российских граждан и официальной прессы. В случае ухудшения международных отношений компания OpenAI может повысить анти-российскую направленность ChatGPT, повышая риски российских граждан. С иронией относясь к мнимым угрозам, реальные риски ChatGPT для российских пользователей можно минимизировать средствами государственного регулирования и повышения культуры информационной безопасности пользователей, а также созданием отечественных решений подобного класса.

В качестве средства государственного регулирования предлагается обязательство маркировать интерфейс ChatGPT предупреждением, что «чат» лишь торговая марка. На деле это автоматизированный трансграничный электронный библиотечный сервис самообслуживания пользователей, базирующийся в США и действующий в соответствии с законами, смысловой цензурой этой страны. В генерируемых текстах проступает, несмотря на всю маскировку, неистребимый грубый американский акцент. Поэтому выдаваемые по запросам тексты должны сопровождаться предупреждением о необходимости проверки из-за возможностей наличия заведомо ложных сведений, в том числе нарушающих российское законодательство, в случае распространения которых к ответственности будет привлечён пользователь. В случае невыполнения этих требований государственными уполномоченными органами могут быть приняты дополнительные меры ограничения и блокировки массового доступа к ChatGPT на территории России и в российском сегменте интернета.

Создателям отечественных автоматизированных генераторов текстов можно рекомендовать увеличивать долю самостоятельных разработок с учётом российских



социально-культурных ценностей, обеспечивая цифровой суверенитет; ввести в выдаваемых по запросам результатах ссылки на источники, автоматизированные сервисы фактчекинга и соответствия российскому законодательству, а также отказаться от имитации чата, создания иллюзии общения.

Эффективной мерой снижения рисков ChatGPT является повышение общегражданской культуры информационной безопасности посредством образовательных организаций, прессы и социальной рекламы, социальных сетей и мессенджеров — разъяснение массовой аудитории сущности и механизмов работы машинных генераторов текстов, сопутствующих угроз и рисков. Также до массовой аудитории необходимо доводить сведения о рисках получения и распространения недостоверных сведений, наступления ответственности в случаях, нарушающих российское законодательство, а также об угрозах, связанных с трансграничным характером сервиса ChatGPT и возможным применением его владельцами и разработчиками для распространения дезинформации.

Полная версия статьи:

Былевский П. Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023. № 8. С. 46–56. DOI: 10.7256/2454-0757.2023.8.43909 EDN: UZDRFW URL: https://nbpublish.com/library_read_article.php?id=43909



ВПЛОТЬ ДО ДАЛЬНОГО КОСМОСА

САМЫЕ АКТИВНЫЕ АТАКУЮЩИЕ — ГРУППИРОВКИ
LOCKBIT И CLOR, КИТАЙСКИЕ ХАКЕРЫ И, ПОХОЖЕ,
ИНОПЛАНЕТЯНЕ

ПЕРВАЯ ТЫСЯЧА

На конец августа 2023 г. кибератака, целью которой было приложение для передачи данных MOVEit от компании Progress Software, скомпрометировала почти одну тысячу организаций, говорится в исследовании американской компании Resecurity.

Первые сведения об инцидентах появились в конце мая, жертвами кибератак программ-вымогателей Clor стали крупные британские компании. Позднее к ним присоединились

американские и европейские. В ходе расследования инцидента с момента обнаружения старта массовой кибератаки Progress Software обнаружила пять дополнительных эксплойтов SQLi.

Группировка использовала SQL-инъекцию «нулевого» дня. Атака на цепочку поставок скомпрометировала более 963 государственных и частных организаций по всему миру. Примерно 80% из них находится в США. Предполагается, что в ходе кампании были раскрыты личные

данные более 58 млн человек. В совокупности на сферу услуг, финансы и образование приходится более 48% зарегистрированных жертв.

Сведений о выплате выкупов не поступало. Однако, по статистике, 25–30% компаний-жертв соглашаются с требованиями хакеров. Ожидается, что Clor получит от \$ 75 до \$ 100 млн выкупа, что делает эту кибератаку самой крупной в истории. Ещё больше средств Clor может монетизировать, продав данные несговорчивых жертв на «вторичных рынках» даркнета.

Исследователи Resecurity оценивают кампанию MOVEit, проводимую Clor, как значимое событие в сфере торговли программами-вымогателями. Оно может повлиять на сценарии будущих атак, поскольку является примером реализации кибератаки с использованием программ без развёртывания специального двоичного файла или криптолокатора программы-вымогателя.

Учитывая масштаб данных о бизнесе, сотрудниках и клиентах, раскрытых в результате взлома MOVEit, исследователи полагают, что утечки станут катализатором новой волны мошенничества в сфере деловой электронной почты. Эксперты призывают компании пересмотреть устаревшие корпоративные подходы и усилить кибербезопасность, проведя оценку состояния систем и приняв меры по снижению рисков от программ-вымогателей и атак в цепочке поставок.

КТО ВЗЛОМАЛ КИБЕРБЕЗОПАСНОСТЬ ЯПОНИИ?

Национальный центр готовности к инцидентам и стратегии кибербезопасности Японии (NISC) подвергся кибератаке. Расследование показало, что хакеры находились в сети NISC с октября 2022 г. по июнь 2023 г., когда и были обнаружены. По данным источников Financial Times, предположительно действовали китайские хакеры, которые получили доступ к конфиденциальным данным.

Обнаружение взлома произошло во время изучения устойчивости инфраструктуры Японии к кибератакам, связанного с началом военного сотрудничества страны с США, Великобританией и Италией. Оно включает совместную работу над проектом истребителя и обмен секретными технологиями.

Ранее правительственные эксперты из США и Великобритании уже выражали сомнения, что Япония готова к обмену секретной информацией. Газета Washington Post напомнила о массовой атаке на оборонные сети Японии, осуществлённой китайскими военными хакерами в конце 2020 г. После этой кибератаки правительство Японии выделило

\$ 7 млрд на 5 лет на меры по защите от киберугроз, однако результатов этой защиты нет. В июле 2023 г. атака, замаскированная под инцидент с программой-вымогателем, привела к временному закрытию порта Нагоя.

Эксперты оценивают атаки как часть «постоянного тестирования Китаем инфраструктурной защиты Японии».

В начале августа NISC объявило, что в результате взлома почтового сервера в период с октября 2022 г. по июнь 2023 г. произошла утечка персональных данных, содержащихся в электронной почте. По данным расследования, проникновение произошло через учётную запись сотрудника. Агентство разослало уведомления о возможной компрометации данных частным и правительственным партнёрам в Японии и за рубежом. В публичном заявлении говорится, что Агентство обнаружило утечку данных и уведомило пострадавших по электронной почте.

NISC является подразделением аппарата Кабинета министров Японии. После выявления инцидента Агентство инициировало проверку других серверов и систем правительства. Представитель NISC заявил, что расследование уже пришло к выводу, что был скомпрометирован только почтовый сервер Агентства. Чиновник отказался комментировать подробности кибератаки. Источники FT связывают взлом с китайскими хакерами, об этом говорят стиль атаки и характер цели.

МИД Китая уже опроверг причастность КНР к нападению, призвав Токио обратить внимание на союзников из США, которые часто шпионят за партнёрами.

Действия Японии по усилению защиты от кибератак сдерживаются нехваткой персонала и низкой квалификацией кадров. В планах правительства увеличить численность киберподразделения, входящего в состав Сил самообороны Японии, и развивать его учебную базу. В конце марта 2023 г. группа насчитывала чуть менее 900 членов, в то время как в аналогичной структуре США работают 6200 человек, в Китае — не менее 30 тыс.

«УТИНАЯ ОХОТА» ПРОШЛА УДАЧНО

Министерство юстиции США сообщило о нейтрализации сети ботнета Qakbot. Его взломали специалисты ФБР и их европейские партнёры. Группа компьютеров, заражённых вредоносной программой, использовалась для проведения кибератак. Специалисты продолжают отключать программы на тысячах компьютеров-жертв, пишет CBS News.

Операция «Утиная охота», в ходе которой попытались уничтожить систему ботнета, также привела к изъятию \$ 8,6 млн в криптовалюте. Эти средства были собраны в ходе преступных кампаний по вымогательству. Следователи утверждают, что Qakbot, также известный как Qbot и Pinkslipbot, активен с 2008 г., изначально действует как банковский троян. Qakbot стал начальной точкой входа для многих ransomware, включая Conti, ProLock, Egregor, REvil, MegaCortex и Black Basta. По словам официальных лиц, эти преступные группировки, вероятно, пострадали в результате «Утиной охоты» ФБР.

По данным Минюста США, общее число жертв Qakbot составило 700 тыс. человек, из них около 200 тыс. проживают в США. Жертвами хакеров стали правительственные учреждения, компании малого и среднего бизнеса, поставщики медицинских услуг и стратегические предприятия.

Ботнет использовался хакерами для удержания компьютерных систем в заложниках до момента получения выкупа. Qakbot получал доступ к устройствам через спам-письма, содержащие вредоносные ссылки, встроенные в сообщения. Такие ботнеты незаметно захватывают контроль над компьютером и скоординированно работают для совершения предполагаемых преступлений, заявили следователи.

По словам высокопоставленных чиновников ФБР и Министерства юстиции США, в рамках операции «Утиная охота» ФБР получило доступ к инфраструктуре QakBot и «перенаправило» киберактивность на серверы, контролируемые спецслужбами. Специалисты смогли внедрить вредоносное ПО с помощью программы,

которая вывела компьютер жертвы из ботнета, освободив его от вредоносного хоста.

Методы уничтожения Qakbot представляют собой новый подход, который пытались внедрить правительству. Сети хакеров были разрушены, а жертвы получили инструменты, необходимые для противодействия атакам вредоносного ПО, отметили в ФБР. Инструменты были санкционированы судом с многочисленными оговорками — только для удаления вредоносного ПО с заражённых устройств.

Операция была успешной благодаря тесному партнёрству со следователями из Франции, Германии, Нидерландов, Великобритании, Румынии и Латвии. В результате международного расследования никто не был арестован, но были изъяты 52 сервера. Полиция Нидерландов, где были захвачены 22 сервера, нашла на них 7,6 млрд учётных данных. Серверы также были отключены во Франции (6) и Германии (8).

Представители спецслужб подчёркивают, что помимо финансовых убытков, связанных с кампаниями Qakbot, на карту были поставлены национальные интересы многих стран. Группы вымогателей нацеливались на больницы и критически значимые объекты социальной инфраструктуры, жизненно важной для национальной безопасности.

Расследование продолжается.

ИЗБИРАТЕЛЬНАЯ КОМИССИЯ ПРОВАЛИЛА ТЕСТ

Избирательная комиссия Великобритании автоматически получила отказ в сертификации во время аудита Cyber Essentials — поддерживаемой правительством схемы, призванной помочь британским организациям защититься от распространённых кибератак. Проверка выявила проблемы, которые способствовали ранее обнаруженному взлому систем избиркома. Как пишет Infosecurity Magazine, аудиторы нашли устаревшее ПО на примерно двухстах ноутбуках сотрудников Комиссии. Ещё одной причиной преждевременного завершения аудита стало использование персоналом

неподдерживаемых требования безопасности Apple iPhone.

Эти факты вызвали обеспокоенность наблюдателей по поводу готовности избиркома к защите от кибератак на фоне требований правительства к сертификации Cyber Essentials для поставщиков, работающих с конфиденциальными данными.

В начале августа Избирательная комиссия Великобритании сообщила, что стала жертвой кибератаки. Впервые злоумышленники получили доступ к серверам Комиссии в августе 2021 г. Подозрительная активность в системах была обнаружена только в октябре 2022 г. Злоумышленники получили доступ к «эталонным копиям» списков избирателей, хранившимся Комиссией в исследовательских целях и для проверки допустимости политических пожертвований. Хакеры получили личные данные 40 млн жителей Великобритании, которые были зарегистрированы для голосования в период с 2014 по 2022 г., включая имена и домашние адреса. Также были раскрыты имена избирателей, проживающих за пределами страны. Беспокойство наблюдателей вызвал как тот факт, что атака оставалась незамеченной в течение 15 месяцев, так и молчание длиной в 10 месяцев, в течение которых Комиссия должна была проинформировать общественность об инциденте.

Изначально Комиссия преуменьшала значимость нарушения, заявив, что сведения «являются общественным достоянием». Утечка повлияла на данные миллионов людей, отказавшихся от участия в публичных реестрах, отмечают эксперты. По их мнению, злоумышленники имели доступ к системам Избиркома в течение нескольких месяцев. Это указывает на то, что они искали нечто особенное, а не традиционную для кибератак финансовую выгоду. Длительное нахождение хакеров в сети служит напоминанием всем организациям о необходимости принятия быстрых мер по усилению киберзащиты. Это затруднит проникновение злоумышленников в сети и предотвратит повторение подобных атак.

Ещё один факт удивляет наблюдателей: Комиссия не подала по-

вторную заявку на сертификацию Cyber Essentials в 2022 г., но заявила, что по-прежнему привержена совершенствованию своих мер кибербезопасности в сотрудничестве с Национальным центром кибербезопасности (NCSC).

Организации Cyber Essentials, участвующие в программе, могут подтвердить свои полномочия в области кибербезопасности и продемонстрировать свою приверженность соблюдению правил безопасности. Cyber Essentials проводится NCSC для любого бизнеса. Организации получают сертификат на основе ежегодных оценок, доступных на двух уровнях — Cyber Essentials и Cyber Essentials Plus. Получив сертификат Cyber Essentials, организации вносятся в базу данных NCSC и могут публиковать значки сертификации на сайте для информирования клиентов.

LOCKBIT ОПЯТЬ НАНЁС УЩЕРБ

Хакерскую группировку LockBit обвиняют в краже и публикации в даркнете тысяч страниц секретных данных, связанных со стратегическими объектами Великобритании: базой атомных подводных лодок ВМС Клайд, лабораторией химического оружия в Портон-Дауне, подразделениями Центра правительственной связи, базами BBC и тюрьмами строго режима. Хакеры атаковали сети компании Zaun, которая занимается обеспечением безопасности объектов повышенной секретности, пишет издание The Daily Mirror. Доступ к украденной информации можно получить с помощью специального программного обеспечения.

Данные были украдены в августе 2023 г. в ходе кибератаки на компанию Zaun, говорится в сообщении на сайте организации. Zaun заявила, что приняла «все разумные меры для предотвращения любых атак на системы». Сведения переданы в Национальный центр кибербезопасности (NCSC).

В компании пояснили, что взлом произошёл через «незаконно установленный компьютер с Windows 7», на котором находилось ПО для одной из производственных машин,

но «в остальном сеть была обновлена». В компании полагали, что принятые меры защитят от утечек данных, однако после инцидента в Zaun согласились, что LockBit удалось загрузить часть информации, возможно, ограниченной уязвимым ПК, но с риском доступа к некоторым данным на сервере. Считается, что это 10 ГБ информации — 0,74% от всех хранимых данных. Компания не стала обсуждать требования о выкупе.

Атака приписывается русскоязычной группировке LockBit, ключевым подозреваемым является Михаил Матвеев, включённый в список самых разыскиваемых ФБР после атак на 1400 объектов по всему миру. В число его преступлений входит попытка шантажа Royal Mail на сумму £ 66 млн. Всего же LockBit предъявил пострадавшим компаниям требования о выкупе на сумму более \$ 100 млн.

Британские политики уже выразили озабоченность фактом утечки, которая может нанести серьёзный ущерб национальной безопасности и некоторым секретным объектам Королевства.

ЕСЛИ НЕ ПРИШЕЛЬЦЫ, ТО КТО?

Две обсерватории на Гавайях и Чили закрыты после обнаружения подозрительной активности.

Национальная исследовательская лаборатория оптической и инфракрасной астрономии Национального научного фонда США (NOIRLab) сообщила, что киберинцидент, произошедший 1 августа, вынудил лабораторию временно приостановить работу самых современных и мощных телескопов Gemini North и Gemini South на Гавайях и в Чили. Также были затронуты телескопы обсерватории Серро Тололо в Чили. Телескопы на Китт-Пик в Аризоне не пострадали.

Сотрудники обсерваторий работают с экспертами по кибербезопасности, чтобы вернуть в сеть все телескопы и сайт Gemini.edu, который в настоящее время работает в автономном режиме, говорится в заявлении NOIRLab от 24 августа. Специалистам удалось подключить некоторые телескопы к сети и собирать данные с помощью обходных путей. Учёные



благодарны астрономическому сообществу за поддержку и терпение, команды продолжают работать над восстановлением нормальной работы обсерваторий.

Пока неясно, какова была природа кибератак и откуда они произошли. NOIRLab отмечает, что расследование продолжается и организация с осторожностью относится к разглашению информации.

Кибератаки на объекты NOIRLab произошли накануне выхода подготовленного Национальным центром контрразведки и безопасности США (NCSC) бюллетеня, информировавшего американские аэрокосмические компании и исследовательские организации об угрозе кибератак и шпионажа, пишет портал Space. Иностранные разведки и хакеры «признают важность коммерческой космической отрасли для экономики и национальной безопасности США, включая растущую зависимость критической инфраструктуры от космических активов», говорится в бюллетене. «Они рассматривают американские космические инновации и активы как потенциальные

угрозы, а также ценные возможности для приобретения жизненно важных технологий и опыта».

Телескопы, принадлежащие Национальному научному фонду США, — одни из самых современных в мире. Диаметр зеркал каждого из них составляет 8,1 метра, что позволяет учёным наблюдать за объектами дальнего космоса в инфракрасном диапазоне. Один день простоя обсерватории ведёт не только к финансовым, но и к научным потерям, ставит под угрозу научные проекты.

Астрономические обсерватории уже были объектами кибератак, напоминает Space. В октябре 2022 г. хакеры нарушили работу комплекса радиотелескопов, расположенного в чилийской пустыне Атакама, — большой миллиметровой/субмиллиметровой решётки Атакамы (ALMA).

НАСА уже много лет является жертвой кибератак. В 2021 г. Агентство пострадало от массовой атаки на софт по управлению ИТ-инфраструктурой от компании SolarWinds.

Подготовила
Марина Бродская

ОДКБ. РЕСПУБЛИКА БЕЛАРУСЬ

АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



**Александр
ВИНОГРАДОВ**
ФГУП
«ЦНИИХМ»



**Сергей
МЕНШИКОВ**
основатель
Belarusian
InfoSecurity
Community



**Андрей
СИТНОВ**
независимый
эксперт

Данной статьёй начинается серия статей по анализу законодательства в области информационной безопасности. На данный момент в мире много разных союзов между странами. Во многих участвует Российская Федерация – Союзное государство, ОДКБ, ЕАЭС, СНГ, БРИКС и др.

При планировании путешествия в другую страну или бизнеса с представителями иностранного государства возникает ряд вопросов, связанных с требованиями по обеспечению безопасности информации в соответствии с местным законодательством. Как будут защищаться ваши персональные/личные данные, какие законы в области ИБ действуют в данной стране, как не нарушить требования ИБ и не стать нарушителем закона и др.? Вопросов много. Можно изучать статьи в интернете, но многие публикации написаны несколько лет назад и потеряли свою актуальность. Законодательство меняется, нормативные документы отменяются, изменяются, выходят новые документы.

Начинаем с публикации, посвящённой анализу законодательства в области ИБ нашего ближайшего соседа – Республики Беларусь. Между нашими странами сложились тесные взаимоотношения. Создано и развивается союзное государство. Россия и Беларусь являются участниками целого ряда союзов с другими странами.

ОБЩИЕ СВЕДЕНИЯ

Республика Беларусь – государство в Восточной Европе. Столица – Минск. Государственные языки – белорусский и русский.

Органы, утверждающие законы и подзаконные акты в области ИБ в стране: Президент Республики Беларусь, Совет министров Республики Беларусь, Совет безопасности Республики Беларусь, Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ), Национальный центр защиты персональных данных Республики Беларусь (НЦЗПД), Национальный банк Республики Беларусь (НБ РБ) и другие отраслевые ведомства.

Все документы, за исключением документов НЦЗПД и НБ РБ, имеют общереспубликанское значение и применяются для организации и обеспечения информационной и кибербезопасности. НЦЗПД имеет свою специфику в регулировании сбора и обработки ПД граждан РБ. Национальный банк Республики Беларусь и другие отраслевые ведомства дополняют и детализируют ИБ в части специфических отраслевых процессов. НБ РБ выделен как более активный отраслевой регулятор ИБ.

ТАЙНЫ

Тайны, определённые законодательством Республики Беларусь:

♦ **коммерческая тайна** утверждена Законом РБ от 5.01.2013 № 16-З «О коммерческой тайне»:

«коммерческая тайна – сведения любого характера (технического, про-

изводственного, организационного, коммерческого, финансового и иного), в том числе секреты производства (ноу-хау), соответствующие требованиям настоящего Закона, в отношении которых установлен режим коммерческой тайны».

♦ **банковская тайна** утверждена Банковским кодексом Республики Беларусь от 25.10.2000 № 441-З:

«Сведения о счетах и вкладах (депозитах), в том числе о наличии счёта в банке (небанковской кредитно-финансовой организации), его владельце, номере и других реквизитах счёта, размере средств, находящихся на счетах и во вкладах (депозитах), а равно сведения о конкретных сделках, об операциях без открытия счёта, операциях по счетам и вкладам (депозитам), а также об имуществе, находящемся на хранении в банке, являются банковской тайной и не подлежат разглашению».

♦ **персональные данные**¹ утверждены Законом Республики Беларусь от 7.05.2021 № 99-З «О защите персональных данных»:

«персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано».

¹ Более подробно про обработку персональных данных в странах наших ближайших соседей можно прочитать в статье «Но есть нюансы... Национальные особенности обработки персональных данных в странах ОДКБ». Виноградов А., Меншиков С., Ситнов А., BIS Journal № 3 / 2023, а также на сайте журнала.

ВЫСОКОУРОВНЕВЫЕ ДОКУМЕНТЫ

Высокоуровневыми концептуальными документами, охватывающими вопросы информационной безопасности, являются:

♦ **Концепция национальной безопасности Республики Беларусь** (утверждена Указом Президента Республики Беларусь 9.11.2010 № 575).

Данная концепция закрепляет совокупность официальных вкладов на сущность и содержание деятельности РБ по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз. Концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения национальной безопасности, а также методологическую основу совершенствования актов законодательства в различных сферах национальной безопасности, разработки документов стратегического планирования.

♦ **Концепция информационной безопасности Республики Беларусь** (утверждена Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1).

Концепция представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области информационной безопасности. Данная концепция обеспечивает комплексный подход к проблеме информационной безопасности, создаёт методологическую основу для совершенствования деятельности по её укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере.

♦ **Концепция обеспечения кибербезопасности в банковской сфере** (утверждена Постановлением Правления Национального банка Республики Беларусь 20.11.2019 № 466).

Концепция представляет собой структурированный документ, разработанный на основе результатов анализа и видения Национальным банком сложившейся ситуации в области обеспечения кибербезопасности банков, небанковских кредитно-финансовых организаций, открытого акционерного общества «Банк развития Республики Беларусь», содержащий перспективные направления решения имеющихся и предотвращения возможных проблем в сфере обеспечения кибербезопасности в банках и Национальном банке в виде систематизированного изложения целей, задач, особенностей текущей ситуации и возможных способов достижения требуемого уровня обеспечения кибербезопасности в банковской сфере.

♦ **Концепция информационной безопасности Союзного государства** (утверждена 22.02.2023 Высшего Государственного совета Союзного государства).

Концепция определяет основы для формирования согласованной государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также выработки мер по совершенствованию систем обеспечения информационной безопасности государств — участников Договора о создании Союзного государства.

ЗАКОНЫ

Законы — нормативные акты высшего уровня, регулирующие определённый круг вопросов. Основными законами в области ИБ являются:

♦ Закон Республики Беларусь от 10.11.2008 № 455-3 «Об информации, информатизации и защите информации».

Настоящим Законом регулируются общественные отношения, возникающие:

- при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также использовании информации;
- создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;

- организации и обеспечении защиты информации.

♦ Закон Республики Беларусь от 28.12.2009 № 113-З «Об электронном документе и электронной цифровой подписи».

Настоящий Закон направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.

УКАЗЫ ПРЕЗИДЕНТА РБ

Указы, декреты Президента РБ — акты, имеющие силу закона, издаваемые главой государства в соответствии с действующим законодательством. Наивысший юридический статус имеют декреты, затем следуют указы. Основными указами в области ИБ являются:

♦ Указ Президента РБ № 40 от 14.02.2023 «О кибербезопасности (центры обеспечения кибербезопасности и реагирования на киберинциденты».

Данный указ создаёт национальную систему обеспечения кибербезопасности, элементами которой являются:

- Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ);
- Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты (Национальный центр кибербезопасности);
- центры кибербезопасности;
- авторизованный оператор электро-связи;
- объекты информационной инфраструктуры.

♦ Указ Президента РБ № 196 от 16.04.2013 «О некоторых мерах по совершенствованию защиты информации». Данный указ утверждает:

- Положение о технической и криптографической защите информации;
- Положение о порядке отнесения объектов информатизации к критически важным объектам информатизации.

♦ Указ Президента РБ № 60 от 01.02.2010 «О мерах по совершенствованию использования национально-го сегмента сети Интернет».

♦ Указ Президента РБ № 449 от 09.12.2019 «О совершенствовании государственного регулирования в области защиты информации».

Данный указ утверждает:

- Положение о технической и криптографической защите информации;
- Положение о порядке отнесения объектов информатизации к критически важным объектам информатизации;
- Положение о технической и криптографической защите информации в Республике Беларусь, утверждённое Указом, изложено в новой редакции;
- дополнение Указа Положением о порядке отнесения объектов информатизации к критически важным объектам информатизации.

♦ Указ Президента РБ № 515 от 30.09.2010 «О некоторых мерах по развитию сети передачи данных в Республике Беларусь».

Данный указ постановляет создать единую республиканскую сеть передачи данных (ЕРСПД), включив в её состав сети передачи данных республиканских органов государственного управления, местных исполнительных и распорядительных органов, иных государственных органов и других государственных организаций, а также хозяйственных обществ.

♦ Указ Президента РБ № 461 от 16.12.2019 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий».

Вводит понятие республиканский центр обработки данных (РЦОД), предназначенный для размещения программно-технических средств республиканской платформы и других программно-технических средств, информационных систем (ресурсов) государственных органов и иных государственных организаций, хозяйственных обществ, в которых Республика Беларусь либо административно-территориальная единица обладает акциями (долями в уставных фондах) в размере более 50 процентов.

♦ Указ Президента РБ № 49 от 28.02.2017 «О государственном регулировании в области экспортно-го контроля».

Данный указ утверждает:

- Положение о порядке предоставления юридическим лицам права на осуществление внешнеторговой либо посреднической деятельности в отношении специфических товаров (работ, услуг);
- Положение о порядке государственного регулирования ввоза специфических товаров (работ, услуг), вывоза объектов экспортного контроля, осуществления посреднической деятельности в отношении объектов экспортного контроля;
- Положение о порядке проведения идентификации;
- Положение о порядке оформления обязательств по использованию импортированных специфических товаров (работ, услуг);
- Положение о порядке организации государственного контроля за выполнением обязательств по использованию импортированных (экспортированных) специфических товаров (работ, услуг) в заявленных целях.

♦ Указ Президента РБ № 188 от 31.05.2022 «О расширении использования государственными организациями информационно-коммуникационных технологий».

Устанавливает, что при оказании электронных услуг и осуществлении административных процедур в электронной форме государственными организациями идентификация и аутентификация физических и юридических лиц для совершения ими юридически значимых действий в электронном виде проводятся с использованием Единой системы идентификации физических и юридических лиц (Единая система идентификации).

♦ Указ Президента РБ № 187 от 25.05.2017 «О республиканской системе мониторинга общественной безопасности».

Данный Указ постановляет создание республиканской системы мониторинга общественной безопасности.

♦ Указ Президента РБ № 350 от 18.09.2019 «Об особенностях использования национального сегмента сети Интернет».

♦ Указ Президента РБ № 422 от 28.10.2021 «О мерах по совершенствованию защиты персональных данных».

Данный Указ постановляет создание Национального центра защиты персональных данных Республики Беларусь (Национальный центр защиты персональных данных).

ОПЕРАТИВНО-АНАЛИТИЧЕСКИЙ ЦЕНТР ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ (ОАЦ)

Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ) обычно выпускает подзаконные акты, регламентирующие конкретные направления и процедуры обеспечения защиты информации. Документы можно найти и ознакомиться с ними на портале ОАЦ — <https://oac.gov.by/law>. В частности, там представлены тематические подборки:

- ♦ законы Республики Беларусь;
- ♦ указы Президента Республики Беларусь;
- ♦ постановления Совета министров Республики Беларусь;
- ♦ постановления Оперативно-аналитического центра при Президенте Республики Беларусь;
- ♦ приказы Оперативно-аналитического центра при Президенте Республики Беларусь.

В частности, ОАЦ издаёт приказы, которые детализируют требования, процедуры в области защиты информации и являются подзаконными актами. Например, в отношении Указа Президента РБ № 40 от 14.02.2023 «О кибербезопасности» подзаконным актом является Приказ ОАЦ № 130 от 25.07.2023, детализирующий работу центра обеспечения кибербезопасности и реагирования на киберинциденты. А Приказ ОАЦ № 65 от 20.02.2020 «О показателях уровня вероятного ущерба национальным интересам Республики Беларусь» является продолжением Положения о порядке отнесения объектов информатизации к критически важным объектам информатизации по Указу Президента РБ № 449 от 09.12.2019.

ПОСТАНОВЛЕНИЕ СОВЕТА МИНИСТРОВ РБ

Важным для реализации технических мер, соответствующих требованиям законодательства РБ, является:

♦ Постановление Совета Министров Республики Беларусь 15.05.2013 № 375. «Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ).

Настоящим техническим регламентом устанавливаются требования к средствам защиты информации в целях обеспечения национальной безопасности, а также предупреждения действий, вводящих в заблуждение потребителей относительно назначения и качества средств защиты информации.

ПРИКАЗЫ НАЦИОНАЛЬНОГО ЦЕНТРА ЗАЩИТЫ ПД РБ

Свод документов регулятора по ПД — Национальный центр защиты персональных данных Республики Беларусь: <https://cpd.by/pravovaya-osnova/natsionalnoye-zakonodatelstvo/>.

♦ Приказ Национального центра защиты персональных данных Республики Беларусь от 15.11.2021 № 12 «О классификации информационных ресурсов (систем)».

Устанавливает следующие классификации:

- общедоступные персональные данные;
- специальные персональные данные (кроме биометрических и генетических персональных данных);
- биометрические и генетические персональные данные;
- персональные данные, не являющиеся общедоступными или специальными.

♦ Приказ Национального центра защиты персональных данных Республики Беларусь от 15.11.2021 № 13 «Об уведомлении о нарушениях систем защиты персональных данных».

♦ Приказ Национального центра защиты персональных данных Республики Беларусь от 15.11.2021 № 14 «О трансграничной передаче персональных данных».

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ НАЦИОНАЛЬНОГО БАНКА РБ

Национальный Банк Республики Беларусь издал ряд технических требований и правил по ИБ (ТТП ИБ)² (<https://www.nbrb.by/legislation/informationsecur>):

ТТП ИБ 1.1–2020 «Общие положения и терминология»;

ТТП ИБ 2.1–2020 «Требования к системам менеджмента информационной безопасности»;

ТТП ИБ 3.1–2020 «Требования по обеспечению информационной безопасности при использовании технологий виртуализации»;

ТТП ИБ 4.1–2020 «Менеджмент рисков информационной безопасности»;

ТТП ИБ 5.1–2020 «Оценка соответствия информационной безопасности банков Республики Беларусь требованиям ТТП ИБ 1.1–2020 и ТТП ИБ 2.1–2020»;

ТТП ИБ 6.1–2020 «Рекомендации по документационному обеспечению деятельности в области обеспечения информационной безопасности в соответствии с требованиями ТТП ИБ 1.1–2020»;

ТТП ИБ 7.1–2020 «Рекомендации по менеджменту инцидентов информационной безопасности»;

ТТП ИБ 8.1–2020 «Технические требования и правила информационной безопасности. Требования по защите программного обеспечения банковских мобильных приложений».

СТАНДАРТЫ

ТТП ИБ разработаны в развитие пяти государственных стандартов серии «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь», действующих с 2013 года:

- СТБ 34.101.41 «Общие положения»;
- СТБ 34.101.42 «Аудит информационной безопасности»;
- СТБ 34.101.61 «Методика оценки рисков нарушения информационной безопасности»;

² Более подробно описание и сравнение комплекса ТТП и СТО БР были опубликованы в статье «Россия — Беларусь: диалог друзей. Как СТО БР возродился в ТТП ИБ». Виноградов А., Меньшиков С., BIS Journal № 4(47)/2022.

- СТБ 34.101.62 «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТБ 34.101.41»;
- СТБ 34.101.68 «Методика оценки соответствия информационной безопасности банков Республики Беларусь требованиям СТБ 34.101.41».

Ресурс <https://tnpa.by> Национального фонда технических нормативных правовых актов содержит перечни и описание Стандартов Беларуси, в том числе и по ИБ.

РИСК-МЕНЕДЖМЕНТ

В заключение перечень официальных документов РБ по тематике риск-менеджмента:

- СТБ 34.101.70–2016 «Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах»;
- СТБ 34.101.61–2013 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки рисков нарушения информационной безопасности»;
- Постановление правления НБРБ 29.10.2012 № 550 «Об утверждении Инструкции об организации системы управления рисками в банках, небанковских кредитно-финансовых организациях, банковских группах и банковских холдингах»;
- Постановление Правления НБ РБ 08.01.2020 № 1 «Инструкция об управлении рисками при аутсорсинге»;
- ТТП ИБ 4.1–2020. «Требования к системам менеджмента ИБ»;
- ТТП ИБ 2.1–2020. «Менеджмент рисков ИБ».

Надеемся, что данная статья поможет «не заблудиться» в Законодательстве Республики Беларусь. Мы постарались облегчить путь изучения и применения на практике нормативных законов и подзаконных актов в области ИБ.

В следующем номере мы продолжим обзор законодательства в области информационной безопасности других стран.

«КТО В МОРЕ НЕ БЫВАЛ...»

РАДИОТЕХНИЧЕСКОЙ РАЗВЕДКЕ РОССИИ 70 ЛЕТ



Иллюстрация 1. Разведчик «Харитон Лаптев»



Борис СТОЛПАКОВ
историк криптографии

Корабли радиотехнической разведки СССР впервые появились в море 70 лет назад. К тому времени стала очевидной необходимость морской разведки средств радиолокации, радионавигации, управления, а также ближней радиосвязи прибрежных государств, прежде всего вероятных противников.

ПРИБЛИЗИТЬСЯ К ВЕРОЯТНЫМ ПРОТИВНИКАМ МОЖНО БЫЛО ЛИШЬ ПО МОРЯМ

Достаточно взглянуть на карту, чтобы убедиться: приблизиться к ним в ту пору можно было лишь по морям. Понятно, что излучения несут много информации не только о характеристиках самих радиоэлектронных средств, но и об их деятельности. И ещё одна очень важная причина принятых решений: заблаговременно обнаружить массовый пролёт стратегических бомбардировщиков с континентальной части США в направлении СССР в то время можно было только развёртыванием специально оснащённых кораблей в удалённых районах Мирового океана. 70 лет назад их было всего четыре — по одному на флот. Первые разведывательные корабли называли посыльными судами. Постепенно формировались дивизионы посыльных судов, затем их стали именовать дивизионами кораблей ОСНАЗ. В дальнейшем дивизионы на флотах были преобразованы в бригады разведывательных кораблей.

РЕЙСЫ ПОД ЛЕГЕНДАРНЫМ ПРИКРЫТИЕМ

С конца 50-х годов в военных доктринах стран НАТО всё большая роль отводилась флотам. США вели строительство первых атомных ракетных подводных лодок, авианосцев и крупных надводных кораблей. Флоты получали и новое вооружение, и самые совершенные средства управления и связи. Разведывательные корабли добывали информацию о них, находясь постоянно в море.

Походы делились на ближние и дальние. Ближними считались походы в прилегающие моря продолжительностью до 30 суток. Подготовка кораблей к выходам в море проходила в условиях особой секретности. Их команды экипировались

в гражданскую одежду, обеспечивались общегражданскими и санитарными паспортами. Легендирование судов существовало с самого начала походов. В начальный период — под рыбаков с красным советским флагом, под гидрографические суда с флагом гидрографии и полосой с серпом и молотом на трубе, затем под суда связи с военно-морским флагом.

ПЛАВАНИЯ ПРОХОДИЛИ В ТЯЖЁЛЫХ УСЛОВИЯХ

Суда имели примерно одинаковую скорость хода 9–11 узлов и автономность 25–30 суток при штате экипажа в 25–35 человек. Но реальные экипажи разведывательных кораблей были в 2–3 раза больше. При этом автономность определялась в те же 30, а иногда и более суток. Опреснителей на кораблях первого поколения практически не было. Плавание зачастую проходило в тропических широтах, когда на палубе нещадно жгло солнце, температура в машинных отделениях достигала 50 градусов, а в каютах — 35 градусов. Недостаток пресной воды чувствовался особенно остро.

ОСВОЕНИЕ МОРСКИХ РАЗВЕДЫВАТЕЛЬНЫХ ПОЗИЦИЙ

С 1962 года корабли ОСНАЗ Северного флота начали вести постоянную разведку у Восточного побережья США и в Северо-Восточной Атлантике. Корабли Тихоокеанского флота освоились в районах деятельности 7-го флота США. Это о. Гуам, Западное побережье США, Гавайские и Алеутские острова, в Японии — о. Окинава. Корабли Балтийского флота вели разведку в Балтийском и Северном морях, в Северной Атлантике; корабли Черноморского флота — в Средиземном море.

Благодаря наращиванию сил смена кораблей на позициях разведки стала происходить непосредственно в назначенных районах. Разведчики начали действовать в непосредственной близости от крупных надводных соединений стран НАТО.

Для длительного слежения за такими группировками потребовались корабли с большой автономностью и увеличенной скоростью хода. Такие суда стали поступать с 1966 года. На Северный флот прибыл «Харитон Лаптев» (илл. 1), на Тихоокеанский — «Гавриил Сарычев». Корабли совершали походы со значительным превышением автономности плавания.

К концу 1960-х годов была в основном создана система радиоэлектронной разведки ВМФ. Её корабли занимались следующим:

- ◆ вели разведку морских испытаний ракет морского базирования;
- ◆ добывали данные по ВМС США во время войны во Вьетнаме, постоянно находясь в Тонкинском заливе;

- ♦ вскрывали ход испытаний новых подводных лодок и баллистических ракет;

- ♦ участвовали в подъёме документов и образцов иностранной техники.

Так, одной из «находок» разведчиков «Харитона Лаптева» стал шарообразный аппарат полутораметрового диаметра. Он относился к новейшим на тот момент устройствам американской системы SOSUS обнаружения советских подводных лодок.

ЧТО МОЖЕТ УЗНАТЬ ВЕРОЯТНЫЙ ПРОТИВНИК?

Как известно, конец 1960-х годов стал временем серьёзного политического напряжения в мире. Например, в 1968 году одновременно происходили острый конфликт на Ближнем Востоке, война во Вьетнаме, Пражская весна и длительные массовые беспорядки во Франции. Все обострения международной обстановки особенно ощущались экипажами разведывательных кораблей, ведь они часто находились вблизи центров конфликтов. В такие моменты становился особенно актуальным вопрос: что они знают о нас, каковы возможности противника с позиции радиотехнической разведки? Определённый ответ удалось получить именно в начале 1968 года.

«ПУЭБЛО» ВЫШЕЛ В СВОЙ ПОСЛЕДНИЙ РЕЙС

55 лет назад, 11 января 1968 года, американский разведывательный корабль «Пуэбло» (AGER-2) вышел из военно-морской базы Сасебо (Япония) с задачей радиоэлектронного контроля баз и портов Северной Кореи и наблюдения за советскими кораблями.

Ему было предписано:

- ♦ вскрыть радиотехническую обстановку восточного побережья КНДР, установить дислокацию береговых радиолокаторов и параметры их излучения;

- ♦ вести техническое и визуальное наблюдение за советскими военными кораблями в проливе Цусима. Выявить цели их постоянного присутствия, начавшегося с февраля 1966 года;

- ♦ проверить информацию о том, что русские временно перевели из замерзающего порта Владивосток в порт Вонсан и на прилегающий остров Майян-До базу подводных сил Тихоокеанского флота.

Поход проходил вполне благополучно, но утром 22 января два северокорейских траулера произвели многократный круговой обход «Пуэбло», причём дистанция между кораблями сократилась до 25 м.

Поскольку корабль был обнаружен, командир отменил режим радиомолчания и приказал радистам передать донесение в радиоцентр. 23 января появилась надводная цель, быстро сближающаяся с «Пуэбло».

«ЗАНЯТ ПРОВЕДЕНИЕМ ОКЕАНОГРАФИЧЕСКИХ РАБОТ»

Это был северокорейский сторожевой катер. По приказу командира на мачте подняли сигнал «Занят проведением океанографических работ». На сторожевике подняли сигнал с требованием к «Пуэбло» сообщить свою государственную принадлежность. В ответ на мачте взвился американский флаг. В 12:10 со сторожевика на берег ушла радиограмма: «Обнаружил судно с бортовым номером AGER-2. Полагаю, что это американский разведывательный корабль. Какого-либо оружия на борту не замечено». В 12:20 на «Пуэбло» заметили приближающиеся к кораблю три торпедных катера, а в 12:27 на мачте сторожевика появился новый сигнал: «Стойте, в противном случае открываю огонь!» Американцы подняли ответный сигнал: «Нахожусь в международных водах». В 12:35 «Пуэбло» оказался в окружении, а над его мачтами несколько раз пронеслись северокорейские истребители МиГ-21.

Сторожевик дал семафор: «Следуйте за мной. У меня на борту лоцман». При этом на один из торпедных катеров перебралась группа военнослужащих. Корейцы повторили сигнал: «Стойте, или откроем огонь!» В ответ «Пуэбло» поднял сигнал «Я отбываю из района», и корабль дал ход. В 13:06 со сторожевика в штаб ушла вторая радиограмма: «...намерен изолировать личный состав AGER2, взять его на буксир и доставить в Вонсан».

«Пуэбло» не останавливался, увеличил ход и начал маневрировать. Тогда катера открыли огонь по «Пуэбло». В 13:34 «Пуэбло» остановился, его командир приказал всему личному составу покинуть верхнюю палубу и приступить к немедленному уничтожению секретных документов и аппаратуры. В результате обстрела была повреждена мачта, получили ранения члены экипажа, находившиеся на мостике, в том числе и командир. Но после того как на сторожевике был поднят сигнал «Следовать за мной для приёма на борт лоцмана», «Пуэбло» в 14:30 вновь дал ход.

Попытка оторваться от катеров окончилась для американцев печально: в результате повторного обстрела были ранены ещё несколько человек, сжигавших в районе трубы секретные документы. Обо всех событиях, происшедших на корабле, известили радиоцентр. В ответ сообщили о направлении в район инцидента нескольких самолётов, но они так и не появились. «Пуэбло» застыл на месте, на борт корабля поднялась досмотровая группа. Экипаж «Пуэбло» собрали на палубе, всем связали руки, а глаза прикрыли тёмными повязками. Корабль взяли на буксир и в 20:30 привели в порт Вонсан, откуда американских моряков доставили на железнодорожный вокзал, там их уже ожидал поезд. Утром 24 января поезд прибыл в Пхеньян, и моряков поместили в тюрьму.

В результате вооружённого инцидента погиб один и были ранены девять членов экипажа.

В ШАГЕ ОТ ВОЙНЫ

23 января после известия о задержании «Пуэбло» в 15:06 командующий Седьмым флотом приказал атомному ударному авианосцу «Энтерпрайз», атомному ракетному лидеру эсминцев и трём эсминцам немедленно перейти в южную часть Цусимского пролива. В 19:21 поступил приказ о размещении эсминцев как можно скорее у порта Вонсан вне территориальных вод КНДР на расстоянии 12 миль от берега, чтобы «быть готовыми участвовать в действиях по освобождению „Пуэбло“». Президент Джонсон собрал совещание. Рассматривались различные варианты ответа: воздушный удар по Вонсану, минирование гавани и морская блокада. Но эти меры не были эффективны для оказания давления на КНДР, а только вели к возможному развязыванию войны. В этот момент ситуация могла привести к прямому столкновению между советским и американским флотами.

ОПАСНОЕ ПРОТИВОСТОЯНИЕ

Тихоокеанский флот сразу взял под наблюдение действия американцев. Гидрографическое (разведывательное) судно «Гидролог» встретило американскую группу во главе с атомным ударным авианосцем «Энтерпрайз» 23 января, едва она вышла из Сасебо. Причём «Гидролог» заблокировал путь движения авианосца «Энтерпрайз». Авианосцу даже пришлось дать задний ход. Утром 24 января два самолёта «Ту-16» выполнили разведывательный полёт над акваторией Японского моря. А в Вашингтоне 24 января при обсуждении ответных действий советник по национальной безопасности Ростоу предложил дать приказ южнокорейским ВМС захватить советское судно, следующее за авианосцем «Энтерпрайз». Подобный «симметричный» ответ мог иметь тяжёлые последствия, ведь по американским данным за авианосцем «Энтерпрайз» во время его перехода шла советская атомная подводная лодка, и неизвестно, какой приказ имел её командир на подобный случай. Вечером 25 января советский сторожевой корабль сопровождал американский эсминец, шедший из Сасебо для присоединения к ударной группе. 27 января большой ракетный корабль «Неудержимый» присоединился к «Гидрологу» и сторожевому кораблю для отслеживания действий американцев. «Неудержимый» вёл наблюдение с расстояния в 11–12 миль, при необходимости это гарантировало эффективное использование противокорабельных крылатых ракет.



Иллюстрация 2. Приборное помещение «Пуэбло»

УСИЛЕННО РАБОТАЛА ДИПЛОМАТИЯ

Американцы продолжали наращивать свою корабельную ударную группу, но усиленно работала и дипломатия. Ещё 23 января посол США в Москве Томпсон попросил о срочной встрече в МИД СССР и передал просьбу своего правительства оказать содействие в возвращении захваченного судна и его экипажа. 24 января командующий Тихоокеанским флотом США приказал кораблям оставаться на расстоянии 80 миль от побережья Северной Кореи. Кроме того, были прекращены разведывательные полёты в Японском и Жёлтом морях. 24 января американский представитель в Военной комиссии по перемирию в Корее вступил в контакт с представителем КНДР.

НЕОЖИДАННАЯ ПРЕСС-КОНФЕРЕНЦИЯ

Как выяснилось, ни одна из сторон не считала свои действия противоправными, и они по-разному оценивали место происшедшего инцидента. Американцы настаивали на том, что захват их судна произошёл за пределами 12-мильных территориальных вод. Северокорейская сторона оправдывала свои действия тем, что американский корабль вторгся в её внутренние воды. Ссылаясь при этом на постановление своего правительства, в котором наряду с установлением ширины территориальных вод значительная часть Восточно-корейского залива, где произошло задержание «Пуэбло», объявлялась внутренними водами КНДР.

25 января в американской прессе зазвучали призывы нанести удар по порту Вонсан и силой освободить «Пуэбло». Основной причиной, по которой бомбардировка не состоялась, явилось то, что уже 26 января в Пхеньяне на пресс-конференции командир «Пуэбло» признал: экипаж корабля занимался шпионажем.



Иллюстрация 3. «Пуэбло» в Пхеньяне

БЛОК ЛИКВИДАЦИИ НЕ БЫЛ ПРИВЕДЁН В ДЕЙСТВИЕ

Американская сторона требовала возвращения судна и экипажа. В ответ корейская сторона настаивала на том, чтобы США принесли извинения и убрали свои войска. К этому времени у побережья Кореи было сосредоточено уже 32 надводных корабля ВМС США, в том числе три ударных авианосца, среди них атомный авианосец «Энтерпрайз». Одновременно в КНДР уже началось изучение аппаратуры и документов с «Пуэбло». В приборном помещении корабля (илл. 2) обнаружили блок ликвидации, начинённый динамитом, но так и не приведённый в действие.

ПРОСЬБА «ПРОЯВИТЬ СНИСХОДИТЕЛЬНОСТЬ»

Наконец 8 мая на переговорах представитель КНДР предложил свой вариант заключительного документа:

«Правительство США, подтверждая обоснованность признаний экипажа американского корабля „Пуэбло“ и документальных доказательств, предъявленных представителем правительства КНДР в отношении того, что корабль, который был захвачен в порядке мер самообороны, принятых военными кораблями Корейской народной армии в территориальных водах КНДР

23 января 1968 года, неоднократно вторгался незаконно в территориальные воды КНДР и занимался разведкой важных военных и государственных секретов КНДР, берёт на себя полную ответственность и торжественно приносит извинения за то, что американский корабль вторгся в территориальные воды КНДР и совершил серьёзную разведывательную деятельность в отношении КНДР, и даёт твёрдую гарантию, что американские корабли впредь не будут больше вторгаться в территориальные воды КНДР. Вместе с тем правительство США, принимая во внимание тот факт, что члены бывшего экипажа американского корабля «Пуэбло», задержанного стороной КНДР, откровенно признались в своих преступлениях и обратились к правительству КНДР, обращается к правительству КНДР с настоятельной просьбой проявить снисходительность в отношении членов экипажа».

Американский представитель должен был подписать этот документ от имени правительства США. Наступила продолжительная пауза — более полугода. Всё же 23 декабря подпись была поставлена. После этого 82 члена экипажа и тело погибшего матроса вернулись домой, а «Пуэбло» остался на приколе в гавани Вонсан (до 1999 года). Ныне корабль используется как туристический объект в Пхеньяне (илл. 3).

ТОРГОВЛЯ КОПИЯМИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

В США допускали, что шифрмашины с «Пуэбло» попали, хотя бы и в повреждённом состоянии, в руки советских криптоаналитиков. Но ежесуточная смена ключей внушала специалистам АНБ уверенность, что потери не катастрофичны. После внесения конструктивных изменений использование этих шифрмашин возобновилось.

До середины 1980-х в США не знали о налаженной американскими связистами торговле копиями месячных комплектов ключей. Ещё в 1967 году Джон Энтони Уокер, дежурный офицер связи в штабе командующего подводным флотом США в Атлантике, приехал в Вашингтон и, подойдя к входу в посольство СССР, пожелал поговорить с кем-либо из службы безопасности. Он принёс тогда для продажи месячные комплекты ключей для шифровальной машины «KL-47» и заявил, что имеет неограниченный доступ к шифровальной аппаратуре и ключам. Это были не пустые слова. Так, с 1971 по 1974 год Джон Уокер проходил службу на корабле снабжения ВМС США «Ниагара Фоллз», который обеспечивал и деятельность американских войск, воевавших во Вьетнаме. На корабле находились секретные документы и ключи к шифровальным машинам, имевшимся на кораблях, включая подводные лодки и авианосцы, на шесть месяцев вперёд, а также большое количество ключей для американских сухопутных войск во Вьетнаме. Советской разведке стали доступны и ключи ВВС США, которые использовались для шифрования приказов стратегическим бомбардировщикам «В-52» при их налётах на Вьетнам.

В характеристике, подписанной флотским начальником Уокера в 1972 году, говорилось: «Джон Уокер в высшей степени лоялен. Отличается обострённым чувством долга и личной порядочностью в сочетании с большим чувством юмора. Дружелюбен, умён, прекрасно уживается с другими». Кое-что здесь вполне справедливо. Ведь Джон сумел вовлечь в продажу криптографических секретов брата, сына и даже своего стажёра, заменившего его на службе.

Особая ценность полученной через Уокера информации заключалась в возможности узнавать заранее об американских планах. Бывший глава резидентуры ЦРУ в Сайгоне с горечью вспоминал, что «на заключительном этапе войны во Вьетнаме противник обычно знал заранее о рейдах бомбардировщиков „В-52“. Даже когда из-за плохой погоды самолёты уходили на запасные цели, вьетнамцам было уже известно, по каким из них будет нанесён удар». Да и на американском флоте замечали, что при проведении секретных маневров поблизости всегда оказывались советские корабли: «Как будто у них были дубликаты наших оперативных планов».

АТАКА В СТУДЁНОЙ НОЧИ

Опасные инциденты происходили и с советскими кораблями разведки. Первая вооружённая провокация случилась ночью 28 декабря 1959 года против корабля «Унго» (илл. 4) у восточного побережья Кореи.



Иллюстрация 4. Судно радиотехнической разведки «Унго» (ГС-34)

Тогда с целью обеспечения скрытности активную радиолокационную станцию не включали. Вдруг наши моряки увидели силуэты трёх кораблей без ходовых огней и каких-либо других опознавательных знаков. Корабли быстро приближались. Один из них, без флага, не отвечая на запросы, прямо шёл на сближение и был опознан как малый противолодочный корабль. Командир «Унго» приказал направить один из прожекторов на гидрографический флаг ВМФ СССР, а вторым прожектором — освещать приближающийся к нему иностранный корабль. Почти у самого борта «Унго» тот развернулся и лёг на обратный курс.

В 20 часов 40 минут тот же корабль вновь приблизился и без предупреждений дал по безоружному «Унго» четыре очереди из 40-миллиметровых автоматических установок. Затем «пират» скрылся. На судне был разбит компас, повреждена радиоантенна, пострадал и корпус корабля. «Унго» уменьшил ход и лёг в дрейф, а «пират» вновь приблизился и открыл огонь. Один из снарядов попал в ходовую рубку, вахтенный рулевой матрос был убит. Раненый сигнальщик продолжал освещать флаг своего корабля, а пиратский корабль стоял так близко, что наши моряки успели подробно рассмотреть его. Подержав луч прожектора на советском флаге, «пират» неторопливо ушёл в сторону. Ушли во тьму и два других корабля.

В район инцидента вылетали самолёты ИЛ-28 авиации флота, и по тревоге был послан дежурный эсминец «Веский», он принял на борт раненых моряков. «Унго» своим ходом дошёл до базы.



Иллюстрация 5. Средний разведывательный корабль «Юрий Иванов»

СПАСАЛИ ЛИШЬ ИСКУСНОЕ МАНЕВРИРОВАНИЕ И ХЛАДНОКРОВИЕ

Большинство инцидентов связано со временем войны во Вьетнаме после вторжения американцев в 1964 году (1964–1975 гг.). Как известно, контингент США достигал 540 тысяч человек. Американские корабли в Южно-Китайском море шли тогда на прямое столкновение с советскими разведывательными судами. К счастью, обычно всё заканчивалось без серьёзных повреждений. Опаснее были нападения южновьетнамских патрульных катеров, нередко открывавших огонь на поражение и принуждавших следовать к берегу. Тогда спасали лишь искусное маневрирование и хладнокровие.

ВРЕМЯ РАСЦВЕТА И ВРЕМЯ ВОЗРОЖДЕНИЯ

В период конца 1960-х — начала 1970-х годов начался расцвет морской радиоэлектронной разведки. Строились новые суда, численность разведывательных кораблей в ВМФ приблизилась к 50 и поддерживалась на этом уровне более 20 лет. Экипажи в автономном плавании стали получать специальный морской паёк. В состав пайка входили: вобла, сухое вино, шоколад, соки, копчёности, стужённое молоко. В море иногда одновременно находилось до 10 кораблей разведки.

Разведывательные корабли Тихоокеанского флота во время войны во Вьетнаме постоянно располагались в Тонкинском заливе. Причём их командиры должны были своевременно определить подготовку палубной штурмовой авиации США к ударам по берегу и доложить об этом командованию.

С развитием радиоэлектроники и гидроакустических средств в начале 1980-х годов была открыта возможность сверхдальнего обнаружения подводных лодок. Тогда же утвердился термин «освещение подводной обстановки» (ОПО).

Создание и внедрение комплексов ОПО на разведывательные корабли было ответом на американские системы гидроакустического наблюдения «СОСУС».

С тех пор средства нападения и обороны существенно изменились, обновились и задачи их разведки. С декабря 2004 года, после длительного перерыва, в России началось строительство серии новых кораблей радиоэлектронной разведки (илл. 5). По мореходным качествам и техническому оснащению эти корабли намного превосходят своих предшественников.

По сообщениям американской прессы, в мае 2021 года корабль наблюдения ВМФ России провёл несколько дней у западного побережья Гавайских островов.

КАК НАШЕ СЛОВО ОТЗОВЁТСЯ?

К СТОЛЕТИЮ РАСЦВЕТА «ЛУЗИТАНИИ»



Борис СТОЛПАКОВ
историк криптографии

В нынешнем году, объявленном годом педагога и наставника, особенно значимой представляется память о событиях, связанных со становлением и расцветом легендарной «Лузитании». Это было уникальное содружество преподавателей, студентов и увлечённой наукой молодёжи. Именно на основе «Лузитании» сложилась и утвердилась советская математическая школа, получившая мировое признание.

«ЗА РЕКОЮ — МЕДВЕЖЬИ БЕРЛОГИ»

Возникновение «Лузитании» в годы Первой мировой и Гражданской войн связано с Московским университетом и личностью Николая Николаевича Лузина, его выпускника предвоенных лет.

Сибиряк Н. Н. Лузин попал в Москву и стал математиком, можно сказать, неожиданно для него самого. Он родился в Иркутске 140 лет назад. Позже семья переехала в Томск. И отец, и мать Николая Николаевича были русско-бурятского происхождения.

В последние годы жизни Лузин ярко и увлекательно вспоминал своё детство. «Томск стоит на берегу небольшой реки Томь. За рекою — медвежьи берлоги. У моих сверстников был культ физической силы; вполне понятно почему: близость столь сильных зверей, как медведи, и рассказы о них заставляли видеть в физической силе высшее благо.

Я был физически очень слабым (хотя и нормальным) и робким. Товарищи хотели меня приохотить к их интересам и, злоупотребляя своею силою, достигали обратного. Я просто боялся быть в их обществе и уединялся, когда только мог. Был в Томске единственный книжный магазин, в нём полная мешанина книг, разбираться в которой я быстро приохотился. Я был единственным ребёнком у моих

родителей. Отец — торговый служащий, оба были полубразованны, но всё же читать и писать могли. Понимая моё отчуждение от товарищей, они предоставили мне полную свободу действий внутри меня самого. За эту свободу — вечное им спасибо! Моя голова была полна миром фантазии. Я читал буквально всё, что видел на прилавке книжного магазина, и, конечно, ничего не понимал. Я читал Канта «Критику чистого разума» раньше романов Жюль Верна. Книги философские больше всего меня привлекали, потому что я их не мог понять, и я искал тайного смысла их, хотел понять его, похитить его, даже «силом». Жюль Верна я считаю своим учителем, так как именно он привил мне веру в науку, любовь к ней и жажду сделаться инженером.



Николай Николаевич Лузин (1883–1950)

Но я хорошо понимал, что без математики невозможно быть инженером. И я пожелал овладеть ею».

Учителя в Томской гимназии, по воспоминаниям Николая Николаевича, были весьма средними людьми, перемещёнными из европейской части России в основном не по своей воле, и не лучших человеческих качеств. Учителя по математике заставляли своих учеников учить наизусть доказательства теорем и правила действий.

«Я СТАЛ ВСЁ ОТСТАВАТЬ И ОТСТАВАТЬ...»

«Механическая память у меня была слабая, и я стал всё отставать и отставать. Учился я средне из-за «фантастики» и неспособности к зазубриванию. Я стал приносить из гимназии отметки по математике 4, потом 3, потом 2. Здесь отец нанял мне репетитора. Репетитор был взят отцом из студентов Томского политехникума, недавно открывшегося в Томске. Студент, благодаря моей судьбе, оказался очень даровитым. Он заметил мою неспособность к механическому запоминанию и поставил дело на дальнейшее развитие фантазии, оплодотворённой логикой. Именно он прямо заставил меня решать задачи из задачника Рыбкина по тригонометрии и геометрии. Когда же я стал возражать, говоря, что для этого надо знать теорию, т.е. зубрить, он отвечал: «Ну она-то Вам и будет ясна из практики». Короче, я, минуя зубрёжку, прямо начал под его наблюдением решать задачи, справляясь с теорией по мере лишь необходимости и беря из неё лишь то, что непосредственно нужно было для решения задачи и получения ответа, указанного в задачнике. Мои отметки по математике стали повышаться, возвратилась 3, потом 4 и через год и 5. Я стал лучшим «решателем» задач в классе. Я хотел идти в инженеры, именно в морские, под влиянием Жюль Верна».

«КОНКУРС — 4-5 СОПЕРНИКОВ НА ОДНО МЕСТО»

Ближе к окончанию гимназии обрисовалась новая проблема: в Морском училище Петербурга, куда Николай собирался поступать, на инженерные специальности установился высокий конкурс — 4-5 соперников на одно место.

«Будучи робким, я отказался идти на конкурс. Тогда отец посоветовал поступить на физико-математический факультет, так как, после двухлетнего учения, молодые люди, сдав экзамены за два года, могли поступить в Морское училище без конкурса. Это решило мою судьбу: я поехал в Москву и поступил на Математическое отделение Московского университета с отращиванием к математике. Но на первой же лекции незабвенного профессора Николая Васильевича Бугаева я услышал буквально следующее: «Поздравляю вас с поступлением. Вы, конечно, пошли сюда, движимые голосом сердца. И, конечно,

вы хотите сделаться знаменитыми математиками. Так вот вам указание и рецепт: для этого надо забыть элементарную математику. Забудьте как можно полнее, до конца, и начинайте снова всё заново: математика высшая есть самая высокая музыка, самое высокое искусство, это — гармония общих идей и интуиции». Я понял, что мне теперь не уйти от проф. Бугаева, пока я не пойму до конца то, что он обещал. И я остался, пройдя два года, ещё на два года, чтобы кончить математическое отделение».

«ОБЯЗАННОСТЬ МАТЕМАТИКА КО ВСЕМУ ОТНЕСТИСЬ КРИТИЧЕСКИ!»

Главным учителем и наставником для Лузина в годы учёбы (1901-1905 гг.) стал Дмитрий Фёдорович Егоров, крупный математик и педагог. Он же оставил Лузина при университете для подготовки к профессорскому званию, теперь это называется аспирантурой.

Николай Николаевич тяжело переживал смутное революционное время, да и засомневался в выборе математики как профессии. Егоров выхлопотал ему командировку в Париж и постоянно поддерживал в письмах. Он писал своему ученику: «Часто в основе непреложных, по-видимому, выводов лежат шаткие и произвольные основы. Вспомните, что Вы математик и что обязанность математика ко всему отнестись критически! А что касается до руководства в жизни, то ведь человеку дан не один разум; и чуткая совесть всегда подскажет, что задача жизни в том, чтобы по мере сил делать добро...» «Необходимо наряду с научной работой и ещё чем-нибудь интересоваться. Посмотрите Париж, его музеи, церкви, окрестности; всё это очень интересно». «Вполне одобряю Ваше намерение остаться в Париже: судя по Вашим письмам, там так много теперь читается интересного, что жалко было бросать в середине; экзамены же успеете сдать осенью». «Научная работа имеет много общего с поэтическим творчеством, и всякое приращение (со стороны или от себя лично во имя какого-нибудь принципа) здесь ни к чему не приводит. Единственно, что следует иметь в виду, это заложить солидный фундамент для будущего, и это приходится делать именно в начале работы».

В 1908 году Лузина приняли на должность приват-доцента Московского университета, и он занялся совместными с Егоровым исследованиями. Уже в 1910 году Николай Николаевич отправился в научную командировку в Германию и Францию.

«ВЫ, МОЖЕТ БЫТЬ, И В МАТЕМАТИЧЕСКОМ ОБЩЕСТВЕ НЕ БЫВАЕТЕ?»

Вновь Егоров напутствовал его в письмах: «По-видимому, Вы до сих пор стесняетесь вступить в более близкие отношения с Гёттингенскими

математиками. Разве это можно?! Ведь тогда и не стоило ехать в Гёттинген: книги читать можно было и в Москве, а собственно лекции много нового дать Вам не могут. Всё дело в более близком общении, при котором Вы много ценного узнаете. Вы, может быть, и в математическом обществе не бываете? Тогда это уж совсем непростительно! Итак, скорее навёрстывайте потерянное время и идите хоть к Ландау, который настолько любезен, что при затруднениях в немецком языке прибегнет и к французскому. А затем на всех совершенствуйтесь в немецком разговоре: практикуйтесь, говорите со всяким встречным! И затем в ближайшем будущем представьтесь Клейну и Гильберту».

«От знакомых я услышал, что Вы нехорошо себя ведёте: опять переутомились работой и чувствуете себя плохо. Мой совет Вам ехать на Ривьеру, например, в Сан-Ремо. Не теряйте времени и поезжайте, а то в Гёттингене поправляться трудно. Математику не затрагиваю; Вам лучше от неё отдохнуть». «Очень рад, что Вы познакомились с французскими математиками, и в том числе с Борелем. Теперь Ваше пребывание в Париже будет плодотворно гораздо более, чем прежде». «Вам дарован математический талант, и Вы должны его сохранить, а равным образом и постараться, чтобы пришедшие Вам счастливые идеи не остались бесплодными. А потому возьмите себя в руки и займитесь прежде всего своим моральным лечением. Без нравственной уравновешенности научная работа не может успешно идти».

ЛЕКЦИИ НИКОЛАЯ НИКОЛАЕВИЧА БЫЛИ ВПЕЧАТЛЯЮЩИМИ

Незадолго до начала Первой мировой войны, летом 1914 года, Лузин вернулся в Москву. Вскоре он защитил докторскую диссертацию и стал профессором Московского университета. К этому времени заботами Д. Ф. Егорова уже и студенты готовы были воспринимать его лекции по новой тогда тематике теории функций. А лекции Николая Николаевича были впечатляющими. Вот отзывы маститых математиков, когда-то первых его студентов.

«Это был удивительный лектор. Все мы испытывали необыкновенное увлечение, мы чувствовали себя взволнованными почти как в Художественном театре». «Я впервые встретился с Н. Н. Лузиным, будучи студентом второго курса. Впечатление от этой встречи было, можно прямо сказать, потрясающим и навсегда запомнилось мне. Даром увлекать умы и воспалять сердца Н. Н. Лузин обладал в высшей степени». Ещё только взрослеющих учеников «поражали большая свобода и непринуждённость, отсутствие всякой официальности и замена внешних проявлений почтительности со стороны студентов действительно глубоким уважением». «Лекции Николая Николаевича не кончались со звонком; беседа продолжалась и в

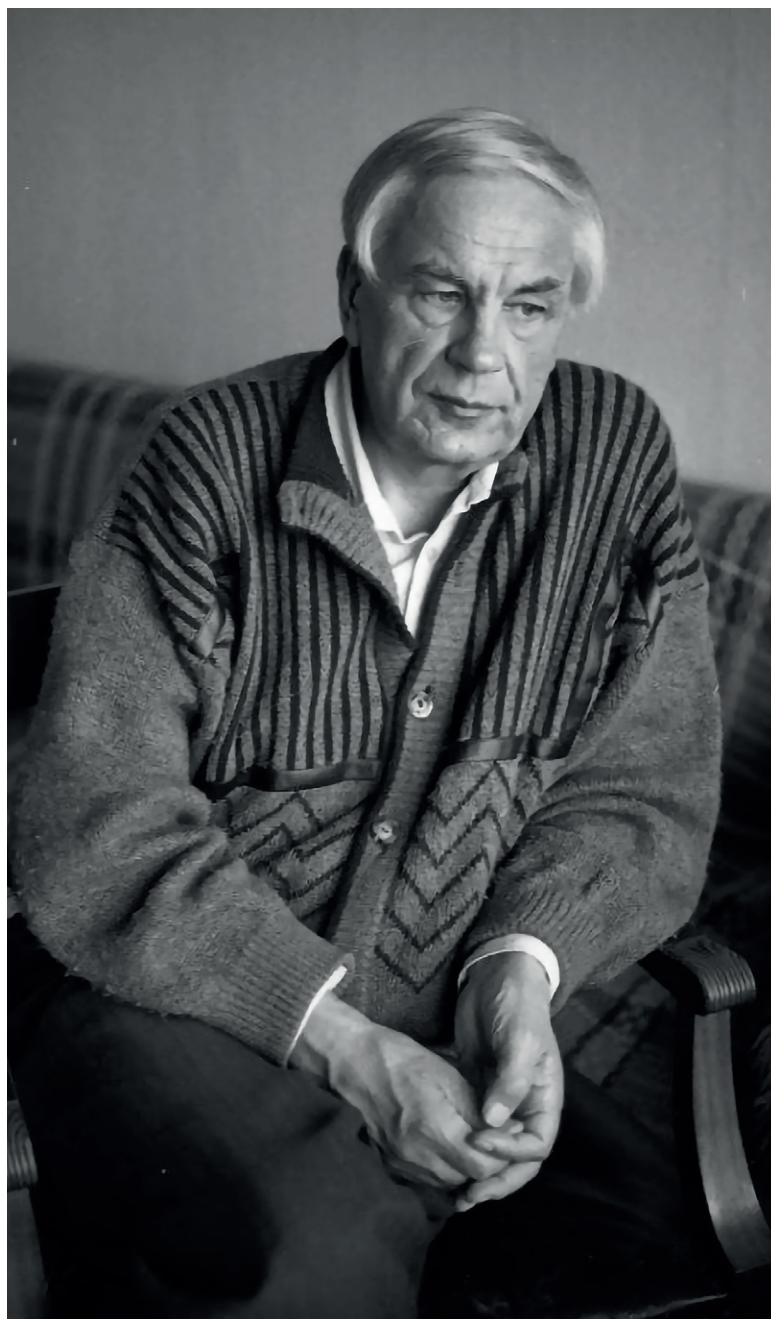


Дмитрий Фёдорович Егоров (1869–1931)

перерыве между лекциями в коридоре, а весьма часто слушатели провожали его гурьбой по окончании лекций до его квартиры».

«ПРЕЗРЕВ КЛАССИЧЕСКИЙ АНАЛИЗ, ЗДЕСЬ СОВРЕМЕННЫМ УВЛЕКАЛИСЬ»

«Лузин беседовал с нами. И была такая непринуждённая товарищеская беседа. И здесь он новые задачи ставил. И вот одну из этих задач я решил тогда. Лузин очень заинтересовался и пригласил к себе на квартиру для того, чтобы поговорить со мной о тех задачах, которые в этом направлении можно решать. И у нас была увлечённая беседа примерно в течение трёх часов». «В 1915/16 учебном году, когда я уже был на четвёртом курсе, он прямо приглашал к себе на квартиру, была одна группа, и мы все вместе обсуждали вопросы. Иногда семинар продолжался до двух часов ночи. И мы видели, как надо вести научную работу». «Тут началась революция. Революция Февральская только



Игорь Ростиславович Шафаревич (1923–2017)

была, ещё условия примерно оставались старые, и мы продолжали интенсивно заниматься математикой. Осенью этого года Лузин рекомендовал мне (Д. Е. Меньшову — Б.С.), Александрову и Хинчину написать заметки во Французской Академии наук. И эти три заметки были направлены Адамару». Надо сказать, что Н. Н. Лузин взял на себя редактирование статей как с русским текстом, так и по-французски, а также их отсылку Ж. Адамару. «Он много времени на это тратил. Считаю, что лучший способ почтить его память — вести работу с молодёжью так же тщательно и основательно, как он вёл с нами». Постепенно вокруг Лузина «образовалась дружная семья молодёжи, охваченная горячим интересом к разработке научных задач».

ЖИЗНЬ С «ИНТЕЛЛЕКТУАЛЬНЫМ ОЗОРСТВОМ»

«Лузитаны» — так называли себя в начале 1920-х годов молодые математики, объединившиеся вокруг своего учителя. Они собирались главным образом в квартире Н. Н. Лузина на Арбате. Хотя это было время общей разрухи в стране и Москве, молодые «лузитаны» жили «не только напряжённой математической жизнью, но и жизнью, которая была непосредственно радостной», с юмором и «интеллектуальным озорством», по их собственным отзывам. «Лузитания» неизменно пользовалась авторитетной поддержкой Д. Ф. Егорова, он перед революцией был назначен помощником ректора университета, в 1921 г. стал вице-президентом Московского математического общества, а с 1923 г. — его президентом.

«А ДАЛЬШЕ ВСЁ...»

К середине 1920-х годов «лузитаны» осознали свою силу, приобрели собственный авторитет. Достаточно напомнить лишь некоторых учеников Н. Н. Лузина: А. Н. Колмогоров и П. С. Александров, М. А. Лаврентьев и П. С. Новиков, А. Я. Хинчин и Д. Е. Меньшов... Уже вскоре более десяти из них стали членами Академии наук. Они создали собственные научные школы, которые все вместе составили славу советской математики. Уже ученики учеников становились докторами наук и академиками.

«А дальше всё как будто просто — процесс естественного роста,

Тематика всё расширялась, своей дорогой каждый шёл —И школа Лузина распалась на ряд блестящих новых школ.

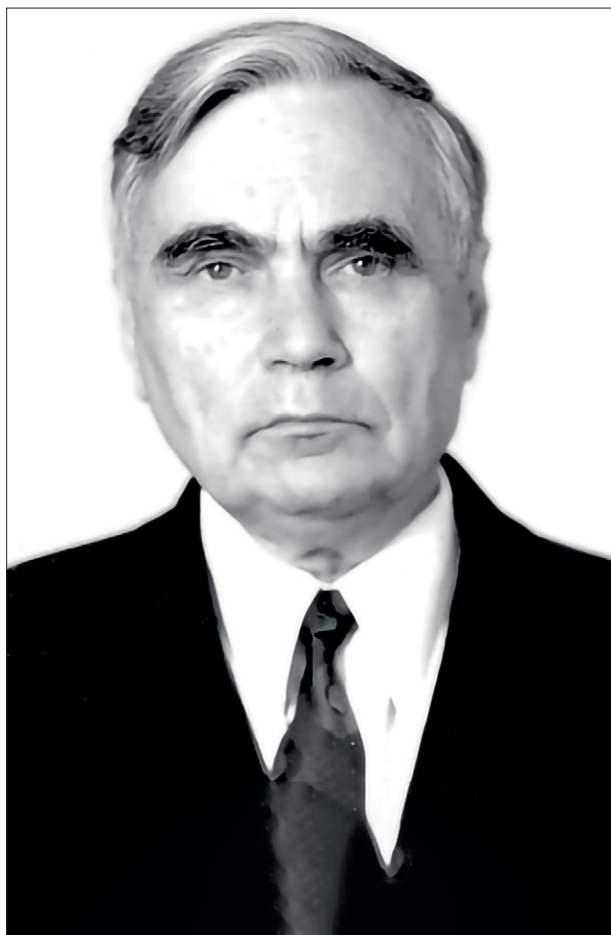
Но был мучительно тяжёлым процесс распада этой школы...» (Воспоминания одного из именитых учеников).

Свидетельством окончательного распада школы Н. Н. Лузина стали «дело Егорова» и «дело Лузина». Первое из них — уголовное, а второе — внутреннее академическое, но политическое. Д. Ф. Егорова арестовали в 1930 г. по делу «о катакомбной церкви» вместе с философами П. А. Флоренским и А. Ф. Лосевым, в 1931 г. он умер в тюремной больнице. Н. Н. Лузин остался в академиках, но с 1936 г. до конца своих дней носил клеймо «врага в советской маске».

ОТКРОВЕННО ОБ ИДЕАЛЬНОМ ЧИТАТЕЛЕ

Педагогическое наследие Н. Н. Лузина остаётся по-прежнему актуальным и востребованным. Вот, например, фрагмент написанного им предисловия к учебнику «Курс математического анализа» И. И. Жегалкина и М. И. Слудской (1935 г.).

«Основная идея И. И. Жегалкина — совершенно ясно осознанная им невозможность исходить при составлении учебника от обычного представления



Владимир Яковлевич Козлов (1914–2007)



Нина Карловна Бари (1901–1961)

об идеальном читателе. А между тем большинство учебников именно и отправляется от этого представления, наделяя этого абстрактного читателя беспредельными внимательностью, понятливостью, догадливостью и сообразительностью. Для этого читателя нет ни в чём никаких затруднений и препятствий: достаточно автору хотя бы один раз указать на какое-нибудь обстоятельство, как этот идеальный читатель уже понимает его с полуслова и запоминает если не на всю жизнь, то, во всяком случае, на всё время изучения книги... Когда вдумываются в причины возникновения иллюзии „идеального читателя“, то немедленно замечают, что под таким читателем автор просто понимает себя самого и именно то самое состояние своего ума, которое он имел в момент создания учебника, но отнюдь не то состояние ума, которое было у автора, когда он сам впервые знакомился с излагаемыми им идеями. Об этом последнем обычно говорят очень неохотно, вспоминая его исполненным всяких недоумений и рассматривая его по этому как «неправильное», тогда как именно оно самое и было вполне «правильным», потому что являло действительность, наблюдаемую у всех без исключения. В действительности первые движения изучающего ума всегда исполнены всяческих сомнений, недоумений и заблуждений...»

О «МАТЕМАТИЧЕСКИХ ВНУКАХ И ПРАВНУКАХ»

Отрадно, что педагогическую традицию, начатую Д. Ф. Егоровым и Н. Н. Лузиным, сохранили их ученики и последовавшие поколения учеников. Ярким тому свидетельством явился недавний столетний юбилей Игоря Ростиславовича Шафаревича, выдающегося математика и замечательного педагога и мыслителя. И. Р. Шафаревич принадлежал к «математическим правнукам» Н. Н. Лузина.

К поколению «математических внуков» Н. Н. Лузина принадлежал и В. Я. Козлов, крупный математик и выдающийся деятель и педагог в области криптографии.

Владимир Яковлевич ещё в годы учёбы был отмечен весьма престижной премией Московского математического общества для молодых учёных. Его наставницей тогда была Нина Карловна Бари, талантливая и преданная ученица Н. Н. Лузина.

По подсчётам исследователей, к настоящему времени «Родословное математическое древо Н. Н. Лузина» насчитывает около пяти тысяч математиков, заметно проявивших себя. Результат уникальный!

ЗАМКИ НА ПЕСКЕ

ЗАМЕТКИ БЕЗОПАСНИКА

Александр ИГОНИН
эксперт BIS Journal

В ИТ-индустрии специалистов, которые разрабатывают сложные системы и определяют их поведение, именуют архитекторами. Задолго до появления ИТ-технологий так называли людей, которые проектировали здания и сооружения. Эта схожесть в названии профессии неспроста: построить сложную информационную систему порой немногим легче, чем воздвигнуть многоэтажный дом.

В отрасли ИБ тоже есть архитекторы. Ими часто называют тех, кто проектирует систему защиты организации. И аналогия со строительством и здесь видна очень хорошо, а уж какое именно «здание» в итоге получится, зависит от бюджета, сроков, команды, используемых технологий, а также степени зрелости ИТ-инфраструктуры. Развивая эту мысль, интересно подумать, а что же можно тогда сравнить с фундаментом системы защиты информации? На этот счёт можно долго дискутировать, и у каждого опытного ИБшника наверняка будет своё мнение. Со своей невысокой колокольни я бы сказал, что фундамент — это очень базовые процессы, причём из области скорее ИТ, чем ИБ. Навскидку я бы назвал следующие.

- ♦ Управление сетевыми активами: отлаженный и реально работающий процесс добавления (и удаления!) элементов корпоративной сети. У компании должна быть централизованная база данных своих цифровых активов. И когда что-то новое где-то в сети появляется, в этой базе должна появляться новая запись, а когда актив выводится из эксплуатации, в базе напротив него должна ставиться соответствующая пометка.

- ♦ Управление учётными записями: всё то же самое, но в отношении пользовательских (и сервисных) аккаунтов и назначенных им прав.

- ♦ Управление процессами и документированием: опять абсолютно те же принципы, но в отношении процессов и документов.

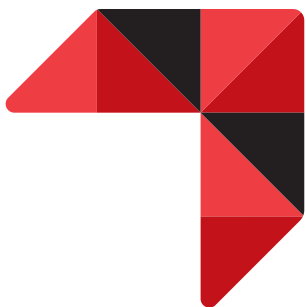
Нетрудно заметить простую, но чрезвычайно мощную общую мысль, объединяющую все эти пункты: **появление любого нового объекта, его изменение и вывод из эксплуатации должны сопровождаться соответствующим документированием.**

Всё это, конечно, не новость, и перечисленные рекомендации в той или иной форме кочуют из стандарта в стандарт. Вспомним хотя бы NIST Cybersecurity Framework, стандарт ISO/IEC 27001 и его российского «брата» ГОСТ Р No ИСО/МЭК 27001–2021. Тем не менее на практике дела с этим обстоят очень и очень плохо. Автор заметок в своей карьере повидал немало крупных корпоративных инфраструктур, и, например, степень инвентаризации хостов сети по ощущениям мало где доходила даже до 70%. Наверное, плюс-минус такой же (если не меньший) уровень был и в двух остальных рассмотренных областях.

Разумеется, тезис о том, что же именно является фундаментом системы защиты информации, можно оспорить. Но если хотя бы отчасти согласиться с изложенной выше точкой зрения, то становится очевидно, что на полусыром фундаменте крепкого здания не построить. По этой причине автор всегда испытывает богатую гамму чувств, когда в очередной раз видит, как крупная компания с упорством, достойным лучшего применения, сосредоточенно внедряет сложный комплексный продукт для защиты информации, при этом не имея толком представления о том, как же работает её сеть или хотя бы из каких узлов она состоит. КПД такого внедрения обычно невелик, а в особо выдающихся случаях может и вовсе быть отрицательным.

К сожалению, «продавать» руководству «фундамент» сложно, особенно когда приходится конкурировать с красочными презентациями воздушных замков, которые якобы сделают драгоценное ИТ-болото заказчика полностью неприступным для хакеров. А ведь от того, насколько прочны «сваи», зависит надёжность всей системы защиты. И нужно всегда помнить, что какой бы скучной, рутинной, некрасивой и бессмысленной ни казалась работа по выстраиванию базовых процессов в ИТ-инфраструктуре, без неё нельзя всерьёз говорить ни о каком обеспечении безопасности. Потому что в отсутствие этого фундамента все усилия в конечном счёте занесёт песком сумятицы и неразберихи случайных изменений.





АВАНГАРД



BIS JOURNAL



IB-BANK.RU



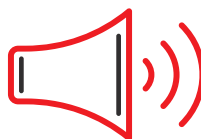
BIS TV

Медиа Группа «Авангард»

обеспечивает эффективную многоуровневую
бизнес-коммуникацию на рынке ИБ



проводит знаковые
деловые мероприятия
отрасли



предлагает самые
широкие возможности
медийного освещения



производит
видео контент



предоставляет
медиа ресурсы
для решения ваших
маркетинговых задач



Воспользуйтесь уникальным
опытом и медийными площадками
«Авангарда» — с нами вы донесёте
информацию до аудитории
самым эффективным способом!

Kaspersky Unified Monitoring and Analysis Platform



Центральный элемент вашей системы
безопасности



kaspersky АКТИВИРУЙ
БУДУЩЕЕ

Реклама. АО «Лаборатория Касперского», 125212, г. Москва, Ленинградское шоссе, д. 39А, стр.2.