

BIS

JOURNAL

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ
БИЗНЕСА

№1 (60) 2026

Анатолий
АКСАКОВ

Госдума
«Это не будет
навязчивой
кампанией»
→ 4



Игорь
ШЕРЕМЕТ

РАН
Что ждет
мировую отрасль
ИИ в 2026–30 гг.
→ 72



Цифровой рубль:
«А от тебя,
мошенница,
я точно уйду!» → 4

Безопасность
КИИ: эволюция
доверия → 16

РБПО. Испытания
закончились.
Что дальше? → 48



Юрий
ШАБАЛИН
AppSec.Sting
Программный
модуль
цифрового
рубля → 8



Алексей
ПЕТУХОВ
RuSCADAsec
ЦУПС
и сообщество
RuSCADAsec
→ 16



Сергей
ГРУЗДЕВ
Аладдин Р.Д.
Аутентификация,
ЭП и биометрия
→ 25



Форум 2026

Сонар киберустойчивости

14–15 АПРЕЛЯ 2026 ГОДА

НКЦКИ ПРОВЕДЁТ СПЕЦИАЛИЗИРОВАННЫЙ ФОРУМ
ПО ТЕМАТИКЕ ГОССОПКА



**Официальная
публичная
площадка**

- для обсуждения важнейших вопросов функционирования ГосСОПКА
- для взаимодействия участников процессов ГосСОПКА
- для консолидации опыта и конструктивного диалога между государственными органами, центрами ГосСОПКА и представителями ключевых сфер экономики РФ



forum.gossopka.ru

14–15 апреля 2026 года
Москва, Кластер «Ломоносов»

Организатор: НКЦКИ
Оператор: Медиа Группа «Авангард»



Сергей ПАЗИЗИН
научный редактор
BIS Journal

Данный номер у нас юбилейный, 60-й, журналу – 15 лет. Мы продолжаем освещать наиболее интересные события в области ИБ и предоставлять площадку не только для авторитетных авторов, но и для молодых специалистов, чтобы они могли высказать своё мнение по всем аспектам обеспечения информационной безопасности. Наша цель – информировать читателей об актуальных угрозах, а также об эффективных методах и средствах защиты информации.

В этом году начинается активная фаза внедрения цифрового рубля. С 1 сентября 2026 года использование нового способа расчётов должны обеспечить крупнейшие банки и крупные торговые предприятия из числа их клиентов. А в течение следующих двух лет цифровой рубль будет доступен клиентам всех банков в расчетах с продавцами, имеющими выручку более 5 млн руб. 12 марта 2026 года в Москве пройдет конференция «Массовое внедрение цифрового рубля». Поэтому основная тема данного номера посвящена обеспечению безопасности использования цифрового рубля.

В теме обеспечения безопасности КИИ мы ещё раз поговорим о методах аутентификации пользователей, промышленном интернете вещей и финансовой сфере. Выпуск данного номера приурочен в том числе к Уральскому форуму «Кибербезопасность в финансах», который пройдет в Екатеринбурге 18–20 февраля 2026 года.

В нашем постоянном разделе «Разработка безопасного ПО» мы публикуем итоги испытаний статических анализаторов исходного кода. Несмотря на необходимость разработки методологии и наборов используемых тестов (это признают сами организаторы испытаний), важность и полезность проделанной работы трудно переоценить. И результат не только в полученных оценках характеристик статических анализаторов. Опыт, приобретённый в процессе испытаний, может быть применён для развития понятийного аппарата, совершенствования стандартов и процедур сертификации процессов РБПО.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Батранков Д. В. – директор по развитию бизнеса группы компаний «Гарда»

Виноградов А. Ю. – старший научный сотрудник ФГУП ЦНИИХМ

Горелов Д. Л. – управляющий партнер, коммерческий директор компании «Актив»

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

Курило А. П. – советник по информационной безопасности ФБК и ФБК CS, кандидат технических наук, доцент

Мельников С. Ю. – профессор кафедры теории вероятностей и кибербезопасности факультета физико-математических и естественных наук РУДН им. Патриса Лумумбы, доктор физико-математических наук

Некрасов И. В. – главный редактор журнала

Пазизин С. В. – заместитель начальника Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО), кандидат физико-математических наук, научный редактор журнала

Самойленко Д. П. – начальник Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО)

Щедрин М. В. – начальник Управления тестирования безопасности Т1 Иннотех

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И. В.**

Выпускающий редактор: **Рачкова Е. В.**

Коммерческий директор: **Минаков А. В.**

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

Арт-директор: **Мельников Н. С.**

Обозреватели: **Оздемиров У. У., Покатаева Е. Н.**

Иллюстрация на обложке: **Виктор Миллер Гаусса**

Фото в номере: **FreePik**

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».

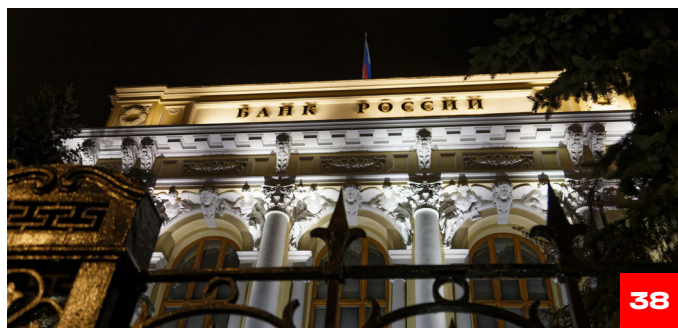
Зарегистрирован 11 июля 2023 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как «BIS Journal – Информационная безопасность бизнеса». Свидетельство ПИ № ФС 77-85487 от 11.07.2023 г.

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.

Подписан в печать 03.02.2026. Тираж 7000 экз. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

ТЕМА НОМЕРА — 1: БЕЗОПАСНОСТЬ ЦИФРОВОГО РУБЛЯ

- 4 Анатолий Аксаков (Госдума)
«Это не будет навязчивой кампанией»
- 8 Юрий Шабалин (AppSec.Sting)
**Программный модуль цифрового рубля
Банка России**
- 11 Руслан Фахретдинов (Фродекс)
**Подводные камни и прозрачная водная
гладь**
- 13 Антон Плетнев, Леонид Дорофеев
(Информзащита)
От временного к постоянному



38

ТЕМА НОМЕРА — 2: ЗАЩИТА КИИ

- 16 Алексей Петухов (RuSCADASec)
**Цифровая устойчивость
промышленных систем (ЦУПС)
и сообщество RuSCADASec**
- 20 Вячеслав Половинко (АМТ-ГРУП)
Мир IoT-решений просит защиты
- 22 Алексей Плешков (BISA)
**Пароль #Зима2026 не подходит,
или пять фактов о парольной политике
в копилку CISO**
- 25 Сергей Груздев (Аладдин Р.Д.)
**Аутентификация и ЭП с использованием
биометрии**
- 28 Илья Новойдарский (УЦСБ)
Эволюция доверия

ТЕМА НОМЕРА — 2: ЗАЩИТА КИИ. СЕТЕВАЯ БЕЗОПАСНОСТЬ

- 30 Екатерина Голунчикова (Нетопия),
Александр Товстолип
(Ассоциация ФинТех)
В соответствии с ГОСТ Р 57580.1-2017
- 34 Евгений Кутумин
(Positive Technologies)
Производительность NGFW
- 36 Денис Батранков (ГК Гарда)
**Первые 60 минут после того, как вас
взломали**

РЕГУЛЯТОРЫ

- 38 **Парад законов**
Екатерина Рачкова (BIS Journal)
Квартальный отчёт



8

УГРОЗЫ И РЕШЕНИЯ

- 42 **Security Profile Compliance**
Роман Душков (Security Vision),
Валерий Горбачёв (ДиалогНаука)
Security Vision SPC
- 45 **Облака**
Юрий Горячев (NGENIX)
**Облачная защита или требования
регуляторов?**

РАЗРАБОТКА БЕЗОПАСНОГО ПО

- 48 Испытания**
Дмитрий Пономарев
(НТЦ «Фобос-НТ»)
Итоги испытаний статических анализаторов исходного кода при организационной и методической поддержке ФСТЭК России
- 52 Статические анализаторы**
Андрей Белеванцев (ИСП РАН)
Что нового в Svnase
- 53 SAST-инструменты**
Антон Прусак (AppSec.Wave)
Ускорение и точность
- 54 Статические анализаторы**
Сас Арустамян (НПО «Эшелон»)
Трансформация отечественных инструментов безопасной разработки программного обеспечения
- 56 Интервью**
Евгений Тодышев (УЦСБ)
Безопасная архитектура
- 58 Защитницы**
Карина Нападовская
(Лаборатория Касперского),
Елена Быханова, Евгения Ремезова
(НТЦ «Фобос-НТ»),
Елена Маньжова (ИСП РАН), Натали
Дуботолкова (Базис), Анастасия
Калугина (ИнфоТекС), Альбина
Аскерова (Swordfish Security), Нелли
Магакелова
(АО «НПО «Эшелон»)
Девушки в РБПО

ЗА РУБЕЖОМ

- 88 Законодательство**
Александр Виноградов
(ФГУП «ЦНИИХМ»),
Сергей Меньшиков (Belarusian
InfoSecurity Community),
Андрей Ситнов (независимый
эксперт), Наталья Казанцева
(независимый эксперт)
**Содружество Непризнанных Государств
(СНГ-2)**

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 65 Цифровой рубль**
Андрей Жаркевич (Start X)
Цифровой рубль на марше

БЕСЕДЫ С ШЕРЕМЕТОМ

- 72 Искусственный интеллект**
Игорь Шеремет (РАН)
**«Стоит вообще отказаться
от использования термина
„искусственный интеллект“»**



72

СУБЪЕКТЫ

- 85 История**
Борис Столпаков
Прорыв к современной математике
- 90 Рассказ**
Андрей Жаркевич (Start X)
Цветы для Ани
- 92 Заметки безопасника**
Александр Игонин (BIS Journal)
Все юзвери равны, но некоторые равнее

«ЭТО НЕ БУДЕТ НАВЯЗЧИВОЙ КАМПАНИЕЙ»

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ ПРЕДСЕДАТЕЛЬ КОМИТЕТА ГОСДУМЫ ПО ФИНАНСОВОМУ РЫНКУ АНАТОЛИЙ АКСАКОВ



Анатолий АКСАКОВ
председатель
комитета
Госдумы
по финансовому
рынку

— Несмотря на то, что пилотный проект по расчетам в цифровых рублях шел довольно успешно, массовое внедрение в этом году было отложено на неопределенный срок. В процессе пилота были выявлены какие-то вопросы, требующие проработки, или вмешались внешние факторы?

— Широкое внедрение цифрового рубля начнется с 1 сентября 2026 года, когда к платформе подключатся крупнейшие банки и торговые предприятия из числа их клиентов с годовым оборотом от 120 млн руб. А в течение следующих двух лет цифровой рубль освоит средние и небольшие банки и ритейлеры.

Законодательная и нормативно-правовая база под цифровой рубль готова, операции с ним успешно протестированы крупнейшими банками. Но, очевидно, что средним и малым кредитным организациям тоже нужно время и ресурсы на доработку своей IT-инфраструктуры. Соответственно, сроки решили сдвинуть, чтобы у этих банков и у розничных магазинов было время на подготовку. Главная задача — чтобы внедрение новой формы российского рубля прошло гладко, спешить ради галочки смысла нет.

— Насколько критичен для коммерческих банков возможный отток безналичных в цифровой рубль?

— Очевидно, будет некоторое сокращение пассивов, то есть депозитной базы, но не в том объеме, который будет критичным для банковской системы. Вклады как самый простой и популярный способ накопления никуда не денутся — отсутствие процентов по счетам в цифровых рублях не дает использовать их для формирования сбережений. Речь прежде всего о расчетном инструменте — и население, и предприятия вряд ли будут держать основные средства на счете цифрового рубля, потому что отток с банковских счетов не будет значительным.

В перспективе появление новой формы рубля и новых возможностей для расчетов будет способствовать развитию конкуренции на банковском рынке. Кредитные организации будут заинтересованы в повышении качества обслуживания, разработке новых продуктов и улучшении условий по действующим предложениям, чтобы сохранять лояльность клиентов. От развития платежных услуг в результате выиграют как потребители, так и сами банки. Но для последних регулятору нужно будет создать условия для комфортного внедрения цифрового рубля, чтобы небольшие кредитные игроки не проиграли на старте из-за дорогого входного барьера.

— Каковы затраты среднего банка на внедрение в расчеты цифрового рубля?

— Расходы на технологическую интеграцию цифрового рубля, по разным оценкам, могут составлять 150–

300 млн руб. на банк, что включает в себя оборудование, программное обеспечение, настройку обмена данными с платформой цифрового рубля, расходы на кибербезопасность и подготовку кадров. Это критичная сумма для региональных и малых банков.

И здесь мы ожидаем от регулятора поддержки. С одной стороны, необходима совместная работа участников рынка с поставщиками программного обеспечения для разработки типовых решений, возможно, на базе уже существующих решений системно значимых банков — «коробочный» продукт поможет кредитным организациям сократить затраты на внедрение цифрового рубля. С другой стороны, Банк России может в какой-то степени учесть понесенные банками расходы при выработке новых регуляторных требований. С учетом увеличения масштабов операций с цифровым рублем, уже сейчас нужно думать об оптимизации расходов на поддержание работы системы — за счет отладки инфраструктуры и стандартизации процедур, в том числе с точки зрения отчетности и комплаенса.

— Какие преимущества расчетов цифровым рублем по отношению к классическим безналичным, СПБ и карточным расчетам для банков, населения, юридических лиц?

— Для людей операции с цифровым рублем будут полностью бесплатными. В перспективе каждый пользователь сможет получить доступ к своему цифровому кошельку через любое банковское приложение. Через него можно будет менять цифровые рубли на безналичные и



наоборот, а в кафе и магазинах будет доступна опция оплаты цифровыми рублями по единому QR-коду.

Для юридических лиц операции с цифровыми рублями будут дешевле текущих банковских комиссий. Торговые предприятия смогут экономить на эквайринге. Снижение транзакционных издержек бизнеса позитивно отразится на ценообразовании и в масштабе страны позволит ежегодно экономить сотни миллиардов рублей.

Банки обеспечивают взаимодействие клиентов с платформой ЦБ, предоставляя сервисы по открытию кошельков, пополнению, проведению расчётов и другим операциям с цифровыми рублями. Это позволит кредитным организациям создать на базе платформы цифрового рубля обширную экосистему, в рамках которой могут появиться инновационные финансовые продукты, например, с использованием смарт-контрактов — алгоритмов, которые автоматически выполняют переводы при соблюдении заданных условий.

Адля бюджета цифровой рубль обеспечит строго целевой характер госрасходов, препятствуя нецелевым тратам и коррупционным схемам. Для государства и каждого отдельного региона это означает огромную экономию средств, которые можно будет инвестировать в развитие предприятий и социальную поддержку.

— Насколько цифровой рубль поможет в упрощении международных расчетов при взаимодействии между сторонами сделки, находящимися в разных юрисдикциях?

— Национальные цифровые валюты позволят в будущем упростить международные расчеты, ведь транзакции будут проходить между центральными банками дружественных стран, минуя традиционную банковскую инфраструктуру. Это означает скорость, отсутствие комиссий, укрепление национальных валют и снижение зависимости от доллара и евро. Для реализации трансграничных расчетов цифровыми валютами

потребуется, во-первых, широко внедрить их на национальном уровне, а уже затем приступить к совместной настройке платежной инфраструктуры.

Существует несколько моделей использования цифровых валют в международных расчётах, включая создание общих платформ или мостов между платформами разных стран, интеграцию с платёжными системами, а также открытие корреспондентских счетов в системах других стран. Это многоступенчатый процесс, имеющий под собой экономическую, технологическую и, наконец, политическую составляющую. О расчетах в национальных цифровых валютах могут договориться между собой два государства или даже объединения, как, например, БРИКС.

— Как предполагается разрешить вопрос применения различных криптографических алгоритмов участниками расчетов, находящимися в разных странах?

— В будущем этот вопрос может быть решен через создание общих технических спецификаций, которые определяют допустимые алгоритмы шифрования и другие параметры. При трансграничных расчетах в цифровых валютах страны могут согласовывать конкретные адаптированные механизмы и гибридные протоколы. Объединение информационных систем дружественных стран через специальные «мосты» может позволить обходить различия в криптографии.

— Насколько оплата цифровым рублем будет прозрачна для третьих сторон? Не приведет ли его внедрение к введению вторичных санкций к некоторым участникам расчетов со стороны недружественных государств?

— Мы пока говорим только теоретически и можем предположить, что если транзакция проходит через закрытую платформу, оплата цифровым рублем будет прозрачна только для Банка России, участников сделки и регулятора страны-партнера. Такие операции не отслеживаются третьими странами, как в случае с международными платежными системами и корсчетами в крупных иностранных банках, что минимизирует риск вторичных санкций для участников. Поэтому финансовые операции в национальных цифровых валютах в рамках двусторонних или многосторонних соглашений вполне могут быть более безопасными с точки зрения внешнего недружественного вмешательства, чем традиционные банковские расчеты.

— Планируется ли совершенствование подходов к обеспечению криптографической защиты цифрового рубля?

— Аудит безопасности проводят специальные службы, проверки включают в себя различные стресс-тесты. Можно констатировать, что платформа цифрового рубля надежно защищена. Анализ инфраструктуры на предмет возможных уязвимостей будет продолжаться. Банк России

как оператор платформы будет совершенствовать меры защиты цифрового рубля по мере развития технологий. Централизованная модель упрощает системные обновления криптографии, что позволяет обеспечить устойчивость платформы к новым, в том числе потенциальным киберугрозам.

В технологической части я не вижу никаких серьезных рисков для цифрового рубля. Что действительно представляет опасность, так это социальная инженерия. Криптография не поможет, если под воздействием психологических манипуляций владелец счета цифрового рубля собственноручно переведет деньги с электронного счета на обычный банковский, а потом перечислит их киберпреступнику.

Поэтому в своей законодательной работе мы делаем упор на проработку общих механизмов противодействия социальной инженерии, таких как период охлаждения при выдаче кредитов, самозапрет на кредиты, сервис второй руки. Одновременно создается единая система информационного обмена между всеми участниками финансового и телекоммуникационного рынков ГИС «Антифрод», чтобы оперативно выявлять киберпреступников, блокировать их сим-карты и операции по счетам.

— Исторически в России есть некоторая предубежденность против трансформации твердой осязаемой валюты в новые более сложные сущности. Проводились ли исследования, по восприятию цифрового рубля населением? Как планируется повышать доверие к цифровому рублю и его привлекательность для целевой аудитории?

— Действительно, у части наших граждан скептическое отношение к цифровому рублю, как и к любой новой технологии. Так же было с банковскими карточками, когда люди отказывались ими пользоваться для платежей, предпочитая снимать наличные. Затем недоверие было в отношении появившихся мо-

бильных банков и онлайн-переводов. Скептицизм будет снижаться по мере того, как люди начнут осваивать новый инструмент — уже сейчас 15% россиян готовы полностью или частично получать зарплату в цифровых рублях, а среди молодежи таких уже больше 20%. С сентября в торговых точках появятся единые QR-коды для оплаты товаров и услуг, позволяющие расплатиться в том числе и цифровыми рублями, бизнес начнет подключаться к платформе для экономии на банковских комиссиях — постепенно цифровой рубль войдет в нашу жизнь, станет привычным и понятным инструментом. Параллельно государство продолжит вести разъяснительную работу, рассказывая о преимуществах цифрового рубля. Это не будет навязчивой кампанией. И, разумеется, никто не станет принуждать людей переходить на цифровой рубль.

— Много говорится о внедрении смарт-контрактов, позволяющих сделать автоматической оплату по выполнению условий сделки. Поможет ли цифровой рубль обеспечить качественный скачок в данном направлении? Какие здесь основные преимущества применения цифрового рубля относительно банковских аккредитивов и эскроу-счетов, стейблкоинов?

— Цифровой рубль может стать катализатором для более широкого распространения смарт-контрактов благодаря сочетанию скорости, безопасности, централизованному характеру платформы и возможностям контроля за расходами. По сравнению с традиционными инструментами, такими как аккредитивы и эскроу-счета, он предлагает более гибкие и автоматизированные решения, а по сравнению со стейблкоинами — государственное регулирование и доверие к эмитенту.

Внедрение цифрового рубля упростит и ускорит автоматизацию корпоративных сделок и госзаказа, повысит безопасность и прозрачность операций. Смарт-контракты на платформе цифрового рубля будут ис-



полняться мгновенно и не будут зависеть от бизнес-процессов банков. Возможность «окрасить» средства ограничит риски их нецелевого расходования контрагентом. А технология распределенного реестра сделает невозможным одностороннее изменение условий контракта. Единая платформа также позволит стандартизировать оформление сделок и при необходимости обеспечить к ним централизованный доступ для банков и других участников финансового рынка.

— **Может ли помочь цифровой рубль в решении такой актуальной проблемы, как борьба с мошенничеством? Например, помочь обеспечить обратимость сделок с недвижимостью, осуществленных под влиянием мошенников?**

— Цифровой рубль может повысить эффективность борьбы с мошенничеством благодаря полной прозрачности транзакций в рамках платформы Банка России и уникальным кодам

каждой единицы валюты, что упрощает блокировку и возврат средств, если есть подтверждение незаконности операции.

Для части сделок с недвижимостью смарт-контракты на базе цифрового рубля позволят автоматизировать условия исполнения договора, например, привязав платеж к регистрации недвижимости. Но не всегда структура сделки позволяет применить такой смарт-контракт.

Кроме того, мошенники научились использовать обратимость сделки в свою пользу, и мы сейчас работаем над тем, чтобы защитить и покупателя, и продавца недвижимости от подобных схем.

— **Есть ли планы или прогнозы, насколько активно цифровой рубль будет использоваться в экономике? Предполагается ли обязательное применение цифровых рублей в каких-то случаях?**

— Сейчас безналичные платежи приблизились к 90%, и среди них

доля таких инструментов, как оплата по биометрии и QR-коду, составляет около 15%. После внедрения с 1 сентября 2026 года единого платежного кода, позволяющего расплачиваться в торговых точках в том числе цифровым рублем, расчеты с его помощью начнут постепенно расти. Сначала процесс может идти медленно, но, когда в течение ближайших трех лет к платформе подключатся все банки и продавцы с годовой выручкой от 5 млн руб., доля цифрового рубля в розничных расчетах станет уже заметной и может достичь 5% и более. Причем в B2B переводах между юрлицами доля цифрового рубля может быть значительно выше. Что касается бюджета, то там цифровой рубль может занять весомую долю уже в ближайшее время — это сразу же снизит часть издержек, поэтому таким преимуществом, конечно же, нужно пользоваться.

Вопросы задавал
Сергей Пазизин,
научный редактор BIS Journal

ПРОГРАММНЫЙ МОДУЛЬ ЦИФРОВОГО РУБЛЯ БАНКА РОССИИ



Юрий ШАБАЛИН
директор
продукта AppSec.
Sting

Введение цифрового рубля — это огромный шаг вперед для российской финтех-индустрии. Из плоскости теоретических дискуссий проект перешел в стадию реальной имплементации: банки-участники пилотной группы уже интегрируют в свои мобильные приложения Программный модуль Банка России (ПМ БР).

Однако за фасадом пользовательских интерфейсов скрывается сложнейший технологический и регуляторный вызов. ПМ БР — это не рядовая библиотека, а компонент, содержащий средства криптографической защиты информации (СКЗИ). Встраивание такого модуля превращает обычное банковское приложение в среду функционирования СКЗИ, что автоматически активизирует жесткие требования регуляторов, в частности ФСБ России.

Перед индустрией встал вопрос: как совместить требования безопасности с реальностью мобильной разработки, в которой релизы выходят, как правило, каждые две недели? В этой статье мы детально разберем опыт пилотного тестирования, проанализируем недостатки классических инструментов анализа кода и представим методику, позволяющую соблюдать требования стандарта платформы цифрового рубля без ущерба

для скорости выпуска ПО на рынок (Time-to-Market).

1. КОНФЛИКТ ПАРАДИГМ: СКОРОСТЬ РЕЛИЗОВ ПРОТИВ РЕГЛАМЕНТОВ БЕЗОПАСНОСТИ

Современное банковское приложение — это живой организм. Команды работают спринтами, «выкатывая» обновления функционала, исправления багов и UI-улучшения в непрерывном режиме.

С точки зрения регуляtorики любое изменение программного обеспечения, взаимодействующего с криптографическим модулем, требует прохождения повторной оценки влияния. Согласно нормативной базе, любое обновление приложения («среды функционирования») потенциально может сказаться на работе СКЗИ.

Что говорит Стандарт? Опубликованный «Стандарт платформы цифрового рубля» от 20 ноября 2024 года четко определяет правила игры. В классическом сценарии, работающем «по умолчанию», каждое обновление приложения требовало бы прохождения процедуры «оценки влияния изменений» в аккредитованной испытательной лаборатории. Эта процедура включает экспертизу кода, анализ документации и составление заключения. В реалиях рынка это могло бы занимать недели или даже месяцы, что фактически парализовало бы развитие мобильного банка.

Нормативное «окно возможностей». Регулятор, понимая специфику мобильной экосистемы, заложил в Стандарт критически важный механизм оптимизации. Документ вводит понятие «неизменности трасс вызовов». В частности, в эксплуатацион-

ной документации на мобильное ПО должны быть определены условия, неизменность которых будет являться достаточной для подтверждения его безопасности, включая неизменность трасс вызовов¹ и порядка вызовов ПМ БР в составе приложения.

Это ключевой пункт. Если банк может доказательно подтвердить, что в новой версии приложения графы обращения к модулю цифрового рубля остались идентичными эталонной версии, полная повторная оценка не требуется. Таким образом, задача из юридической плоскости перешла в инженерную: как технически гарантировать и доказать эту неизменность?

2. ТЕХНИЧЕСКИЙ ТУПИК: ПОЧЕМУ SAST-ИНСТРУМЕНТЫ НЕ СПРАВИЛИСЬ

На старте пилота казалось логичным использовать существующие на рынке инструменты статического анализа кода (SAST, Static Application Security Testing). Задача выглядела тривиальной: просканировать репозиторий, построить граф вызовов (Call Graph) и сравнить его с предыдущим. Однако практика показала несостоятельность этого подхода для задач цифрового рубля. Мы столкнулись с тем, что анализ исходного кода не дает достоверной картины.

Проблема 1: Полиглоти́зм и разрывы контекста. Современное мобильное приложение представляет собой полноценную систему со

¹ **Трасса вызовов (трасса выполнения программ)** — это последовательность машинных инструкций в порядке их выполнения в программе. В трассе могут быть:

- вызовы функций;
- создание объектов;
- операции выделения памяти.



своими архитектурными подходами и правилами разработки, крайне сложную для анализа. В экосистеме Android код пишется на Kotlin и Java, которые компилируются в байт-код DEX, но критичные участки часто реализуются на C/C++ (Native Code) и подключаются через механизм JNI (Java Native Interface). Классические анализаторы, работающие с Java или Kotlin, часто «слепают» на границе JNI, не видя, что происходит внутри нативной библиотеки. В свою очередь, приложения iOS сочетают Swift и Objective-C, а также C-библиотеки. Динамическая диспетчеризация методов в Objective-C (message passing) часто ставит статические анализаторы в тупик, не позволяя построить связную картину вызовов.

Проблема 2: Фреймворки и «синтаксический сахар». Разработчики активно используют реактивные фреймворки (RxJava, Combine) и синтаксические конструкции, называемые «сахаром», которые делают код удобным для чтения человеком, но сложным для анализа машиной. Статические анализаторы исходного

кода часто не могут развернуть эти абстракции в реальную последовательность вызовов, что приводит к разрывам в графе.

Проблема 3: Ложные срабатывания. Попытка анализировать «сырой» исходный код приводила к огромному количеству ложноположительных срабатываний. Изменение форматирования, рефакторинг внутренней логики UI или обновление не связанных библиотек воспринимались сканерами как изменения кода, требующие перепроверки. Для регулятора такой вероятностный подход недопустим. Требовалась математическая точность.

3. РЕШЕНИЕ: СМЕНА ПАРАДИГМЫ — АНАЛИЗ БИНАРНОГО КОДА

Ключевая идея альтернативного подхода — отказ от анализа исходников в пользу анализа результата компиляции. Компилятор выступает здесь как «великий уравниватель»: он разворачивает все высокоуровневые абстракции, фреймворки и синтаксический сахар в унифицированные инструкции. Анализ бинарного файла дает

единственно верную картину того, как приложение будет исполняться на устройстве.

АЛГОРИТМ ПРОЗРАЧНОЙ ПРОВЕРКИ (STEP-BY-STEP)

Подход к анализу регламентирует строгий процесс, состоящий из четырех последовательных этапов.

Этап 1: Подготовка «Чистой сборки». Для корректного анализа необходимо сформировать специальную версию приложения. В ней должна быть отключена обфускация (запутывание кода), но при этом сохранены все криптографические подписи. Для платформы Android требуется предоставить приложение в формате Android Package (APK) или Android App Bundle (AAB) без применения R8/ProGuard. Для iOS критически важно наличие dSYM-файлов (Debug Symbols), так как без них имена методов в бинарном файле превращаются в бессмысленные адреса памяти и построить осмысленный граф становится затруднительно.

Этап 2: Построение ориентированного графа. Специализированное ПО загружает бинарный

файл и дизассемблирует его. Инструмент строит полный ориентированный граф вызовов приложения, где вершины представляют собой методы и функции, а ребра отражают факты вызова одного метода другим. Важно, что на этом этапе инструмент должен уметь проходить сквозь границы языков (Cross-language analysis), корректно обрабатывая JNI-вызовы и нативные методы.

Этап 3: Фильтрация и выделение трасс ПМ БР. Полный граф приложения может содержать сотни тысяч узлов, но для целей Стандарта нас интересует только взаимодействие с ПМ БР. Алгоритм фильтрации берет известные точки входа в модуль ПМ БР и рекурсивно обходит граф, находя все пути, которые ведут к этим точкам. Результатом становится выделенный подграф или трасса, описывающая все возможные маршруты обращения приложения к крипто-модулю.

Этап 4: Автоматическое сравнение с эталоном. На финальном этапе полученный подграф сравнивается с эталонной трассой, зафиксированной при первичном прохождении оценки влияния. Сравнение идет не по тексту кода, а по структуре графа. Алгоритм проверяет наличие новых узлов, удаление старых элементов и изменения порядка вызовов. Результат сравнения всегда бинарен: либо «Изменений нет», либо «Есть изменения». Это исключает человеческий фактор и субъективную трактовку результатов.

4. ЭКОСИСТЕМА ДОВЕРИЯ: РОЛИ УЧАСТНИКОВ И НЕОБХОДИМЫЕ РЕСУРСЫ

Реализация методики требует не только софта, но и выстраивания правильных процессов взаимодействия между банком, испытательной лабораторией и регулятором. Стандарт жестко регламентирует эти роли.

Участник, использующий ПМ БР (банк). В банке должна быть создана или наделена соответствующими полномочиями Служба безопасности и контроля. Стандарт требует наличия у персонала профильного

высшего образования в области ИБ и стажа работы не менее трех лет. Банку необходимо внедрить практики DevSecOps, при которых сборка «чистой» версии для анализа происходит автоматически в Continuous integration (CI)/Continuous deployment (CD)-контуpe, исключая ручное вмешательство разработчиков. Ответственность за процесс несет сотрудник службы безопасности, который проводит сравнение трасс. Если изменений нет, он составляет отчет, разрешает релиз и отправляет отчет вместе с новой контрольной суммой и сборочным манифестом в лабораторию.

Испытательная лаборатория. Лаборатория выступает гарантом объективности. Получив отчет и сборку от банка, она проводит процедуру построения и сравнения трасс, используя свои экземпляры инструментов. Кроме того, в архиве лаборатории хранятся эталонные версии и результаты всех проверок, обеспечивая непрерывный «аудиторский след». Раз в полгода в лабораторию направляет накопленные данные регулятор.

Регулятор (ФСБ России). Регулятор получает сводные данные и уведомления об инцидентах. В случае выявления нарушений, таких как расхождение контрольных сумм или несанкционированное изменение трасс, регулятор может потребовать блокировки использования ПМ БР до устранения нарушений.

5. «ПОДВОДНЫЕ КАМНИ»: ПРОБЛЕМА ИДЕНТИЧНОСТИ СБОРОК

Существует еще одна неочевидная проблема, связанная с дистрибуцией приложений. Стандарт требует гарантии, что проверенная в лаборатории программа идентична той, что скачивает пользователь. Однако сравнить их простым вычислением контрольной суммы (хэша) невозможно по техническим причинам.

В магазине Google Play при загрузке формата Android App Bundle (AAB) платформа сама разделяет приложение на части (split APKs) и переподписывает их своими ключами,

из-за чего хэш-сумма меняется полностью. Магазин App Store применяет к бинарным файлам технологию FairPlay-шифрования (DRM — digital rights management, управление цифровыми правами), которая изменяет структуру исполняемого файла и, соответственно, хэш-сумму.

Решение: «Отпечаток происхождения». Поскольку побайтовое сравнение невозможно, было предложено решение, основанное на комплексе организационно-технических мер. Вместо контроля всего бинарного файла внедряется проверка «отпечатка происхождения» — набора неизменяемых метаданных, вшиваемых в приложение на этапе сборки.

Процесс выстроен следующим образом: CI/CD-система в рамках одной сессии собирает из одного исходного кода два артефакта — «чистую» сборку для лаборатории (без обфускации) и продуктовую сборку для магазина приложений (с обфускацией). Затем в обе сборки автоматически внедряются уникальные идентификаторы номера коммита из системы управления исходным кодом и отпечаток релизного ключа, которым подписывается приложение. Организационные меры, такие как строгое ограничение доступа к ключам подписи и логирование всех действий CI/CD, гарантируют, что подмены кода между этими двумя действиями не произошло.

ЗАКЛЮЧЕНИЕ

Предложенная методология, закрепленная в стандарте платформы цифрового рубля, позволяет достичь баланса интересов всех вовлеченных сторон. Бизнес сохраняет скорость Time-to-Market, проходя проверки в упрощенном режиме. Регулятор, в свою очередь, получает гарантию неизменности условий эксплуатации СКЗИ, подтвержденную независимой лабораторией.

Цифровой рубль задал высокую планку требований к информационной безопасности, и рынок ответил на нее созданием технологий и методик, которые делают безопасность не тормозом, а встроенной и прозрачной функцией процесса разработки.

ПОДВОДНЫЕ КАМНИ И ПРОЗРАЧНАЯ ВОДНАЯ ГЛАДЬ

КОНТРОЛЬ ОПЕРАЦИЙ ЦИФРОВОГО РУБЛЯ



**Руслан
ФАХРЕТДИНОВ**
руководитель
департамента
развития
продуктов
Antifraud & AML
Фродекс

Цифровые валюты центральных банков – новый финансовый инструмент, позволяющий, в частности, реализовать концепцию, при которой мониторинг за движением денежных средств, в том числе бюджетных, упрощается для государства. Но не всё так просто – даже если контроль осуществляет единый орган, то, конечно же, не стоит рассматривать такую систему как изолированную от прочих финансовых инструментов и форм валюты.

Банк России одним из первых национальных банков в мире озаботился вопросом реализации новой формы национальной валюты и платформы, позволяющей с этой формой денежных средств работать. При этом цифровой рубль полностью оперируется Банком России: эмиссия, осуществление операций, контрольные функции и т.д.

Платформа цифрового рубля имеет следующие характерные черты:

1. обеспечение конвертируемости и быстрых переводов из одной формы денег в другую;
2. привычные каналы обслуживания и отсутствие прямого взаимодействия с клиентами, осуществляемыми операциями;

3. наличие инструментов, предоставляющих новые возможности для граждан.

Все эти составляющие положительно влияют на доступность и функционал технологической платформы, но в то же время усложняют контрольные функции оператора и влияют на риски использования платформы в противоправных целях.

Благо этот вопрос также «в объёме» оператора цифрового рубля. Законодательство устанавливает обязанности Банка России как в отношении процедур борьбы с мошенничеством, так и в рамках противомонополизационных норм.

Есть одно но – с кредитной организацией (финансового посредника) требований также никто не снимает. Их ничуть не меньше, чем у Центрального банка, а с учётом особенностей реализации платформы цифрового рубля для минимизации рисков, выстраивания процессов и реализации отчётности могут потребоваться существенные ресурсы – как человеческие, так и вложения капитала.

Прежде всего, счёт цифрового рубля – это не классический банковский счёт, и движения денежных средств по нему, за редким исключением, не проходят через баланс кредитной организации и недоступны для анализа в привычных для этого системах.

Это существенный момент, с которым не приходилось сталкиваться банкам в подобном масштабе, даже несмотря на относительно недавнюю экспансию Системы быстрых платежей (СБП) на платёжный рынок. Но в случае с цифровым рублём, в отличие от СБП, отражения операций в балансе не будет даже по факту

их исполнения, то есть нет возможности провести даже постконтроль.

В банковских проводках можно увидеть только операции по покупке и продаже цифровых рублей, но не операции по их переводам между счетами. Это означает, что весь инструментарий, имеющийся на стороне банка и реализованный на базе Автоматизированной банковской системы (АБС) для анализа операций, не может помочь контролировать операции с цифровым рублём работающими в банке системами без необходимости существенных доработок.

Второй момент – требования к наличию широкого перечня процедур онлайн-контроля, которые до сих пор внедрялись во многих организациях лишь частично. Теперь же они должны применяться в операциях с платформой цифрового рубля повсеместно – от обычных переводов до создания и редактирования смарт-контрактов. Кроме того, контроль предполагается как в части выявления операций без добровольного согласия клиента, так и в целях соблюдения требований законодательства по противодействию отмыванию (легализации) доходов, полученных преступным путём, и финансирования терроризма и экстремистской деятельности.

Контроль должен осуществляться и в офлайн-режиме, то есть после исполнения операции. Причём такой постконтроль проводится не только банком, через который была инициирована операция, но и всеми прочими финансовыми посредниками, обслуживающими второго участника операции.

Хорошей новостью является то, что платформа цифрового рубля



Рисунок 1. Схема с источниками данных

для обеспечения полноты и корректности проверок по требованиям Федерального закона № 115-ФЗ предоставляет финансовому посреднику расширенный состав данных, включающий ИНН, наименование и другую информацию. Это позволяет осуществлять проверки на должном уровне и устанавливать связи между проведенной ранее аналитикой, внешними доступными источниками информации и вновь поступающими на мониторинг операциями с цифровым рублём.

Как уже отмечалось, операции на платформе цифрового рубля зачастую не связаны с АБС и требуют отдельных инструментов для контроля. Но как раз общепринятые атрибуты, а также тот факт, что к платформе цифрового рубля могут подключаться исключительно клиенты банка, даёт возможность использовать связи по этим атрибутам (например, ИНН, номера телефонов и т.д.) для нахождения информации во внутренних и внешних источниках. Начиная от аналитики, проводимой Anti-Money Laundering (AML) и антифрод-системами по транзакциям/контрагентам/клиентам, и заканчивая дополнительными источниками, такими как платформа «Знай своего клиента» (ЗСК) Банка России, база ЕГРЮЛ и прочее. Это большое подспорье, особенно когда речь заходит о новых ка-

налах обслуживания, коим и является платформа цифрового рубля.

Банк России проводит собственный анализ операций, например, в рамках антифрод-контроля передаёт не только вердикт о возможности проведения операции, но и статус с точки зрения наличия признаков мошенничества.

Так, зная обо всех аспектах транзакционного поведения клиента и сессионных данных, а также оперируя общими открытыми и служебными источниками, финансовый посредник может использовать результаты анализа, проводимого Банком России на всём объёме операций платформы цифрового рубля для дополнительного снижения рисков мошенничества (рис. 1).

Дорожная карта развития цифрового рубля даёт основания полагать, что список типов доступных операций и её функционал будет расширяться. Следствием этого станет и распространение инструментов контроля на новые типы операций и самоисполняемых сделок.

При этом, поскольку разработка технологической платформы напрямую зависит от Центрального банка, то он, как субъект федеральных законов в сфере обеспечения экономической безопасности, заинтересован в своевременном появлении механизмов такого контроля. А это значит,

что, несмотря на частые изменения, всё же есть возможность успевать за ними, оперативно внедряя новые инструменты мониторинга.

Кроме того, если взглянуть на это с другой стороны, появление платформы цифрового рубля способно в том числе стать драйвером для развития механизмов оперативного обмена информацией и ещё большего смещения от реактивного к проактивному подходу в снижении вероятности совершения экономических преступлений.

В своё время появившиеся автоматизированная система обработки инцидентов (АСОИ) ФинЦЕРТ Банка России, платформа ЗСК Банка России, Система информирования о мошенничестве Национальной системы платёжных карт (НСПК) стали реальностью также ввиду роста объёма операций и появлению новых каналов обслуживания и необходимости бороться с рисками мошенничества и легализации и отмыванию доходов.

Отдельно хотелось бы отметить, что ограниченное количество вендоров и интеграторов, занятых в реализации проектов с цифровым рублём, а также сроки поставки серверного оборудования и сами обозначенные сроки запуска платформы цифрового рубля говорят о необходимости проработки подключения к платформе с запасом по времени.

ОТ ВРЕМЕННОГО К ПОСТОЯННОМУ

ОСОБЕННОСТИ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФРАСТРУКТУРЫ ЦИФРОВОГО РУБЛЯ В БАНКАХ



Антон ПЛЕТНЕВ
начальник отдела
системной архитектуры
компании «Информзащита»



Леонид ДОРОФЕЕВ
главный архитектор
отдела системной архитектуры
компании «Информзащита»

Запуск и поэтапное масштабирование платформы цифрового рубля (ПлЦР) сформировали для банковского сектора принципиально новый контур регуляторных и технологических требований в области криптографической защиты информации. Впервые за длительный период Банк России не ограничился рамочными предписаниями по обеспечению ИБ, а детально зафиксировал архитектурные, организационные и эксплуатационные аспекты применения средств криптографической защиты информации (СКЗИ), включая процессы управления ключами и автоматизацию выпуска пользовательских сертификатов.

Ключевыми нормативными актами, определяющими требования к криптографической защите ПлЦР, выступают Положение Банка России от 03.08.2023 № 820-П «О платформе цифрового рубля» и Положение Банка России от 07.12.2023 № 833-П «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля». Эти документы формируют обязательный минимум, дополняемый стандартами платформы цифрового рубля, регламентом взаимодействия финансового посред-

ника с Банком России при управлении криптографическими ключами, а также временными требованиями ЦБ от 25.12.2023, посвященными автоматизации выпуска сертификатов пользователей.

С точки зрения криптографии ПлЦР изначально проектируется как объект критической информационной инфраструктуры с повышенным профилем угроз, что автоматически влечет применение норм ФСБ России: Приказа № 66 (ПКЗ-2005), Приказа № 796 по средствам электронной подписи и удостоверяющим центрам, а также положений 63-ФЗ «Об электронной подписи». Дополнительный слой требований формируют методические документы Минцифры и регламенты подключения к ЕСИА. Таким образом, банк-участник ПлЦР оказывается в зоне пересечения сразу нескольких регуляторных вертикалей — ЦБ, ФСБ, ФСТЭК и Минцифры, каждая из которых транслирует собственную логику контроля и комплаенса.

Криптографическая модель ПлЦР выстроена по принципу жесткой сегментации каналов взаимодействия и разграничения классов СКЗИ в зависимости от уровня доверия и характера обрабатываемых данных. Для канала связи между пользователем и банком-финансовым посредником

применяется ГОСТ-ориентированный TLS. На стороне пользователя используется программный СКЗИ класса КС1: на этапе первичного обращения — в режиме одностороннего TLS для выпуска сертификата безопасности и подачи запроса на открытие кошелька, после получения сертификата — в режиме двустороннего TLS. На стороне банка требования существенно выше: используется ПАК TLS-шлюз класса не ниже КС2, что автоматически исключает большинство облачных и виртуализированных сценариев размещения.

Связь между банком и Банком России реализуется через защищенные VPN-каналы с применением СКЗИ класса не ниже КС2. При этом ЦБ централизованно ограничивает как перечень допустимых криптосредств, так и провайдеров связи, через которых допускается подключение к тестовой и промышленной среде ПлЦР. С практической точки зрения это означает потерю гибкости при проектировании телеком-архитектуры и необходимость раннего согласования даже, казалось бы, второстепенных технических решений.

Логическим продолжением данной модели становится усложнение инфраструктуры управления ключами и сертификатами. В инфраструктуре

банка-участника должны быть возвращены как минимум два удостоверяющих центра (УЦ). Подчиненный удостоверяющий центр включается в иерархию УЦ Банка России и предназначен для выпуска сертификатов ключей проверки электронной подписи пользователей платформы цифрового рубля. Транспортный удостоверяющий центр, также именуемый УЦ безопасности или УЦ TLS, на текущий момент является корневым и используется для выпуска сертификатов безопасности, применяемых при построении ГОСТ TLS-каналов между пользователями и участником ПлЦР. Такая конфигурация существенно повышает требования к процессам управления жизненным циклом ключей, регламентам администрирования и квалификации персонала, поскольку любые отклонения от утвержденных процедур подлежат оценке со стороны регулятора.

Наиболее чувствительным с точки зрения практической реализации элементом криптографической инфраструктуры ПлЦР стал сервис автоматизации выпуска сертификатов. Банк России впервые формализовал требования к подобным сервисам, закрепив их во временных требованиях от 25.12.2023. С точки зрения клиентского сервиса автоматизация выпуска сертификатов позволяет существенно сократить время подключения пользователя к платформе, однако для банков это означает появление нового высокорискового сегмента ИТ-ландшафта. Ключ подписи подчиненного УЦ должен храниться в неизвлекаемом виде в программно-аппаратном HSM, сегмент CABC подлежит защите с применением сертифицированных средств защиты информации, а при размещении компонентов сервиса в разных контролируемых зонах требуется использование СКЗИ класса не ниже КВ.

Дополнительную сложность создает обязательность подключения инфраструктуры участника ПлЦР к ЕСИА через типовые решения, перечень которых зафиксирован в методических рекомендациях Минцифры. Подключение должно осуществляться через VPN-шлюз класса не ниже КСЗ,

а сама подключаемая система должна соответствовать ряду требований по информационной безопасности. На практике в 2024–2025 годах значительная часть типовых решений ЕСИА находилась в стадии оценки влияния на СКЗИ и удостоверяющие центры, что существенно ограничивало выбор и затягивало сроки ввода ПлЦР в промышленную эксплуатацию.

ЭКСПЛУАТАЦИОННЫЕ ОГРАНИЧЕНИЯ, ОТКАЗОУСТОЙЧИВОСТЬ И ЭКОНОМИКА ВНЕДРЕНИЯ

Отдельного анализа требует вопрос обеспечения доступности и отказоустойчивости инфраструктуры цифрового рубля. Банк России предъявляет высокие требования к непрерывности оказания услуг, однако их реализация в условиях применения сертифицированных СКЗИ сопряжена с рядом системных ограничений. Отказоустойчивость в пределах одного центра обработки данных технически реализуема, но требует строгого следования эксплуатационным документам на СКЗИ и зачастую не допускает стандартных кластерных схем. Катастрофоустойчивые решения с географически разнесенными основным и резервным ЦОД дополнительно требуют защищенных междоудовых каналов с применением СКЗИ класса КВ и согласования архитектуры синхронизации данных с регулятором. Сценарии «холодного резерва» формально возможны, однако не обеспечивают выполнение требований по доступности и несут риск потери части данных при инциденте.

Практика 2024–2025 годов показала, что для ряда сертифицированных решений, включая удостоверяющие центры, CABC и типовые решения ЕСИА, эксплуатационная документация не содержит описаний отказоустойчивых кластерных конфигураций. Это вынуждает банки развертывать отдельные тестовые стенды для моделирования архитектур, проведения испытаний и выработки согласуемых с регулятором схем, что напрямую увеличивает сроки и стоимость проектов.

Экономический эффект от внедрения криптографической инфраструк-

туры ПлЦР для банков выражается не только в капитальных затратах, но и в росте операционной сложности. Необходимость применения СКЗИ классов КС2 и КС3 предполагает использование физических серверов, что на фоне ухода западных вендоров, ограниченной доступности отечественного оборудования и длительных сроков поставки приводит к существенному удлинению проектных циклов. Дополнительные затраты формируются на этапе подбора совместимых АМДЗ, операционных систем и средств защиты информации, перечни которых жестко зафиксированы в формулярах на конкретные СКЗИ. Ошибки на этапе выбора оборудования или версий ОС зачастую приводят к необходимости пересмотра архитектуры уже после начала проекта.

В операционном плане это означает смещение центра тяжести затрат и управленческого внимания из области клиентских сервисов в область инфраструктуры, комплаенса и взаимодействия с регуляторами. Усиливается зависимость банков от ограниченного круга отечественных производителей и интеграторов, способных работать в условиях жестких криптографических ограничений, одновременно обостряется кадровый дефицит специалистов, обладающих практическими компетенциями в области СКЗИ, требований ФСБ и банковских технологических процессов.

С высокой вероятностью временные требования Банка России будут институционализированы и переведены в статус постоянных нормативных актов, а контроль за эксплуатацией СКЗИ и процессами управления ключами станет более формализованным. В этих условиях стратегически оправданным для банков представляется переход к риск-ориентированному подходу при проектировании архитектуры ПлЦР, раннее вовлечение подразделений информационной безопасности в бизнес-планирование и формирование долгосрочных технологических партнерств с вендорами, способными обеспечить предсказуемость жизненного цикла криптографических решений.

Линейка ИБ-продуктов

R-Vision SIEM

R-Vision TIP

R-Vision VM

R-Vision TDP

R-Vision SOAR

R-Vision UEBA

R-Vision SGRC

R-Vision - разработчик систем цифровизации и кибербезопасности

С 2011 года помогаем финансовым организациям, крупнейшим банкам, государственному и промышленному сектору, энергетике и ритейлу противостоять киберугрозам и обеспечивать надёжность ИТ-инфраструктуры.

ЦИФРОВАЯ УСТОЙЧИВОСТЬ ПРОМЫШЛЕННЫХ СИСТЕМ (ЦУПС) И СООБЩЕСТВО RUSCADASEC



Алексей ПЕТУХОВ

лидер центра компетенций «Кибербезопасность»
Национальной технологической инициативы (НТИ)
«Энерджинет», RuSCADASec COIN №18

RuSCADASec — независимая некоммерческая инициатива по развитию открытого международного сообщества специалистов по промышленной кибербезопасности / кибербезопасности автоматизированных систем управления технологическими процессами (АСУТП).

Когда мы слышим слова «цифровизация», «цифровая устойчивость», «технологический суверенитет», кто-то воспринимает их как внедрение «ИТ-штучек» поверх существующих процессов с максимальным использованием российских решений, а кто-то — как необъятный край работ, включающий изменение мышления и процессов, использующий информационные и другие современные технологии. Я отношусь ко второму типу и в рамках статьи постараюсь описать масштаб того, что происходит и предстоит сделать в области цифровой устойчивости промышленных систем.

Задача большинства производственных компаний — устойчивое развитие, поэтому им нужно находиться на уровне конкурентов, а лучше опережать их. В мире, когда большая часть вещей и встреч проходит в интернете, всё определяет уровень

цифровизации. То есть то, насколько глубоко бизнес и производственные процессы компании интегрированы в цифровую среду, а также стабильность работы созданного ИТ-ландшафта.

На цифровую устойчивость промышленных систем влияют разные тренды.

С одной стороны те, которые относятся к цифровизации:

1. Активное расширение областей применения и глубины проникновения дистанционных датчиков (Internet of Things (IoT) устройств), а также продуктов на базе технологий машинного обучения.

Сюда входит изменение архитектур промышленных систем автоматизации: широкая и глубокая аналитика на локальных участках или даже устройствах с централизованной обработкой результатов как внутри производственного процесса, так и за его пределами, то есть от закрытых и автономных систем к системам, глубоко интегрированным с корпоративными процессами и другими системами предприятия.

2. Изменение модели управления: организация и управление производством на основе взаимодействия «цифрового помощника» (робот, система усовершенствованного управ-

ления, система прогнозирования, отраслевая база знаний и т.п.) и человека (пятая промышленная революция).

Человек уже не может самостоятельно анализировать все потоки данных, поэтому работает с предварительно обработанными данными, а его управляющие решения также преобразуются в наборы команд и действий, выполняемых «цифровым помощником».

3. Интеграция производственных систем между различными предприятиями. Речь идёт о создании продуктов одной компанией за счёт глубокой интеграции с информационными системами другой. Например, взаимодействие на базе систем автоматизированного проектирования (CAD) или подключение внешних компаний к системам управления жизненным циклом продукта и бизнес-процессами (PLM / BPM системам).

С другой стороны те, которые относятся к технологическому суверенитету Российской Федерации:

1. Импортозамещение;

2. Обеспечение информационной безопасности объектов критической информационной инфраструктуры (КИИ);

3. Разработка безопасного ПО и обеспечение безопасности цепочек поставок.

При этом важно учитывать и тренды киберугроз для промышленных систем:

1. Использование IoT для попадания в инфраструктуру, создания ботнетов и проведения DDoS-атак;

2. Сложные целевые атаки на КИИ;

3. Активное использование искусственного интеллекта (ИИ) в кибератаках;

Поэтому в части цифровой устойчивости промышленных систем можно выделить следующие открытые вопросы:

1. Как обеспечивать цифровую устойчивость промышленных систем в современных реалиях (инструменты, кейсы, методологии)?

2. Как наиболее эффективно реализовать защиту промышленных интернет-устройств, систем с машинным обучением, выполняя все требования законодательства?

3. Как оптимально создавать и развивать защищённые промышленные системы?

4. Как оценивать эффективность информационной безопасности на разных уровнях и для разных объектов?

5. Что должны знать и делать первые лица компаний, руководители и специалисты служб информационной безопасности, руководители и сотрудники других функций, чтобы компания была устойчивой?

Несмотря на кажущуюся похожесть современных промышленных систем и тридцати-/десятилетней давности, произошло много изменений в том,

Кстати, при подготовке конференции RuSCADASec CONF 2026 среди более чем 3 000 участников соответствующего сообщества проводился опрос про наиболее интересные темы докладов. И в пятёрку самых востребованных тем в области информационной безопасности промышленных систем попали:

- ◆ доверенная АСУТП (42%);
- ◆ управление и эксплуатация ИБ АСУТП (41%);
- ◆ решения и продукты для защиты промышленных систем (36%);
- ◆ перспективные технологии для автоматизации и их безопасность (32%);
- ◆ инциденты, уязвимости, итоги пентестов и другая аналитика (30%).

как их создают и как с ними работают, а следовательно, должны меняться подходы к эксплуатации и защите таких систем (обеспечению устойчивой работы).

ПРИМЕР 1. ОТКРЫТАЯ АСУТП (РИС. 1)

В конце 2025 года были продемонстрированы первые стенды на базе идеологии и формализующихся стандартов по построению и защите открытой АСУТП.

В отличие от привычных и устоявшихся правил, основанных на том, что

АСУТП является закрытой, моновендорной и недоступной, предложены подходы, которые позволяют создавать её как конструктор на базе заменяемых компонентов разных производителей. При этом вычисления могут происходить на виртуальных машинах, в которых контроллер или сервер диспетчерского управления и сбора данных (SCADA сервер) – виртуальный образ.

Получается, что компоненты ОАСУТП всё те же: исполнительные устройства, контроллеры, датчики и система управления, а подход к защите должен быть кардинально изменён:

1. Нельзя полагаться только на защиту периметра («воздушный зазор») между АСУТП и другими системами предприятия. Периметра у открытой АСУТП (ОАСУТП) может не быть. То есть нельзя изолировать ОАСУТП от внешних угроз техническими и организационными мерами. Необходимо строить систему, интегрированную с внешним миром.

2. Подход к безопасной разработке (Security by design) при создании ОАСУТП и её компонентов – основа устойчивой работы данных систем при эксплуатации. Если не учитывать меры информационной безопасности в архитектуре, компонентах и процессах, то надёжность системы будет низкой.

3. Интеграция офисных и технологических сетей как типовое решение. Требуется прорабатывать меры информационной безопасности, подразумевающие возможность многоуровневого доступа и подклю-

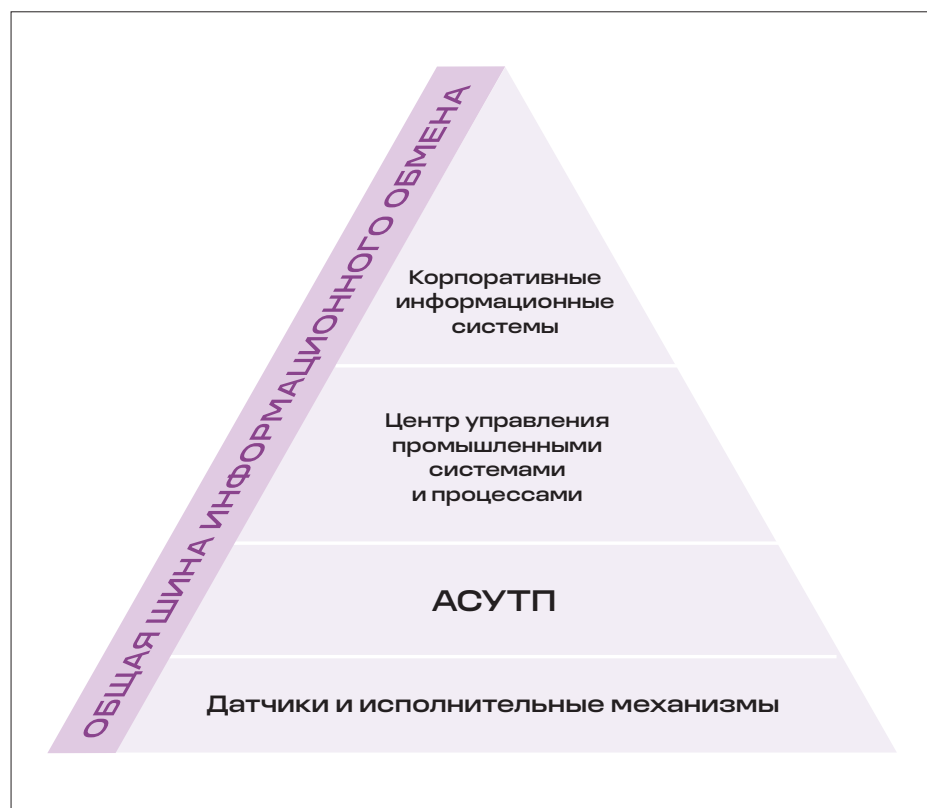


Рисунок 1. Обобщённая концепция архитектуры открытой АСУТП)

чения к технологическому сегменту через интернет как стандартные сценарии.

ПРИМЕР 2. ЦИФРОВОЙ ПОМОЩНИК

Ранее в промышленных системах использовались информационные системы, в которых информация была верифицирована (но ограничена и/или очень объёмна), либо сразу подразумевалось, что она требовала дополнительной аналитики и корреляции между разными источниками.

Появление систем, имитирующих общение с человеком и предоставляющих самостоятельно сгенерированную информацию из базы знаний, изменяет сам подход к восприятию информации и принятию решений.

Со временем сотрудники перестают проверять или с недоверием относиться к предоставляемой информации, выполняют всё, что посоветует «цифровой помощник». При этом сами технологии имеют свойства сбоят и ошибаться.

Достоверность и качество выдаваемой информации требуется контролировать. Причём речь идёт не только о подмене информации злоумышленником, но и в первую очередь о достоверности выдаваемой информации самим ПО.

Требуется вести безопасную разработку ИИ-систем, создавать отраслевые модели знаний, а также расширять меры информационной безопасности по защите ПО и соответствующих баз знаний. В противном случае у злоумышленников возникают возможности по корректровке логики работы ИИ.

ПРИМЕР 3. СИСТЕМЫ ПРЕДИКТИВНОЙ АНАЛИТИКИ

Вместе с ростом, усложнением систем и их компонентов возникает необходимость мониторинга состояния самой инфраструктуры: прогнозирование не только износа производственного оборудования (насосы, двигатели и т.д.), но и сетевого, вычислительного. А также требуется оценка корректности всей работы в целом.

Так как разобраться в работе инфраструктуры становится сложным, то для оценки её работы также необходимы системы, которые будут анализировать состояние множества параметров и определять отклонения всего процесса от нормы и плановых показателей, а также определять источники таких отклонений.

Важным вопросом здесь становится то, кто этим должен заниматься в новых условиях. Ведь исторически не было возможности удалённо влиять на показатели технологического процесса. А теперь такое влияние может быть следствием и естественного износа оборудования, и целенаправленной атаки.

Необходимо формировать новые процессы взаимодействия производства, информационных технологий и информационной безопасности для обеспечения стабильности работы всего производства. И естественно, обеспечивать их соответствующими решениями.

Сам процесс управления рисками (устойчивостью работы) предприятия в целом также не изменился, и можно выделить 12 основных его составляющих (см. таблицу 1), но буквально каждый пункт теперь должен

учитывать возможности внешнего удалённого воздействия, а следовательно, должны рассматриваться меры информационной безопасности внутри него.

Поднятые выше темы лишь малая крупинка изменений, которые сейчас происходят. А поиск наилучших решений и наработка практик – процесс длительный. Для выработки наиболее эффективных решений необходимо обмениваться опытом, и с учётом современных ритмов жизни лучше это делать интерактивно. Сообщество RuSCADASec создано для того, чтобы обмениваться опытом в области цифровой устойчивости промышленных систем, а в этом году совместно с BIS Journal при поддержке Медиа Группы «Авангард» открывает базу знаний по цифровой устойчивости промышленных систем в виде тематического блока в журнале и портала на сайте.

Приглашаем вас делиться опытом, практикой и аналитикой. Будем рады вашим предложениям.



t.me/ruscadasec
www.ruscadasec.ru



t.me/BISInside
www.ib-bank.ru

№	Название	Краткое описание
1	Управление программой устойчивого развития	Создание объединения (комиссия / рабочая группа / совет директоров и т.п.), курирующего устойчивое развитие. Создание единой программы по обеспечению устойчивого развития. Развитие корпоративной культуры в части цифровой прозрачности, контролируемости и устойчивости. Разработка и актуализация стратегии устойчивого развития
2	Оценка и снижение рисков	Определение рисков и компенсирующих мероприятий. Системная актуализация рисков и плана мероприятий. Актуализация стратегии развития
3	Оценка воздействия простоев на компанию	Формирование единой методики расчёта простоев. Определение максимально допустимого уровня простоя. Проведение аудитов по производственным цепочкам и цепочкам поставок, включая проектируемые и строящиеся объекты. Определение критичного оборудования и систем для новых объектов
4	Стратегии непрерывности и восстановления	Формирование и актуализация стратегий устойчивости для критичных бизнес-процессов, бизнес-подразделений, ИТ и ОТ (Operational technology) систем, а также компании в целом с учётом возможных внешних воздействий. Координация работ по обеспечению непрерывности и восстановлению бизнеса/производства на всех уровнях
5	Планы устойчивости бизнеса	Формирование и актуализация планов по обеспечению устойчивости бизнеса. Организация процессов работы команд реагирования на инциденты. Включение процесса разработки планов по обеспечению устойчивости бизнеса в обязательный блок работ для планируемых объектов и систем
6	Планы аварийного восстановления	Разработка и актуализация планов восстановления критичного оборудования и систем. Разработка системы нормативных документов в области аварийного восстановления
7	Кризисное управление и реагирование	Организация процедуры каскадирования работ кризисных штабов. Разработка нормативных документов в области антикризисного управления
8	Обеспечение ресурсами	Формирование механизма по обеспечению ресурсами сотрудников, процессов и объектов. Выделение ресурсов
9	Обучение и повышение осведомлённости	Обучение операционного и управляющего персонала действиям по устранению инцидентов. Обучение операционного персонала восстановлению работоспособности процессов и систем. Обучение всех сотрудников кризисному реагированию. Проведение мероприятий по взаимодействию сотрудников (ключевых ролей) в случае инцидентов
10	Тренировка и тестирование	Организация тренировок по восстановлению. Организация тренировок по кризисному управлению
11	Постоянное совершенствование	Оценка обстоятельств, которые привели к инциденту. Оценка эффективности действий при реагировании. Определение требуемых улучшений. Обновление планов, нормативных документов и образовательных программ.
12	Цифровизация	Цифровизация процесса обеспечения устойчивости: • формирование источников данных по объектам, процессам и системам; • проектирование системы сбора информации и реагирования на инциденты; • внедрение необходимого оборудования и ПО

Таблица 1. Обеспечение (цифровой) устойчивости промышленных систем

МИР IIoT-РЕШЕНИЙ ПРОСИТ ЗАЩИТЫ



Вячеслав ПОЛОВИНКО
руководитель
направления
собственных
продуктов
AMT-ГРУП

Промышленный интернет вещей (IIoT), будучи новой и легкодоступной технологией, сегодня обещает революцию в производстве, энергетике и других ключевых отраслях. Практически все эксперты сходятся на том, что рынок IIoT-устройств и решений будет только увеличиваться. Особый вклад в его рост внесут интеграция с искусственным интеллектом, системами аналитики, применение высокоскоростных систем и сетей связи для оперативного сбора данных. Однако этот значительный потенциал может быть сведён на нет в случае, если не будет обеспечена хотя бы базовая информационная безопасность применяемых решений и технологий. Постараемся разобраться, почему это так и в чём состоят проблемы построения безопасных решений IIoT сейчас, а также какие доступные на рынке решения могут нивелировать возникающие риски.

ПРЕИМУЩЕСТВА

IIoT-решения и устройства обладают очевидными преимуществами для потребителей, которым необходим оперативный сбор данных, аналитики и «быстрая» автоматизация. Прежде всего это:

1. Стоимость и доступность решений. Огромное количество производителей предлагают хотя и не всегда надёжные, но низкобюджетные решения, которые позволяют добиться эффекта «низкой базы» — когда даже самые простые устройства при минимуме инвестиций могут дать значительное количество данных, аналитики для дальнейших решений и изменений, экономии или получения дополнительных средств.

2. Актуальные и простые протоколы интеграции типа ZigBee и LoRaWAN, MQTT, CoAP, AMQP, которые опираются на современные сети и системы связи и позволяют легко и без ёмких инвестиций настроить сбор и передачу важных данных уже на существующих (иногда низкопроизводительных) ethernet и беспроводных сетях.

3. Достаточно высокая производительность в части обмена данными на высокопроизводительных сетях. За счёт современных протоколов обмена становится возможным собрать и передать большое количество структурированных данных в самых разных форматах, что ранее было недоступно или достаточно трудоёмко.

В КОНТЕКСТЕ ИБ

Однако современные устройства IIoT часто становятся слабым звеном в системе из-за архитектурных особенностей и условий эксплуатации в контексте информационной безопасности:

♦ Значительное количество небольших вендоров предлагают дешёвые и простые устройства, при этом вся инфраструктура сбора и передачи данных построена, что называется, «на коленке». Промежуточные данные о регистрируемом в сети устройстве могут уходить на непроверенные и недоверенные серверы и прокси-серверы далеко за пределы организации, а устройство может устанавливать связь с внешним миром произвольным образом.

♦ Многие устройства создаются с упором на функциональность, а безопасность отходит на второй план. Часто такие устройства не поддерживают установку наложенных средств защиты, не имеют даже базовых механизмов аутентификации, способны выполнять неконтролируемо загружаемые скрипты и компоненты стороннего ПО, невозможен контроль за их состоянием.

♦ IIoT-устройства часто спроектированы или как «одноразовые» решения (запустил, забыл, сломалось, заменил) или, наоборот, рассчитаны для работы десятилетиями (запустил и забыл), и акцент в их «конструкции» делается на простоте и надёжности в ущерб иным аспектам функционирования. В частности, обновление встроенного ПО в таких типах устройств либо вообще не предполагается, либо, наоборот, предполагается в онлайн-режиме с промежуточных серверов малоизвестных вендоров без каких-либо ограничений и контроля в части ИБ. Это приводит к тому, что в обоих случаях эти устройства, будучи легко компрометируемыми, могут столь же легко выступать в качестве

IIoT-устройства часто спроектированы или как «одноразовые» решения или, наоборот, рассчитаны для работы десятилетиями, и акцент в их «конструкции» делается на простоте и надёжности в ущерб иным аспектам

источника угрозы для сети, в которой они располагаются.

♦ В ряде случаев устройства выпускаются с поддержкой современных каналов и систем связи, стандартов, но изначальная цель их создания — работать на устаревших и уязвимых протоколах в переходный период трансформации предприятия, например, поддерживать работу протокола Modbus поверх TCP. В таких случаях устройства изначально поставляются с игнорированием требований безопасности, таких как шифрование, аутентификация и др.

♦ Для сегмента IIoT характерно повсеместное использование устройств со стандартными или слабыми учётными данными, настройками и паролями по умолчанию, дефолтными IP-адресами, DNS-серверами, что предоставляет злоумышленникам простой путь для доступа к ним.

БЕЗОПАСНЫЙ СБОР ДАННЫХ

Каким же образом можно обеспечить безопасный сбор данных с использованием данного типа устройств, когда практически каждое из них является уязвимым и требует передачи данных в менее доверенные сети?

Решение в значительной степени зависит от критичности того сегмента, в котором собираются данные. Если речь идёт о достаточно автономных датчиках, основная цель которых — только собрать данные, сеть их сбора достаточно автономна, не сопрягается с иными сетями, а потеря самих данных (или прерывание процесса сбора) не является критичным аспектом — можно ограничиваться типовыми и хорошо зарекомендовавшими себя мерами защиты с использованием межсетевых экранов, базовых логических средств сегментации сетей. С ростом значимости сети — источника данных с IIoT-устройствами, особенно с ростом конфиденциальности данных, в этой схеме появляются системы и узлы шифрования, которые позволяют эффективно исключить раскрытие данных злоумышленниками посередине. В особенности это актуально, если передача данных ведётся по недоверенным каналам.

Если же речь идёт о критических объектах автоматизированных систем управления технологическими процессами (АСУТП), наиболее эффективным средством обеспечения безопасности становятся диоды данных¹, обеспечивающие физическую изоляцию среды сбора данных от получателей, которые находятся в менее доверенных сегментах (облака, корпоративные сети, центры аналитики, системы управления производственными процессами в реальном времени (MES-системы), ситуационные центры, AI-системы, системы больших данных). Одной из базовых задач диодов данных является передача промышленных протоколов, хотя пока не так много производителей готовы обеспечивать даже передачу основных промышленных протоколов: OPC UA/DA, Modbus, не говоря уже о том, чтобы передать достаточно экзотические и новые MQTT, AMQP или обеспечить сквозное взаимодействие с интеграционными шинами типа RabbitMQ, Kafka. Между тем именно такие решения становятся всё более востребованными по мере роста количества внедрений IIoT-устройств в контексте проблем безопасности, обозначенных выше.

ДИОДЫ ДАННЫХ

Диоды данных, которые умеют передавать, например, MQTT-трафик, решают одну из главных проблем IIoT в критических сегментах: как передавать данные из защищённой операционной (Operational technology, OT) сети для анализа в ИТ-системе, не подвергая производственное оборудование риску кибератак извне, в условиях, когда само оборудование и IIoT-элементы являются легко компрометируемыми устройствами.

Основное преимущество диодов данных — физическая невозможность обратной связи. Поэтому такие решения являются идеальным для объектов энергетики, водоснаб-

жения, транспорта и промышленности.

Отдельным преимуществом диодов данных для критических сегментов и сетей является высокая прозрачность и контроль за передачей данных. Это означает, что если какое-то IIoT-устройство попытается установить соединение с внешним миром в попытке запросить обновление или просто передать данные на сервер малоизвестного вендора, то такие попытки будут легко обнаружены и однозначно заблокированы. Это возможно благодаря тому, что никакого прямого физического соединения с внешним миром для конкретного IIoT-устройства не существует. Таким образом, и руководство, и службы мониторинга получают полную прозрачность происходящего на производстве в реальном времени, но без риска, что случайная ошибка или злонамеренное действие из офисной сети повлияют на работу оборудования, а само оборудование, будучи достаточно производительным и массово применённым, не попытается самостоятельно связываться с внешними серверами и системами.

Современный мир IIoT-решений требует адекватных мер защиты. Скорость и объёмы передачи, разнообразие IIoT-устройств, простота и доступность протоколов должны быть эффективно компенсированы адекватными решениями в области информационной безопасности. В ряде случаев диоды данных становятся обязательным стандартом безопасности для IIoT, потому что они предлагают единственное на сегодня решение, которое на физическом уровне полностью блокирует возможность внешнего кибервоздействия через IIoT-устройства на критически важные технологические процессы, в которых эти устройства участвуют, позволяя при этом в полном объёме использовать собираемые ими данные для аналитики и оптимизации.

¹ Data diode (диод данных), или одноподключенный шлюз, — устройство, передающее данные только в одном направлении (обратная передача данных исключена на физическом уровне)

ПАРОЛЬ #ЗИМА2026 НЕ ПОДХОДИТ

ИЛИ ПЯТЬ ФАКТОВ О ПАРОЛЬНОЙ ПОЛИТИКЕ В КОПИЛКУ CISO



Алексей ПЛЕШКОВ
независимый
эксперт по ИБ,
эксперт BISA

Как давно я менял свои пароли? Какая длина у моего действующего пароля в символах? А мой мнемонический пароль достаточно сложный или его легко подобрать по словарю?..

Эти и другие вопросы про информационную безопасность (ИБ) регулярно возникают в голове не только у профессионального безопасника (CISO), но и у обычного пользователя ИТ-системы, когда он читает сообщение о массовой утечке паролей в СМИ или в интернете. Но вскоре эти вопросы как-то забываются, оставшись без фактического ответа, тема или контекст быстро меняются, и «правильно-тревожным» вопросам на смену приходит расслабляющая комфортная мысль: «Меня-то эта информация об утечке, в общем-то, и не касается», «мой-то три пароля в безопасности», «спокойно, всё нормально, идём дальше, пароли — это не самое важное сейчас». Знакомо?

ДО АРГУМЕНТОВ И ФАКТОВ

Спешу разочаровать и ответить сразу на все вопросы, прежде чем аргументировать и познакомить с фактами.

1. [если вы используете «популярные» пароли — прим. ред.] Ваши пароли не

уникальные, они уже кем-то когда-то скомпрометированы: пароли/хеши уже есть в базе злоумышленников — дело остаётся за малым, эти пароли кому-то как-то в «правильное время» и в «правильное место» достаточно просто ввести.

К сожалению, вся безопасность на основе паролей сохраняется только потому, что злоумышленники с вашими паролями не успели пока их ввести в целевом интерфейсе для доступа к защищаемой системе от вашего имени.

2. Ваши пароли, сами по себе, создают только иллюзию того, что чувствительная информация находится в безопасности, поскольку уровень реальной угрозы не зависит от длины, сложности или уникальности пароля [если понадобится, любой пароль подберут за какое-то время, но чем это время больше, тем лучше, поэтому рекомендуем использовать сложные пароли в соответствии с рекомендациями ФСТЭК — прим. ред.]

Строить защиту по классическим канонам и рассчитывать только на стойкие пароли в 2026 году ошибочно и НЕбезопасно. Пароль без дополнительных компенсирующих мер и факторов уже не обеспечивает полноценную защиту.

3. Если вы регулярно изменяете свой пароль по созданному мнемоническому принципу (схеме), то злоумышленникам не нужно знать каждый ваш пароль, а достаточно просто узнать и применить используемую схему, получив доступ к нескольким ранее созданным по этой схеме и украденным «кем-то где-то» паролям.

Не рассчитывайте на глупость или ограниченность злоумышленников: вы удивитесь, каких высот уже до-

стигли навыки и смекалка хакеров при наличии технической базы и неограниченного времени.

ЛЮБОПЫТНЫЕ ФАКТЫ

Приведу лишь несколько показавшихся мне любопытными актуальных фактов про пароли.

Факт № 1. Современные пользователи — граждане РФ — НЕ меняют свои удобные пароли годами. Средний «срок жизни» одного пароля у пользователя составляет 3,5–4 года.

Факт № 2. Каждый второй украденный в 2025 году пароль НЕ уникальный. Более половины (54%) паролей/хешей, обнаруженных в утечках 2024–2025 годов, выявлены «не первый раз», то есть были обнаружены исследователями повторно в darknet'e.

Факт № 3. В топ-10 самых популярных паролей, скомпрометированных у RU-пользователей в 2025 году, вошли: **123456, 12345678, 123456789, admin, 1234, Aa123456, 12345, password, 123, 1234567890**. При этом четверть самых популярных утёкших паролей состоит только из цифр, а порядка 40% представляют собой простые последовательности (клавиатурные змейки или рядом стоящие символы).

Факт № 4. По состоянию на январь 2026 года в базе данных международного проекта haveibeenpwned накоплено более 17,3 миллиарда паролей/хешей от скомпрометированных пользователей учётных записей (далее — УЗ).

База данных агрегатора утечек haveibeenpwned ежедневно пополняется новыми паролями. Только за первые две недели января 2026 года на сайте появилась информация о

таких громких утечках, как французская социальная программа Pass'Sport – 6,4 миллиона УЗ с паролями, одна из запрещённых на территории РФ социальных сетей – 6,2 миллиона хешей паролей попали в darknet, сайт знакомств для граждан Евросоюза WhiteDate – 6,1 тысячи УЗ утекли.

Факт № 5. Стойкость выбранного пароля перестала характеризовать уровень безопасности подсистемы аутентификации в целевой системе. Результаты проведённого ИБ-исследователями в 2024 году эксперимента по прямому взлому хешей от 200 миллионов паролей неутешительны: 45% (то есть 87 миллионов хешей паролей) могут быть взломаны современными процессорами с помощью «умных алгоритмов» на быстрой видеокарте менее чем за минуту, и только четверть можно считать стойкими – их взлом займёт более года.

ЗАДУМАЙТЕСЬ!

Задумайтесь: классические парольные политики в российских организациях, субъектах КИИ, уже два года как стоило бы пересмотреть и скорректировать в части установления обязательных пороговых/минимально допустимых значений, например, вот так:

- ◆ минимальная длина нового выбранного пароля – 12 символов;
- ◆ обязательный алфавит: большие и маленькие буквы, цифры, специальные символы;
- ◆ максимальный срок действия пароля: от 50 до 100 дней;
- ◆ минимальное время, прошедшее между двумя фактами смены пароля: 7 дней;
- ◆ количество отличающихся символов в новом пароле: 4;
- ◆ количество различных паролей в цепочке фактов обновления паролей: 10;
- ◆ количество неудачных попыток ввода пароля перед блокировкой УЗ на 2 минуты: 5.

В стойком пароле не должны использоваться даты, имена, фамилии, названия месяцев, времён года, а также популярные клавиатурные

Подтверждение факта невыполнения субъектом КИИ требований собственной парольной политики влечёт снижение итогового значения показателя защищённости сразу на 12,5%

змейки и легко подбираемые последовательности.

У читателя мог остаться неотвеченным вопрос, почему так важно именно в 2026 году обновить и соблюдать парольную политику и чем зима 2026 года отличается от такой же зимы, но годом ранее, в плане ИБ для субъекта КИИ? И здесь я обращаю внимание CISO на официальную позицию ФСТЭК РФ о важности соблюдения каждым пользователем парольной политики в организации, нашедшую своё отражение в Методике анализа защищённости информационных систем (далее – Методика), утверждена ФСТЭК РФ 25 ноября 2025 года.

Методика определяет порядок проведения и содержание работ в ходе испытаний систем защиты информации выбранного объекта. Целью подобных работ является выявление уязвимостей и оценка возможности их использования нарушителем при реализации угроз кибербезопасности. В 10+ пунктах Методики в совершенно разных по сути разделах: СИН.3, УСИ.3, ОПС.1.1–1.5, СУБД. 1.1–1.3, 1.14, СВИ. 1.1 в явном виде присутствуют указания по проверке у субъекта КИИ факта наличия, актуальности, настройки и выполнения базовых требований парольной политики.

Две ключевые метрики, а именно: «отсутствие у субъекта КИИ в АС учётных записей с паролем, сложность которого не соответствует установленным требованиям к парольной политике» и «отсутствие у субъекта КИИ в АС учётных записей разработчиков и/или технических/сервисных учётных записей с паролями, установленными ими по умолчанию» используются при расчёте итогового показателя защищён-

ности. Таким образом, подтверждение факта невыполнения субъектом КИИ требований собственной парольной политики (достаточно одной УЗ или одного подтверждённого факта нарушения в одной АС в периметре проверки) влечёт снижение итогового значения показателя защищённости сразу на 12,5%. Много это или мало – субъективный момент на фоне других возможно допущенных нарушений. Да, и относиться к этому «комплаенс-показателю» со стороны CISO можно по-разному. Но факт того, что ФСТЭК в конце 2025 года формализовал в документе (Методике) подход к проведению проверок и определил алгоритм расчёта метрических показателей (кстати, такого расчёта ещё не было зимой 2025 года), говорит о намерении и готовности регулятора к проведению как выездных, так и камеральных проверок у субъектов КИИ в ближайшем будущем.

В своём выступлении 18.11.2025 на SOC Forum начальник Управления ФСТЭК РФ Е. Б. Торбенко отметила увеличение административных дел в 2025 году по результатам проведённых государственных контрольных мероприятий в отношении субъектов, допустивших типовые нарушения при организации защиты объектов КИИ. Более 1100 нарушений выявлено суммарно за неполные 10 месяцев 2025 года. Наряду с нарушениями в процессе категорирования объектов КИИ, к типовым нарушениям представитель ФСТЭК относит в том числе вопросы, связанные с нарушениями субъектами КИИ собственных парольных политик (слабые/нестойкие/статичные и пароли по умолчанию), повлёкшие реализацию компьютерных инцидентов.

«...Специалисты по безопасности — это физические тела. Да, ну, это тело! А по закону физики любое тело стремится к покою...» — обратилась Е. Б. Торбенко к CISO, говоря о зоне комфорта. «Ваша задача — заставить, запинать своих специалистов выполнять ваши требования!» — так эмоционально она обозначила основные задачи CISO по выполнению обновлённых требований ФСТЭК внутри субъекта КИИ.

Внимательный CISO может в этом месте задать вопрос: ИБ-комплаенс, позиция ФСТЭК, показатели защищённости из Методики, субъекты КИИ и теоретические компьютерные инциденты — это всё прекрасно и замечательно. Но как насчёт безопасности на местах и реальных кейсов? Может быть, есть какой-то практический совет как «рыбак рыбаку»?

СЦЕНАРИЙ ОДНОГО ЭКСПЕРИМЕНТА ДЛЯ CISO

Как проверить, что привилегированные пользователи (ИТ- и ИБ-администраторы, руководители высшего звена и их помощники/советники/секретари) выполняют / НЕ выполняют требования установленной парольной политики в вашей организации, признавшей себя субъектом КИИ?

Подойдите на рабочее место привилегированного пользователя и попросите его при вас ввести свой действующий пароль для доступа в операционную систему, в электронную почту и/или к интерфейсу администрирования сервера, а также к любой известной эксплуатируемой

в вашей компании децентрализованной системе. Да, это будет инцидентом ИБ и фактом явной компрометации паролей. Ничего страшного, поскольку этот эксперимент происходит под вашим непосредственным контролем как CISO.

Затем попросите пользователей устно перечислить вам основные требования утверждённой парольной политики в компании и порекомендуйте ему сменить свои пароли на новые в соответствии с этими требованиями. Для «чистоты эксперимента» повторите этот сценарий несколько раз с типичными представителями разных подкатегорий пользователей в вашей организации и с позиции CISO оцените полученные результаты.

Таким образом вы сможете удостовериться / получите дополнительные факты и примеры, подтверждающие, что:

1. В вашей организации действует (не действует) утверждённая парольная политика и пользователи (в том числе привилегированные) ознакомлены (не ознакомлены), применяют (не применяют) её базовые требования;

2. Привилегированные пользователи соблюдают (нарушают) требования утверждённой парольной политики при доступе к централизованным / не централизованным автоматизированным системам;

3. Учётные записи привилегированных пользователей (и в целом система безопасности, основанная на стойкости паролей) являются / не являются в настоящее время точкой потенци-

альной компрометации и/или каналом проникновения злоумышленников внутрь защищаемого периметра.

[Платная альтернатива эксперименту — настроить парольную политику и заказать услугу по проверке качества всех паролей организации — прим. ред.]

ВМЕСТО ЗАКЛЮЧЕНИЯ

При формулировании и реализации требований парольной политики у субъекта КИИ важно помнить о сложно достижимом балансе: с одной стороны, CISO нужно обеспечить необходимый и достаточный уровень защищённости объектов КИИ, а с другой — попытаться избежать избыточных неудобств для пользователей, применяющих пароли при доступе в системы. Внедрение негибкой парольной политики может вызвать обратный эффект: пользователи, в том числе привилегированные, будут стремиться всеми силами обойти установленные парольные ограничения, что, в свою очередь, приведёт к новым компьютерным инцидентам.

В качестве завершающей рекомендации обращаю внимание читателя на такие технологические, частично компенсирующие парольные уязвимости инструменты, как:

- ♦ системы для безопасного хранения, управления и регенерации уникальных паролей;

- ♦ технологии двухфакторной/мультифакторной аутентификации, как дополнительный к базовому паролю уровень защиты (контактный/бесконтактный токен, биометрия, SMS/PUSH) *[уровень аутентификации должен соответствовать уровню доверия информационной системы, см. статью С. Груздева «Аутентификация. От паролей к адаптивной МФА», с. 12–19 № 3 (58) за 2025 г. «Информационная безопасность бизнеса» (BIS Journal) — прим. ред.]*;

- ♦ обновлённые/дополнительные алгоритмы хеширования и использование «соли» при хранении паролей на серверах/при вынужденной передаче чувствительных данных вовне (для целей миграции, интеграции, тестирования и пр.).

Внедрение негибкой парольной политики может вызвать обратный эффект: пользователи, в том числе привилегированные, будут стремиться всеми силами обойти установленные парольные ограничения, что, в свою очередь, приведёт к новым компьютерным инцидентам

АУТЕНТИФИКАЦИЯ И ЭП С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИИ



Сергей ГРУЗДЕВ
генеральный директор
«Аладдин Р.Д.»

Данная статья является продолжением материала «Аутентификация — от паролей к адаптивной МФА», опубликованного в BIS Journal № 3 (58) за 2025 год, и рассматривает особенности применения биометрических технологий для аутентификации и ЭП пользователей.

ПАРОЛИ

Использование паролей в качестве единственного фактора не позволяет обеспечить надежную аутентификацию пользователей информационных систем (ИС). Дополнительные риски связаны с новыми возможностями генеративного искусственного интеллекта, который (в частности, ChatGPT-4) собрал (и продолжает собирать) все возможные пароли, которые когда-либо были использованы для доступа к информационным сервисам и ресурсам, а учетная запись была взломана или украдена.

Теперь ИИ способен при определенных условиях практически мгновенно выдать¹ нужное значение, независимо от длины пароля или парольной фразы и мощности алфавита (количества используемых букв в разных регистрах, цифр и символов).

¹ По материалам <https://www.hivesystems.com/blog/are-your-passwords-in-the-green>

Организации, использующие только пароли (простую аутентификацию), не контролируют свой периметр и являются первейшими кандидатами на взлом и утечки.

СРЕДСТВА 2ФА (ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ)

В отличие от пароля (единственного фактора — запоминаемого секрета), здесь добавляется второй фактор — владение аппаратным устройством (USB или OTP-токеном, смарт-картой). При этом пароль (или PIN-код) является способом подтверждения факта владения данным устройством.

Долгое время считалось, что этого вполне достаточно, и средства 2ФА обеспечивают должный уровень безопасности при аутентификации пользователей и использовании ими электронной подписи (ЭП, квалифицированной ЭП, усиленной квалифицированной ЭП).

Что видим на практике, какие проблемы и риски безопасности для ИС?

1. Пресловутый «человеческий фактор»:

◆ Пользователи частенько передают свои средства 2ФА другим, а те подключаются и работают в ИС от их имени (нет привязки средства 2ФА к личности его владельца).

◆ Пользователи частенько забывают свой PIN-код, несколько раз подряд вводят его неправильно и устройство блокируется — возрастает простой и нагрузка на администраторов.

◆ Использование PIN-кода, установленного по умолчанию (вопиющие ошибки администрирования) — как следствие, теряется фактор знания — «секрета» для разблокирования аппаратного средства.

2. Удалённая работа, в т.ч. из не-доверенной среды:

◆ Многие пользователи работают удалённо, в т.ч. подключаются к ИС с домашних/личных компьютеров, которые могут скрытно управляться злоумышленниками, на которые могут быть подсажены специализированные трояны, в т.ч. реализующие атаки с подменой подписываемых документов.

Первая проблема — обычные средства 2ФА и ЭП (USB-токены и смарт-карты) не защищают от таких рисков и подобных атак.

Для защиты от них следует использовать специализированные средства обеспечения безопасной дистанционной работы пользователей из недоверенной среды, соответствующие требованиям 32-го Приказа ФСТЭК России, например, Aladdin LiveOffice².

Такие же требования к организации удалённого доступа для пользователей организации, её контрагентов и подрядных организаций содержатся и в новом 117-м Приказе ФСТЭК России.

Вторая проблема, возникающая при удалённой работе, особенно для администраторов и привилегированных пользователей, имеющих расширенный доступ к ИС организации и расширенные полномочия (а как следствие — повышенные риски причинить существенный ущерб) — это подтверждение личности пользователя.

Помним, что чем больше риск, тем больше методов и способов для подтверждения личности пользователя следует применять³.

² См. описание продукта <https://www.aladdin-rd.ru/catalog/liveoffice/>

³ См. ГОСТ Р 70262.2-2025 (Идентификация и аутентификация. Уровни доверия аутентификации), разработчик «Аладдин Р.Д.».

Средства 2ФА являются обязательными и надёжными при работе пользователей в офисе, в доверенной среде исполнения (на администрируемых организацией средствах вычислительной техники (СВТ)).

Однако они не обеспечивают требуемого уровня информационной безопасности (ИБ) при дистанционной работе и работе из недоверенной среды (личные СВТ, не контролируемые и не администрируемые организацией).

БИОМЕТРИЯ

Для подтверждения личности пользователя с учётом упомянутого «человеческого фактора» применяется биометрия. В сфере ИТ и ИБ она стала применяться относительно недавно, и ей, естественно, свойственны многие «детские» болезни — неправильное применение, ошибки реализации и пр.

Давайте разбираться подробнее. Начнём с основ и сфокусируемся на применении биометрии для решения задач аутентификации, ЭП и прохода (доступа) на объекты критической информационной инфраструктуры (КИИ).

Основы биометрии. Краткие выжимки из учебного пособия⁴.

Биометрия делится:

- ♦ На контактную и бесконтактную.
- ♦ По месту и способу хранения биометрических данных — с единой централизованной базой и без неё, с использованием так называемого «распределённого» хранения данных.

Контактная биометрия — к ней относится технология распознавания по отпечаткам пальцев, ладоней и пр.

Бесконтактная биометрия — технология распознавания по лицу, голосу и пр. (лежит в основе ЕБС).

И сразу по тексту книги предупреждение, большими буквами:

Категорически не допускается использование бесконтактной биометрии для целей идентификации и аутентификации пользователей в ИС и для доступа на объекты КИИ.

Почему? Да потому что авторы книги, настоящие профессионалы, еще в 2003–2004 гг. прекрасно понимали и предсказывали, что за 10 лет генеративный ИИ разовьётся до такого уровня, что на лету сможет генерировать нужный для обмана системы голос и видео.

Что мы сегодня и наблюдаем — расцвет дипфейков и доступность инструментов для их создания. Эта первая и самая важная проблема.

Вторая существенная проблема — централизованное хранение собираемых персональных биометрических данных. Защитить такую базу практически невозможно⁵, следовательно, будут утечки. В отличие от паролей или средств 2ФА, которые можно оперативно перевыпустить, с биометрией такой фокус не проходит. Разве что массово делать пластические операции?

Третья проблема — при правильной реализации это достаточно дорого (защита среды исполнения, канала, базы данных и пр.).

То, что нам продолжают навязывать использование ЕБС для целей аутентификации в ИС и доступа на объекты КИИ — это просто опасно.

Контактная биометрия. Лидером здесь является технологии распознавания по отпечаткам пальцев (Fingerprint). Что важно и оказывает существенное влияние на надёжность и безопасность её использования?

1. Используемая технология:

- ♦ идентификация (один отпечаток ко многим из базы данных);
- ♦ верификация (один к одному — сравнение предъявленного отпечатка с эталоном).

2. Место хранения биометрических данных (эталонных шаблонов с привязкой к персональным данным пользователя):

- ♦ централизованное хранение (база данных);
- ♦ распределённое хранение эталонных шаблонов (без единой базы данных):
 - а) в защищённой среде — в персональном аппаратном устройстве пользователя — токене, смарт-карте;

б) в незащищённой среде (например, в компьютере пользователя или в общем терминале доступа).

3. Тип сканера отпечатков пальцев и его расположение:

♦ оптический или полупроводниковый;

♦ внешний или встроенный в персональное устройство или в терминал доступа.

Оптический сканер делает фото отпечатка пальца. А дальше передает его в терминал или в компьютер для обработки и отправки на сравнение с эталоном. Эталон может находиться в базе данных или в персональном устройстве (токене, смарт-карте).

Недорогой сканер можно достаточно просто обмануть, подсунув ему отпечаток, снятый, например, с использованного стакана. Хороший оптический сканер значительно дороже и существенно больше — с собой его носить уже накладно и неудобно.

Основная проблема — передача отпечатков пальцев в ИС. Это делает её владельца оператором персональных биометрических данных со всеми вытекающими...

Полупроводниковые сканеры, как правило, емкостные, существенно дешевле, надёжнее и компактнее, что позволяет размещать их «на борту» специализированных устройств аутентификации и ЭП, не передавать снятые отпечатки пальцев в ИС, а обрабатывать их и производить сравнение с шаблоном (верификацию 1:1) внутри аппаратного устройства.

Различают два типа полупроводниковых сканеров — протяжные (щелевые — когда палец нужно аккуратно протащить через неё), и прижимные, когда палец нужно прижать к сенсору.

Протяжные сканеры снимают с движущегося пальца серию отпечатков (полосок), а далее с помощью специального программного обеспечения (ПО) склеивают их в единое изображение. Качество получаемого изображения плохое, надёжность, как правило, не превышает 1:10 — 1:100. Дешевая никчёмная игрушка.

Прижимные сканеры сразу дают полноценную «картинку» и обеспечивают надёжность на уровне от 1:10,000 до 1:100,000.

⁴ Настоятельно рекомендую прочитать книгу «Руководство по биометрии», Р.М. Болл, Дж.Х. Коннел, изд. Техносфера, 2007

⁵ Знаю это не понаслышке, наша компания занимается этим более 20 лет



Рисунок 1. Персональный BIO-токен и Aladdin SecurBIO Reader

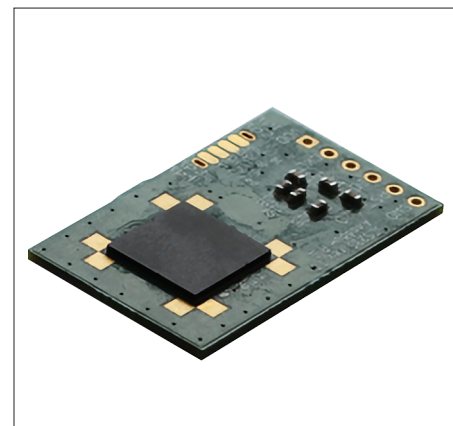


Рисунок 2. OEM-модуль для встраивания в оборудование

Для контактной биометрии это предел. Почему? Потому что на планете Земля с вероятностью 1:100,000 у каждого из нас существует «биологический двойник» с такими же отпечатками. Доказанный факт.

Обмануть полупроводниковый сканер с оставленным на стакане жирным отпечатком не получится.

Что ещё важно знать? Практически все полупроводниковые сканеры поставляются на рынок (производителям электроники) в виде сборок — сенсор + чип.

В чипе реализована необходимая математика, и при сравнении предъявленного отпечатка с сохранённым в чипе шаблоном, на выходе получаем 0 (отказ) или 1 (совпадение) — такой вот простейший тумблер — «свой/чужой». Элементарное изменение в схемотехнике — и ты всегда «свой».

Увы, но многие производители электроники и средств защиты информации (СЗИ) с использованием биометрии допускают эту детскую ошибку, обнуляя их безопасность.

ALADDIN SecurBIO

Под этим названием компания «Аладдин» недавно выпустила три новых продукта:

- ◆ Персональный BIO-токен.
- ◆ Smart-карт ридер со встроенным сканером отпечатков пальцев и smart-карты для безопасного хранения шаблонов.
- ◆ OEM-модуль на базе BIO-токена для встраивания в оборудование (для производителей терминалов, компьютеров и пр.).

Персональный BIO-токен. Обеспечивает «привязку» личности пользователя к физическому носителю (USB-токену с встроенным прижимным полупроводниковым сенсором) и невозможность его передачи и использования посторонними (рис. 1).

Для начала работы с BIO-токеном его необходимо разблокировать, приложив к сканеру палец. После снятия отпечатка внутри BIO-токена производится его оцифровка и получение шаблона — аналога односторонней хеш-функции, и далее — сравнение с ранее сохранённым в чипе BIO-токена эталонным шаблоном. При совпадении с заданной вероятностью⁶ предъявляемого шаблона с эталоном все необходимые функции BIO-токена разблокируются, и он «превращается» в привычный USB-токен JaCarta PKI/ГОСТ — средство строгой или усиленной аутентификации и ЭП.

Важно: отпечатки пальцев не попадают ни в компьютер, ни в ИС, а владелец ИС не становится оператором персональных биометрических данных (в отличие от ЕБС).

SMART-КАРТ РИДЕРЫ И SMART-КАРТЫ С ПОДДЕРЖКОЙ БИОМЕТРИИ

Aladdin SecurBIO Reader — семейство профессиональных smart-карт ридеров Enterprise-класса с встроенным прижимным полупроводнико-

вым сканером отпечатков пальцев (рис. 1):

- ◆ JCR761 — smart-карт ридер с горизонтальной загрузкой smart-карты.
- ◆ JCR781 — smart-карт ридер с вертикальной загрузкой smart-карты.

Рекомендуется для организации совместной или сменной работы пользователей за одним рабочим местом (один ридер и у каждого своя smart-карта с загруженными в неё эталонными шаблонами отпечатков пальцев), при использовании одной smart-карты (с RFID) для доступа на объект/в помещения, для интеграции со средствами контроля и управления доступом (СКУД).

Преимущества. BIO-токены/ридеры и smart-карты позволяют реализовать как трёхфакторную аутентификацию (3ФА), так и 2ФА, отказавшись от использования паролей (PIN-кодов), и убрать тот самый пресловутый «человеческий фактор». При этом останется фактор владения физическим устройством и биометрический фактор — разблокировать и использовать устройство сможет только его владелец.

РЕЗЮМЕ

Внедрение аутентификации и ЭП с использованием биометрии позволит отказаться от использования паролей и кардинально решить проблему «человеческого фактора», правильно и эффективно распределить бюджет на ИБ.

Надёжная система аутентификации в ИС — основа и залог её безопасности.

⁶ FAR и FRR можно настраивать, добиваясь значений 1:10,000 – 1:100,000

ЭВОЛЮЦИЯ ДОВЕРИЯ

КАК НОВЫЕ ТРЕБОВАНИЯ РЕГУЛЯТОРА МЕНЯЮТ DEVSECOPS В ФИНТЕХЕ



Илья НОВОЙДАРСКИЙ
руководитель группы инновационных решений УЦСБ

За последние два года российский финансовый сектор столкнулся с масштабным обновлением требований к защите информации и операционной надежности. В документах Банка России и новой редакции ГОСТ Р 56939–2024 акцент сместился с формального наличия бумажных регламентов на реальную, доказательную защищенность, встроенную в сам процесс разработки.

На практике это означает, что безопасность должна оставлять цифровой след, который можно в любой момент предъявить внутреннему контролю, аудитору или регулятору. Давайте разберемся, как интерпретировать новые положения ЦБ через призму DevSecOps и почему инструменты класса ASOC (Application Security Orchestration and Correlation) становятся фундаментом для построения доказательной базы.

ОТ РАЗОВЫХ ПРОВЕРОК К НЕПРЕРЫВНОМУ ПРОЦЕССУ

Цель регулятора — увидеть полную картину безопасности приложения.

Если приложение обновляется ежедневно, то классический ежегодный аудит безопасности становится скорее архивным документом, чем инструментом управления. В то время как регулятору нужен живой процесс.

Положение ЦБ 821-П, вступившее в силу в 2024 году, стало базовым документом для защиты переводов денежных средств. И ключевой момент здесь — требования к зрелости разработки. Для критичного ПО документ требует сертификации ФСТЭК России либо оценки соответствия по ОУД 4 (ГОСТ Р ИСО МЭК 15408–3). Важно понимать: ОУД 4 отражает не просто факт успешного тестирования, а обеспечение воспроизводимости результатов. У вас должны быть документально зафиксированы проектные решения, доказательства тестов, анализ уязвимостей и жесткий контроль их исправления.

Кроме того, 821-П требует регистрировать действия работников при доступе к защищаемой информации. И речь здесь не о простых коммитах в Git. Код и конфигурации — критичные объекты, поэтому требование регулятора на инженерном языке означает

сквозную трассируемость (traceability): вы должны видеть связь между бизнес-требованием, изменением в репозитории, конкретной сборкой, релизом и записью в журнале эксплуатации. Так вы в любой момент будете четко понимать, кто инициировал изменения, что именно попало в релиз и где сейчас работает.

Положение ЦБ 851-П усиливает требования к регулярным проверкам. В документе закреплено требование ежегодного тестирования на проникновение. Но для банка, работающего в парадигме DevOps, этого критически мало: риски появляются с каждым новым релизом.

Банки вынуждены внедрять непрерывные проверки: статический (SAST) и динамический (DAST) анализ, сканирование зависимостей (SCA), контроль контейнеров и конфигураций. Регулятор не диктует конкретные утилиты, но ожидает, что процесс будет прозрачным и доказуемым.

Новое Положение ЦБ 850-П вводит жесткие требования к операционной надежности и дисциплине изменений. Релиз — теперь объект управления, а не просто факт выкатки в прод.

Немалая доля инцидентов в банках связана не с хакерами, а с дефектами кода и ошибками конфигурации, которые возникли с обновлением. DevSecOps здесь работает в двух направлениях: снижает киберриски и стабилизирует релизный конвейер. Если настроены Quality Gates, а уязвимости реально исправляются и перепроверяются, вы получаете управляемость — именно то, к чему стремятся команды ИБ, разработки и аудиторы от регулятора.

ГОСТ Р 56939–2024: ОТ РЕГЛАМЕНТОВ К ЖИВЫМ ПРОЦЕССАМ

Новая редакция ГОСТ Р 56939–2024 соотносит регуляторные требования с реалиями современной разработки.

Для банка, работающего в парадигме DevOps, ежегодного тестирования на проникновение критически мало: новые риски появляются с каждым новым релизом

Раньше подход строился на мерах: написали регламент – поставили галочку. Теперь фокус на процессах: вход, выход, роли и артефакты. Нужно не просто провести анализ один раз, а выстроить конвейер автоматического запуска анализаторов для каждого релиза и при этом подтвердить существование процесса наличием артефактов.

Стандарт описывает блоки процессов, которые нужно внедрить:

- ◆ Управление требованиями и архитектурой;
- ◆ Контроль исходного кода, сборок и релизов;
- ◆ Все виды проверок (SAST, DAST, SCA, MAST и др.);
- ◆ Управление уязвимостями: найти, исправить и проверить повторно;
- ◆ Мониторинг и метрики: процесс должен быть измеримым.

Чтобы совершить переход без боли, необходимо выстроить целостный контур управления: выделить критичные системы, провести аудит этапов разработки, назначить владельцев бизнес-процессов из команд ИБ, разработки и эксплуатации, а также определить артефакты для аудита. Суть – в автоматизации проверок в пайплайнах, создании задач в трекере и внедрении метрик, таких как скорость устранения уязвимостей (TTE/TTR) и покрытие репозитория. ГОСТ прямо требует автоматизации управления недостатками, поскольку таблицы и почта не обеспечивают ни прослеживаемости, ни дисциплины процесса.

РОЛЬ ASOC В ПОСТРОЕНИИ ДОКАЗАТЕЛЬНОЙ БАЗЫ

В получении оценки по ОУД 4 сложность представляет сбор доказательств. При прохождении аудитов надо иметь аргументированные ответы на вопросы: «Как вы гарантируете, что в релиз не попала критичная уязвимость? Где лог решения по false positive? Кто подтвердил исправление?».

И здесь на сцену выходят решения класса ASOC, такие как Apsafe. Проблему классического AppSec, когда инструменты (сканеры, баг-трекер, документация) не интегрированы друг с другом, решает ASOC-система, работающая как еди-

ный хаб. Система собирает результаты всех сканеров, убирает дубли, связывает находки с конкретными версиями ПО и ведет историю всех решений.

Кейс Apsafe: управляемый сервис как опора. Apsafe – готовый сервис от УЦСБ. Он имеет в ядре систему класса ASOC и берет на себя оркестрацию запуска проверок и валидацию результатов AppSec-аналитиками.

Главное преимущество – скорость старта. Самостоятельное построение ASOC внутри банка предполагает найм, закупку и настройку инструментов, занимающую месяцы. Apsafe позволяет срезать этот угол: техническое подключение и получение первого валидированного отчета занимает около 10 дней. Таким образом, безопасность переводится в режим регулярного конвейера (проверки ежемесячно или чаще) с самого старта.

Как решение работает в банке?

Вы подключаете репозитории и пайплайны. Система автоматически запускает проверки при изменениях. Результаты агрегируются в единый интерфейс, где аналитики отсеивают ложные срабатывания. Подтвержденные баги передаются в трекер разработчиков уже с контекстом и приоритетом.

Банк для аудита получит готовый набор артефактов:

- ◆ полную историю сканирований по каждому релизу
- ◆ реестр уязвимостей с доказательствами и статусами
- ◆ журнал принятых решений (с обоснованием false positive, отложеного исправления и т.д.)
- ◆ подтверждение повторных проверок (re-test) после исправления
- ◆ сводные метрики по динамике рисков.

Производственная доказательная база формируется сама в процессе работы, без судорожной подготовки документов за ночь до прихода проверяющих из ЦБ.

Apsafe – облачная платформа. Для управляемых сервисов это норма. Комплаенс может быть спокоен: в решении применяется сегментация данных клиентов, RBAC (Role-based access control), удаление данных по-

сле анализа. Если банк категорически против облака, возможен on-premise, но на внедрение потребуется выделить больше времени и внутренних ресурсов для поддержки.

ПЛАН ДЕЙСТВИЙ: БЫСТРЫЙ СТАРТ И ВЫХОД НА ЗРЕЛОСТЬ

Если самостоятельное выстраивание процессов обычно занимает кварталы, то с управляемым сервисом график сжимается до 90 дней.

Быстрый старт. Подключение репозитория, настройка доступов и получение первых результатов анализа. Банк видит реальную картину уязвимостей уже через 10 дней.

Процесс. На согласование артефактов для аудита, интеграцию с трекером задач и запуск регулярных проверок (не реже 1 раза в месяц) с валидацией от экспертов сервиса уйдет до 20 дней.

Масштабирование и SLA. Раскатка практики на все ключевые системы. Введение SLA на исправление багов и включение Quality Gates в пайплайны. Формирование пакета документов для внутреннего аудита уже на основе накопленной статистики. Процесс займет до 2 месяцев.

Новая регуляторная реальность финансового сектора устанавливает принцип: безопасность должна быть воспроизводимой и доказуемой. Выигрывают те команды, которые перестают плодить бумажные отчеты и строят единый цифровой контур управления: от коммита до закрытого тикета в таск-трекере. Сервисы класса ASOC позволяют сделать этот процесс промышленным, избавляя ИБ-специалистов от рутины и давая бизнесу прозрачность. Именно таким решением является Apsafe от УЦСБ – компании с 18-летним опытом в ИБ. Apsafe помогает выполнять требования регулирующих органов в части безопасной разработки ПО, предоставляет набор артефактов, необходимых в процессе аудита.

В СООТВЕТСТВИИ С ГОСТ Р 57580.1-2017

СЕГМЕНТАЦИЯ И МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ



Екатерина ГОЛУНЧИКОВА
ведущий сетевой аналитик
компании «Нетопия»



Александр ТОВСТОЛИП
руководитель управления
информационной безопасности
Ассоциации ФинТех

Финансовым организациям необходимо соответствовать большому количеству различных стандартов по защите информации. Эксперты BIS Journal рассказывают, как реализовать и проверить требования ГОСТ Р 57580.1-2017 в контексте мер процесса «Обеспечение защиты вычислительных сетей».

ОСНОВНЫЕ СЛОЖНОСТИ

При выстраивании работы по соблюдению требований ГОСТ Р 57580.1-2017 финансовые компании сталкиваются со множеством проблем и вопросов. Основные из них:

- ♦ Что такое «контур безопасности» согласно ГОСТ Р 57580.1-2017 вообще и как его выделить в своей сети?
- ♦ Какие сегменты сети будут входить в контур безопасности, а какие остаются за его пределами и какой трафик может ходить между этими сегментами?
- ♦ Как правильно настроить межсетевые экраны и доказать соответствие требованиям, когда в сети десятки межсетевых экранов от разных производителей?
- ♦ Как обеспечить не разовую проверку, а постоянное соответствие требованиям?
- ♦ Можно ли это всё автоматизировать и когда без этого никак?

Сегодня мы подробно рассмотрим эти вопросы и постараемся найти ответы на каждый из них.

О ГОСТ Р 57580.1-2017

Начнём с азов. ГОСТ Р 57580.1-2017. «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» — отраслевой стандарт, который содержит требования к созданию системы защиты для финансовых организаций.

Полный текст ГОСТ Р 57580.1-2017 можно посмотреть по ссылке¹.

Положения Банка России (851-П, 821-П, 757-П, 802-П) делают его обязательным для следующих организаций:

- ♦ кредитные финансовые организации (банки);
- ♦ страховые организации, негосударственные пенсионные фонды;
- ♦ операторы по переводу денежных средств, операторы электронных платформ и многие другие.

ОПРЕДЕЛЕНИЕ КОНТУРОВ БЕЗОПАСНОСТИ

Первоочередная задача — это определение контура безопасности и требуемого для него уровня защиты информации (рис. 1). В сети выделяются сегменты (подсети), в которых размещаются защищаемые финансовые системы.

Какие системы являются защищаемыми — это отдельная большая тема. Например, в Положении № 821-П указано, что объектами защиты являются

все автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, которые эксплуатируются и используются при осуществлении переводов денежных средств. Таким образом, все средства и системы, используемые для переводов денежных средств, будут входить в контур безопасности.

После определения перечня защищаемых систем анализируется состав сегментов корпоративной сети и выделяются те, которые войдут в контур безопасности (Contour):

- ♦ сегмент хранения и обработки данных — серверы систем;
- ♦ сегмент управления — рабочие места администраторов;
- ♦ сегмент пользователей — рабочие места пользователей.

Помимо контура безопасности, в сети выделяются следующие сегменты:

- ♦ сегмент для банкоматов и платёжных терминалов — Terminal;
- ♦ сегмент разработки и тестирования — DevOps;
- ♦ сегмент беспроводной сети — Wi-Fi;
- ♦ сегмент мобильных устройств — Mobile;
- ♦ остальные внутренние сегменты локальной вычислительной сети — LAN.

Важно отметить, что не все перечисленные сегменты обязательно должны присутствовать в сети. Их наличие зависит от конкретной структуры и процессов организации.

¹ <https://clck.ru/3RMtVr>

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
СМЭ.1	Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры каждого из контуров безопасности (далее – сегменты контуров безопасности)	Н	Т	Т
СМЭ.2	Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, сегментов контуров безопасности и внутренних вычислительных сетей финансовой организации, не предназначенных для размещения информационной инфраструктуры, входящей в контуры безопасности (далее – иные внутренние вычислительные сети финансовой организации)	Н	Т	Т
СМЭ.3	Межсетевое экранирование вычислительных сетей сегментов контуров безопасности, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1	Н	Т	Т

Рисунок 1. Требования ГОСТ Р 57580.1–2017 по выделению контуров безопасности

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
СМЭ.7	Реализация запрета сетевого взаимодействия сегмента разработки и тестирования и иных внутренних вычислительных сетей финансовой организации по инициативе сегмента разработки и тестирования	Н	Т	Т

Рисунок 2. Мера «СМЭ.7» из ГОСТ Р 57580.1–2017

ФОРМИРОВАНИЕ МАТРИЦЫ ДОСТУПА

Меры ГОСТ Р 57580.1–2017 определяют требования к взаимодействию между сегментами сети. Например, мера «СМЭ.7» запрещает взаимодействие между сегментом разработки и тестирования и внутренними сетями (рис. 2).

На основе анализа всех требований стандарта для соответствующего уровня защиты составляется матрица доступа. Эта матрица будет основой для настройки межсетевых экранов и фильтрации трафика между сегментами.

На рисунке (рис. 3) приведён пример матрицы доступа, составленной

для второго (стандартного) уровня защиты, где:

♦ allow – разрешённое взаимодействие;

♦ deny – запрещённое взаимодействие;

♦ знак со стрелками обозначает, что взаимодействие разрешено только для конкретного ограниченного трафика.

	Contour	LAN	Terminal	Devops	WiFi	Mobile	Internet
Contour	allow	↔	↔	↔	↔	↔	↔
LAN	↔	allow	↔	↔	↔	↔	↔
Terminal	↔	↔	allow	↔	↔	↔	↔
Devops	deny	deny	deny	allow	deny	deny	↔
WiFi	deny	↔	deny	deny	allow	↔	↔
Mobile	deny	↔	deny	deny	↔	allow	↔
Internet	deny	↔	deny	deny	deny	deny	allow

Рисунок 3. Матрица доступа

Настройка межсетевых экранов должна осуществляться в соответствии с разработанной матрицей доступа.

АУДИТ И ПОДДЕРЖАНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

В рамках аудита проверяются настройки межсетевых экранов. Анализ правил одного или нескольких межсетевых экранов на соответствие установленным требованиям безопасности не представляет сложности. Однако ситуация кардинально меняется в условиях распределённой

корпоративной сети с большим количеством филиалов, где функционирует множество межсетевых экранов. И всё это усложняется «зоопарком» из кучи оборудования разных производителей.

Для того чтобы гарантировать соответствие установленным требованиям, необходимо провести анализ правил каждого межсетевого экрана. Кроме того, необходимо не только провести однократную проверку или аудит, но и обеспечить постоянное соответствие требованиям. Важно следить за тем, чтобы добавление новых правил в полити-

ки межсетевых экранов не противоречило созданной матрице доступа.

В таких условиях без автоматизации процесса уже невозможно обойтись, поскольку ручные методы управления становятся неэффективными и могут привести к ошибкам и нарушению требований.

КАК АВТОМАТИЗИРОВАТЬ

Политики безопасности межсетевых экранов — это набор правил, которые определяют, как межсетевого экран обрабатывает сетевой трафик для определённых IP-адресов, номеров портов и протоколов (рис. 4).

```
access-list 101 permit tcp 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255 eq telnet
access-list 101 permit tcp 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255 eq ftp
access-list 101 permit tcp 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255 eq http
access-list 101 deny ip 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255
```

Рисунок 4. Пример правил межсетевого экрана

По опыту аудита в финансовых организациях можно сказать, что эти политики иногда содержат десятки и даже сотни тысяч правил. А в больших банках количество правил может достигать нескольких миллионов!

Для решения задач управления политиками межсетевых экранов и упрощения процесса проверки могут использоваться автоматизированные инструменты. Инструменты бывают разные, и у них есть свои плюсы и минусы (рис. 5).

Выбор инструмента для автоматизации зависит от конкретных потребностей организации, а также от таких факторов, как поддержка вендоров межсетевых экранов, функциональность и стоимость.

РЕПОЗИТОРИЙ АФТ

ГОСТ Р 57580.1-2017 требует от финансовых компаний внимательно подхо-

дить к выбору ИТ-решений и оценке их безопасности. Для поиска таких решений компания может обратиться напрямую к вендорам, а может использовать доверенные репозитории. Так, на российском финансовом рынке уже существует отраслевой репозиторий для финансовой отрасли – Репозиторий ИТ-решений Ассоциации ФинТех (АФТ). В нём реализован многофакторный интуитивный поиск, а размещаемые решения проходят всестороннюю проверку.

ЗАКЛЮЧЕНИЕ

При соблюдении мер, прописанных в ГОСТ Р 57580.1-2017, у представителей отрасли возникают вопросы и проблемы, основные из которых мы сегодня разобрали. В частности, мы выяснили, что меры процесса «Обеспечение защиты вычислительных сетей» ГОСТ Р 57580.1-2017 транс-

лируются в матрицу доступа, которая должна быть применена на межсетевых экранах.

В небольших организациях проверка корректности настроек и их соответствия матрице доступа может осуществляться вручную, путём анализа политик межсетевых экранов. Однако в крупных сетях не обойтись без автоматизации. Внедрение автоматизированных решений класса NSPM облегчает аудит и позволяет поддерживать постоянное соответствие требованиям ГОСТ Р 57580.1-2017 в условиях распределённой сетевой инфраструктуры.

В заключение следует подчеркнуть, что грамотная сегментация сети и настройка межсетевых экранов играют ключевую роль в обеспечении сетевой безопасности. Это важно не только для соблюдения требований регуляторов, но и для обеспечения реальной безопасности сетей.

Тип инструмента	Стоимость	Примеры инструментов	Плюсы	Минусы
Ручные проверки	Бесплатно	Чек-листы по матрице доступа	Простота	Если правил много — нереализуемый сценарий
Скрипты и утилиты	Низкая	Python, Bash	Быстрая реализация, низкая стоимость	Требует навыков программирования. Невозможно обеспечить постоянный мониторинг изменений правил
Решения NSPM (Network Security Policy Management — управление сетевыми политиками безопасности)	Средняя/Высокая	Netopia, Tufin, Efron, Check Point SmartCenter	Автоматизация процесса, мониторинг изменений. Генерация отчётов «по кнопке» для оценки соответствия конкретным требованиям стандартов	Высокая стоимость внедрения и поддержки. Не все поддерживают разных вендоров МЭ

Рисунок 5. Сравнение инструментов управления политиками межсетевых экранов

ПРОИЗВОДИТЕЛЬНОСТЬ NGFW

САМОЕ ГЛАВНОЕ ДЛЯ ВЫЯВЛЕНИЯ АТАК НА ВЫСОКИХ СКОРОСТЯХ



Евгений КУТУМИН
эксперт группы разработки PT NGFW
в Positive Technologies

Представьте, вы управляющий банком. Звонит начальник безопасности: «Слишком много желающих нас ограбить. Снимаем решетки с окон и открываем сейфы, так проще работать». Абсурд? Но именно это делают некоторые межсетевые экраны, когда под нагрузкой молча отключают защиту, чтобы не тормозить трафик.

Но за PT NGFW можно не переживать, он так никогда не сделает. Расскажу, почему и чего это стоило.

Бизнесу нужны одновременно две вещи: безопасность и скорость. Причем требования к скорости растут лавинообразно. Российский ИТ-рынок прибавляет по 19–20% в год. 4G переходит в 5G, умные устройства множатся, видеопотоки переползают на 4K и 8K, нейросети встраива-

ются во все подряд. Каналы «толстеют», и все это нужно защищать без компромиссов.

Positive Technologies разрабатывает продукты с учетом требований ИБ, но при этом не жертвует важной для ИТ и сетей функциональностью. PT NGFW уже зарекомендовал себя как один из самых производительных межсетевых экранов на российском рынке. Модельный ряд покрывает широкий диапазон: от 400 Мбит/с до 100 Гбит/с, от 500 тысяч до 40 миллионов одновременных сессий.

Это не просто цифры. Данные по каждой модели мы получили на реальном трафике, максимально приближенном к клиентскому, со всеми включенными модулями безопасности: контроль приложений и пользователей, инспекция SSL/TLS, IPS, антивирус, URL-категоризация, Geo

Реальная производительность PT NGFW 3040 превышает заявленные показатели — максимальная пропускная способность при проверке зашифрованного трафика достигла 33 Гбит/с (при заявленных 25 Гбит/с)

Это возможно благодаря нашим инженерным решениям:

◆ **Модернизированный сетевой стек.** Мы отказались от стандартного сетевого стека Linux и перенесли обработку пакетов в user space с использованием технологий DPDK (Data Plane Development Kit). Это позволяет принимать пакеты напрямую в пользовательское пространство и обрабатывать их в пакетном режиме, убирая лишние переключения контекста и копирования буферов.

◆ **Zero-copy архитектура.** Нулевое копирование в памяти позволяет значительно снизить накладные расходы на работу с данными. Тем самым значительно увеличить количество обрабатываемых пакетов в секунду без потери функциональности.

◆ **Разделение management plane и data plane.** Резервирование отдельных ядер ЦП для management plane исключает потерю контроля над устройством при пиковых нагрузках на data plane.

КАЧЕСТВО ДЕТЕКТА

Производительность без качественного обнаружения атак бессмысленна. Здесь у нас принципиальная позиция: никакого Open Source. Мы провели эксперимент с 40 000 сигнатур из открытых источников (Snort, Suricata) и получили крайне слабый catch rate. Поэтому PT NGFW использует собственные сигнатуры, предоставляемые экспертным центром PT ESC. Если просто вставить сторонние Open Source правила, то одно неудачное может убить производительность всего устройства. У нас каждая сигнатура оптимизирована под архитектуру и конвейер обработки трафика PT NGFW.

Кроме того, тесная интеграция с другими продуктами экосистемы Positive Technologies (MaxPatrol SIEM, PT Sandbox, PT NAD, и др.) позволяет значительно повысить качество детекта за счет получения дополнительных данных об атаках.

НЕЗАВИСИМЫЕ ТЕСТЫ

Мы сознательно отдаем продукт на независимые проверки. Компания «Инфосистемы Джет» завершила комплексное тестирование PT NGFW, которое охватило более 300 проверок, включая производительность, функциональность и отказоустойчивость. В итоге производительность PT NGFW оказалась в два раза выше, чем заявлял Positive Technologies.

Тестирование в лаборатории BI.ZONE показало, что реальная производительность модели PT NGFW 3040 выше, чем указано в даташите. Максимальная пропускная способность при проверке зашифрованного трафика достигла 33 Гбит/с. При этом в документации PT NGFW указан потолок в 25 Гбит/с. Результаты испытаний также показали, что PT NGFW 3040 поддерживает до 20 млн одновременных соединений, тогда как в даташите указано 14 млн.

УСТОЙЧИВОСТЬ ПОД НАГРУЗКОЙ

В архитектуру PT NGFW изначально заложена возможность выдерживать пороговые значения производительности, не отключая и не сокращая ни на процент количество сигнатур. Защита остается стабильной, даже когда трафик упирается в потолок. Это принципиальное отличие от решений, которые ради скорости жертвуют безопасностью.

IP и 100 тысяч правил безопасности, включая NAT.

КАК УДАЛОСЬ ДОБИТЬСЯ ТАКОЙ ПРОИЗВОДИТЕЛЬНОСТИ

Долгое время считалось, что высокие скорости на межсетевых экранах невозможны без аппаратных ускорителей ASIC или FPGA. PT NGFW доказывает обратное, работая на процессорах общего назначения x86.

Мы проверяем производительность и стабильность PT NGFW по мировому стандарту тестирования межсетевых экранов — RFC9411, что жестче, чем у большинства российских разработчиков. И придерживаемся требования стандарта, что количество «дропов», то есть разницы между скоростью входящего и исходящего трафика, должно быть не более 0,01%.

Современные шифровальщики работают быстро:
в отдельных тестах — минуты, в типичном сценарии — менее часа.
У вас почти нет времени на раздумья.

ПЕРВЫЕ 60 МИНУТ ПОСЛЕ ТОГО, КАК ВАС ВЗЛОМАЛИ

ЧТО ДЕЛАТЬ, ЧТОБЫ НЕ СТАЛО ХУЖЕ



Денис БАТРАНКОВ
директор
по развитию
бизнеса
ГК «Гарда»

Эта статья — о первом часе после того, как вы узнали о киберинциденте. Когда неправильные управленческие решения могут нанести больший ущерб, чем сама атака: регуляторный, юридический и репутационный.

КАК КОМПАНИИ УЗНАЮТ О ВЗЛОМЕ

Взлом почти никогда не выглядит как «срочная тревога». В реальности это:

- ♦ Утром не работает бизнес-критичная система;
- ♦ Клиент сообщает об утечке;
- ♦ Журналист присылает запрос с вашими внутренними данными;
- ♦ Приходит письмо с вымогательством и реальным «образцом».

Общее одно: вы узнаете о проблеме после того, как всё уже произошло. Между проникновением и обнаружением часто проходят недели. Согласно статистике, в среднем мы узнаем о взломе через 42 дня. Поэтому первые 60 минут — это не борьба за инфраструктуру, а борьба за контроль последствий.

ТИПОВЫЕ ОШИБКИ ПЕРВЫХ МИНУТ

♦ **«Разберёмся сами».** Внутренняя команда редко имеет опыт расследо-

ваний. К моменту привлечения экспертов доказательства уже уничтожены.

♦ **«Выключите всё».** Потеря данных из оперативной памяти лишает следствие ключевых улик. Иногда это оправдано, но чаще — паника.

♦ **«Никому не говорить».** Информация всё равно выйдет наружу. В худшем случае компания узнаёт о собственном взломе из СМИ.

♦ **«Заплатим — и всё закончится».** Оплата не гарантирует восстановления и повышает риск повторной атаки.

♦ **«Быстро переустановим».** Вы теряете ответ на главный вопрос: как именно вас взломали. Значит — повторение неизбежно.

ПОЧЕМУ ВЫ УЖЕ ОПОЗДАЛИ — И ЭТО НОРМАЛЬНО

Любая целевая атака развивается по одной схеме:

1. Первичный доступ (фишинг, слабый пароль, уязвимость);
2. Разведка (карта сети, поиск админов);
3. Повышение привилегий (права администратора);
4. Полный контроль (почта, файлы, бэкапы);
5. Закрепление в нескольких системах и создание запасных входов.

Когда инцидент становится заметным бизнесу, злоумышленник уже на последнем этапе. Первый час — это не техническая гонка, а управленческий кризис.

ЧЕТЫРЕ ПРИОРИТЕТА ПЕРВОГО ЧАСА

1. Контроль. Должен быть один человек, принимающий решения. Не

комитет. Обычно — CISO или технический директор с явным мандатом от CEO.

Создаётся чистый канал связи: личные телефоны, личные мессенджеры. Корпоративные системы могут быть скомпрометированы.

2. Стабилизация. Цель: остановить распространение атаки.

При наличии SOC:

- ♦ Изоляция сегментов;
- ♦ Блокировки на сетевом уровне;
- ♦ Сохранение систем включёнными для расследования.

При отсутствии SOC:

- ♦ Физическое отключение кабелей;
- ♦ Вплоть до отключения питания;
- ♦ Потеря улики < потеря бизнеса.

3. Фиксация событий. Без журналирования происходящего компания уязвима юридически и регуляторно. Фиксируйте:

- ♦ Время событий и принятых решений;
- ♦ Скриншоты требований с экранов;
- ♦ Кто и на основании чего принял решения;
- ♦ Всю внешнюю коммуникацию.

После того как всё закончится, в отношении вас будет проводиться расследование, и вам будет необходимо вспомнить, что и почему вы делали. Лучше всего носить с собой включённую видеокамеру, чтобы потом были доказательства того, что вы не сделали хуже.

4. Коммуникации и PR. PR должен подключаться в первый час, а не после публикации новости.

Ключевой момент: в кризисе PR — это не «продажи» и не «репутация», а управление ожиданиями и защита от скальпирования.

Что нужно сделать сразу:

- ◆ Назначить одного официально-го спикера (все остальные молчат);
- ◆ Зафиксировать базовую позицию компании (1–2 абзаца максимум);
- ◆ Согласовать позицию между информационной безопасностью (ИБ), юристом и PR (единый фронт).

Чего нельзя делать:

- ◆ Говорить «инцидента нет», если он есть — потеря доверия навсегда;
- ◆ Обещать сроки и масштабы, которых вы не знаете;
- ◆ Спорить с журналистами и клиентами — это занимает время;
- ◆ Раскрывать технические детали на эмоциях.

Универсальная формула первого сообщения:

«Мы выявили инцидент информационной безопасности и проводим расследование. Работаем с профильными специалистами. Сообщим дополнительную информацию, как только будем готовы».

Эта формула защищает вас юридически, не создаёт ложных ожиданий и не блокирует будущие коммуникации.

РЕГУЛЯТОРИКА

Субъекты КИИ (критическая информационная инфраструктура). Для КИИ инцидент подразумевает взаимодействие с НКЦКИ (ГосСОПКА).

Критическое правило: публичные заявления не должны противоречить информации, направляемой регулятору. Несостыковки между пресс-релизом и официальным уведомлением — красный флаг при проверке.

Процесс согласования: ИБ подготавливает уведомление для НКЦКИ →

юрист согласует → PR пишет публичное сообщение на основе согласованного текста.

Банки и финансовые организации. Для банков ключевой кон-тур — ФинЦЕРТ Банка России и мониторинг ЦБ.

Здесь особенно важно:

- ◆ Согласование PR-сообщений с ИБ и комплаенс-отделом;
- ◆ Осторожность в терминологии: «сбой» vs «инцидент ИБ» vs «атака»;
- ◆ Отсутствие любых формулировок, которые могут трактоваться как сокрытие;
- ◆ Информирование о качестве управления кризисом, а не только о факте.

Для ЦБ важен не только факт атаки, но и ваша реакция на неё.

ЧЕК-ЛИСТ ГОТОВНОСТИ КОМПАНИИ

5 критических вопросов команде:

- ◆ Кто принимает решения ночью и в выходные? (Фамилия, личный телефон и резервный номер)
- ◆ Есть ли личные контакты ключевых людей вне корпоративных систем?

◆ Когда последний раз проводили полное тестовое восстановление из бэкапа?

◆ Сколько минут займёт изоляция критического сегмента сети?

◆ Есть ли подписанный договор с внешней командой реагирования?

5 действий на неделю:

1. Составить список критических систем с владельцами и их контактами;

2. Собрать личные номера кризисной команды — CEO, CISO, CTO, юриста, PR-директора;

3. Провести тестовое полное восстановление инфраструктуры из бэкапа;

4. Подготовить шаблоны сообщений: для сотрудников, клиентов, прессы, регуляторов;

5. Заключить или актуализировать договор с командой реагирования.

3 метрики для постоянного контроля:

1. Время до обнаружения (от начала атаки до обнаружения): цель < 24 часов.

2. Время до локализации (от обнаружения до полной изоляции): цель < 1 часа.

3. Покрытие мониторингом (% критических систем под наблюдением 24/7): цель 100%.

ГЛАВНЫЙ УРОК

Запомните из этой статьи одну вещь: в первые 10 минут определите одного человека, который принимает ВСЕ решения. Не комитет. Не совещание. Один человек с полномочиями. Это экономит часы хаоса.

Современные шифровальщики работают быстро. У вас мало времени, чтобы понять масштаб и не сделать хуже. Злоумышленники терпеливо ждали подходящего момента. Не отдавайте им ещё и первый час после того, как узнали.

Риск кибератаки неустраним — управляемы только её последствия. Первый час определяет не то, произойдёт ли взлом, а то, как быстро вы восстановитесь и какой урон понесёте.

Кого уведомлять	Когда	Зачем
СЕО	Немедленно (минуты 1–5)	Мандат на критические решения
Юрист	Первые 30 минут	Юридическая защита и консультация
PR / Коммуникации	Первый час	Подготовка к внешним обращениям
Внешняя команда реагирования	Первый час*	Расследование и фиксация улик
Страховая компания	2–4 часа	Условие выплаты — уведомление в срок
Регуляторы (НКЦКИ, ФинЦЕРТ)	По закону (24–72 ч)	Соблюдение требований безопасности

* Типовой «вторичный провал» — отсутствие договора с командой реагирования. Это означает, что в кризис вы будете искать её 1–2 часа. Подпишите договор заранее.

КВАРТАЛЬНЫЙ ОТЧЁТ

О НОРМАТИВНОМ РЕГУЛИРОВАНИИ В СФЕРЕ ИБ В IV КВАРТАЛЕ 2025 ГОДА



Екатерина РАЧКОВА
обозреватель BIS Journal

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА (КИИ)

23.10.2025 было опубликовано постановление Правительства Российской Федерации от 07.11.2025 № 1762 «О внесении изменений в некоторые акты Правительства Российской Федерации». Меняются Правила категорирования объектов КИИ и Перечень показателей критериев значимости объектов КИИ и их значений. Объекты КИИ решено категорировать с учётом отраслевых особенностей. Исходными данными для категорирования послужат в том числе перечни типовых отраслевых объектов КИИ и иные данные, определённые отраслевыми особенностями.

18–19.11.2025 были опубликованы проекты ведомственных актов ФСБ России:

- ♦ Об утверждении «Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведённых в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26.07.2017 № 187-ФЗ „О безопасности критической информационной инфраструктуры Российской Федерации“»;

- ♦ Об утверждении «Порядка обмена информацией о компьютерных атаках и компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты»;

- ♦ Об утверждении «Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и спо-

собах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

- ♦ Об утверждении «Порядка осуществления непрерывного взаимодействия субъектов критической информационной инфраструктуры Российской Федерации, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры Российской Федерации, а также руководителей органов и организаций, на которых возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26.07.2017 № 187-ФЗ „О безопасности критической информационной инфраструктуры Российской Федерации“, с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

25.12.2025 ФСТЭК России утвердил Приказ от 25.12.2025 № 548 «Об утверждении Порядка осуществления непрерывного взаимодействия субъектов критической информационной инфраструктуры Российской Федерации, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры Российской Федерации, а также руководителей органов и организаций, на которых возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26.07.2017 № 187-ФЗ „О безопасности критической информационной инфраструктуры Российской Федерации“, с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Также 25.12.2025 ФСТЭК России утвердил Приказ от 25.12.2025 № 547 «Об утверждении Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведённых в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26.07.2017 № 187-ФЗ „О безопасности критической информационной инфраструктуры Российской Федерации“».

25.12.2025 ФСТЭК России утвердил также Приказ от 25.12.2025 № 546 «Об утверждении Порядка обмена информацией о компьютерных атаках и компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными



органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты».

25.12.2025 ФСБ России опубликовала приказ от 24.12.2025 № 540 «О внесении изменений в Положение о Национальном координационном центре по компьютерным инцидентам, утвержденное приказом ФСБ России от 24.07.2018 № 366». Приказ устанавливает обновленные правила взаимодействия, информирования и реагирования на киберинциденты для субъектов КИИ, в том числе:

- ♦ уточняет, что задачей НКЦКИ является обеспечение координации деятельности не только субъектов КИИ, но и аккредитованных центров ГосСОПКА, а также органов и организаций по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

- ♦ определяет форматы представления информации о компьютерных атаках и компьютерных инцидентах в ГосСОПКА;

- ♦ определяет состав технических параметров компьютерной атаки и компьютерного инцидента, указываемых при представлении информации в ГосСОПКА.

Приказ вступает в силу с 30.01.2026.

26.12.2025 ФСБ России опубликован приказ от 23.12.2025 № 539 «Об утверждении Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».

ПРЕЗИДЕНТ И ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

09.10.2025 был опубликован проект постановления Правительства Российской Федерации «О государствен-

ной информационной системе противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий».

23.10.2025 было опубликовано распоряжение Президента Российской Федерации от 23.10.2025 № 409-рп «О подписании Конвенции Организации Объединённых Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определёнными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьёзным преступлениям».

05.11.2025 опубликован указ Президента Российской Федерации от 05.11.2025 № 815 «О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утверждённый Указом Президента Российской Федерации от 10.11.2018 № 648».

18.11.2025 в Государственную думу Российской Федерации был внесён Законопроект № 1071966-8 «О внесении изменений в статью 274 Уголовного кодекса Российской Федерации». Предлагаемые изменения предусматривают уточнение объективной стороны состава преступления в части корректировки определения общественно опасных последствий, а также внесение примечания, устанавливающего основания освобождения от уголовной ответственности в случае совершения преступления, предусмотренного частью третьей статьи 274 УК РФ.

29.11.2025 опубликовано постановление Правительства Российской Федерации от 28.11.2025 № 1931 «Об утверждении Правил формирования и ведения перечня доверенных российских программ для электронных вычислительных машин и баз данных».

29.12.2025 были опубликованы Федеральный закон от 29.12.2025 № 568-ФЗ «О внесении изменений в

Федеральный закон „Об информации, информационных технологиях и о защите информации“ и Федеральный закон от 29.12.2025 № 569-ФЗ „О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации“». Первый закон вступает в силу с 01.09.2026 и касается правового регулирования функционирования государственных информационных систем, второй – вводит возможность проверки возраста с помощью многофункционального сервиса обмена информацией (мессенджера МАХ), внесудебный механизм ограничения доступа в интернете к информации, содержащей предложения о розничной онлайн-продаже табачной и никотинсодержащей продукции, а также иной продукции, розничная онлайн-продажа которых ограничена или запрещена законодательством (с 01.03.2026), а также изменения в порядке регистрации доменных имён. С 01.09.2026 регистрацию доменных имён будут осуществлять российские юридические лица, включённые в перечни регистраторов доменных имён, за исключением отдельных случаев. Регистрация доменных имён будет проводиться только после прохождения лицом, на которое регистрируется доменное имя, идентификации посредством ЕСИА.

МИНЦИФРЫ РОССИИ

07.11.2025 опубликован приказ Минцифры России от 28.10.2025 № 982 «Об утверждении перечня нормативных правовых актов, содержащих обязательные требования, применение которых подлежит оценке в 2026 году, в сфере отношений, связанных с обработкой персональных данных».

03.12.2025 был опубликован приказ Минцифры России от 02.12.2025 № 1106 «Об утверждении Требований к обеспечению информационной безопасности в рамках предоставления облачных услуг посредством государственной единой облачной платформы».

19.12.2025 Минцифры России опубликован приказ от 16.12.2025 № 1174 «Об утверждении Требований к сетям и средствам связи собственников или иных владельцев технологических сетей связи, имеющих уникальный идентификатор совокупности средств связи и иных технических средств в информационно-телекоммуникационной сети „Интернет“, для обеспечения безопасности Российской Федерации по направлению деятельности федеральной службы безопасности».

ФСБ РОССИИ

18–19.11.2025 были опубликованы проекты ведомственных актов ФСБ России:

- ♦ О внесении изменений в «Положение о Национальном координационном центре по компьютерным инцидентам», утверждённое приказом ФСБ России от 24.07.2018 № 366;

- ♦ Об утверждении «Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и спо-

собах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

- ♦ Об утверждении «Порядка аккредитации центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и «Требований к центрам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к аккредитованным центрам».

28.11.2025 опубликован проект ведомственного акта «Об установлении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе к средствам, предназначенным для поиска признаков компьютерных атак».

ФСТЭК РОССИИ

27.10.2025 опубликовано информационное сообщение ФСТЭК России от 09.10.2025 № 240/24/5405 «О внесении изменений в Порядок проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации, утверждённый приказом ФСТЭК России от 01.12.2023 № 240». При сертификации процессов безопасной разработки программного обеспечения средств защиты информации теперь следует руководствоваться требованиями ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

29.10.2025 было опубликовано информационное сообщение ФСТЭК России от 16.10.2025 № 240/24/5531 «О внесении изменений в приказ ФСТЭК России от 02.06.2020 № 76 „Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий“». Исключена необходимость наличия сведений об аппаратных платформах средств защиты информации и их компонентах в едином реестре радиоэлектронной продукции.

29.10.2025 также опубликовано информационное сообщение ФСТЭК России от 22.10.2025 № 240/84/3451 «О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий». Изменилась типовая форма представления сведений о результатах присвоения объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

28.11.2025 ФСТЭК России опубликовал «Рекомендации по базовой настройке механизмов безопасности почтовых сервисов от атак, связанных с подменой отправителя (спуфинг-атак)».

05.12.2025 ФСТЭК России были опубликованы «Рекомендации по настройке механизмов безопасно-

сти почтового сервера, созданного с использованием программного обеспечения с открытым исходным кодом Ehim, от атак, связанных с подменой отправителя (спуфинг-атак)».

10.12.2025 ФСТЭК России опубликованы «Рекомендации по настройке механизмов безопасности почтового сервера, созданного с использованием программного обеспечения с открытым исходным кодом Postfix, от атак, связанных с подменой отправителя (спуфинг-атак)».

12.12.2025 ФСТЭК России опубликовал документ от 25.11.2025 «Методика анализа защищённости информационных систем».

16.12.2025 ФСТЭК России опубликовал проект национального стандарта ГОСТ Р «Защита информации. Защита информации от неправомерной передачи или распространения из информационных и автоматизированных систем. Общие положения». Проект направлен на противодействие утечке информации из программной среды информационных систем в результате действий пользователей, имеющих права доступа к защищаемой информации в этих системах, в том числе с применением специальных технических средств защиты от утечки (DLP-систем).

19.12.2025 ФСТЭК России опубликовал рекомендации по настройке механизмов безопасности почтового сервера Microsoft Exchange Server от атак, связанных с подменой отправителя (спуфинг-атак).

25.12.2025 ФСТЭК России опубликовал рекомендации по базовой настройке регистрации событий безопасности.

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

13.11.2025 Банк России опубликовал обзор отчётности об инцидентах информационной безопасности при переводе денежных средств за III квартал 2025 года.

13.11.2025 также был опубликован Приказ Банка России от 05.11.2025 № ОД-2506 «Об установлении признаков осуществления перевода денежных средств без добровольного согласия клиента и отмене приказа Банка России от 27.06.2024 № ОД-1027». С 01.01.2026 Банк России вводит учёт новых признаков перевода денежных средств без добровольного согласия клиента (или с согласия, полученного путём обмана или злоупотребления доверием). Признаки мошеннических переводов будут учитываться и при операциях с цифровым рублём.

24.11.2025 Банк России опубликовал проект Указания «О внесении изменений в Положение Банка России от 25.07.2022 № 802-П». Предлагается ввести следующие дополнительные требования по защите информации для участников платёжной системы об осуществлении деятельности по планированию, реализации, контролю и совершенствованию мер и мероприятий, направ-



ленных на реализацию требований, применяемых в отношении технологии обработки защищаемой информации, и к расчёту значений показателей оценки выполнения требований к мерам защиты информации в отношении технологии безопасной обработки защищаемой информации. Также предполагается предусмотреть возможность использования автоматизированного рабочего места обмена или собственных объектов информационной инфраструктуры (по решению участника обмена) для организации обмена с платёжной системой Банка России.

29.12.2025 Банком России опубликовано информационное письмо от 26.12.2025 № ИН-017-56/118. Техническим комитетом по стандартизации № 122 «Стандарты финансовых операций» одобрена новая редакция методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций». Документ обновлён, в том числе с учётом практики применения «ГОСТ Р 56939-2024. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования».

ОТРАСЛЕВЫЕ ДОКУМЕНТЫ

26.12.2025 утверждён ГОСТ Р 72484-2025 «Системы искусственного интеллекта в здравоохранении. Термины и определения. Классификация». Стандарт вступает в силу с 01.02.2026.

30.12.2025 были утверждены ГОСТ Р 72498-2025 «Системная инженерия. Системный анализ интероперабельности. Определение существенных угроз и условий» (вступает в силу с 01.02.2026) и ПНСТ 1041-2025 «Системы киберфизические. Умный дом. Требования к интерфейсам подключения оконечных устройств умного дома и их защита от сетевых атак» (действует с 30.06.2026 до 30.06.2029).

SECURITY VISION SPC

ФУНДАМЕНТ ЗРЕЛОЙ КИБЕРБЕЗОПАСНОСТИ



Роман ДУШКОВ
эксперт, Security Vision



Валерий ГОРБАЧЁВ
руководитель группы
внедрения систем мониторинга
АО «ДиалогНаука»

В современной корпоративной среде автоматизированное управление конфигурациями безопасности и контроль соответствия перестали быть исключительно вопросом выполнения требований регуляторов. Продукты класса SPC (Security Profile Compliance) превратились в фундаментальный элемент зрелой стратегии кибербезопасности.

Некорректные конфигурации ИТ-активов являются одним из наиболее распространённых и опасных векторов атак, открывающая злоумышленникам доступ к критически важным системам, а непрерывный и автоматизированный контроль за состоянием конфигураций становится стратегическим процессом проактивного снижения поверхности атаки и минимизации рисков.

ЦЕЛИ И ОСОБЕННОСТИ АРХИТЕКТУРЫ

Внедрение Security Vision SPC подразумевает централизацию функции контроля соответствия в рамках одномоментно GRC-подразделения, команды, отвечающей за автоматизацию процессов ИБ и директоров по информационной безопасности.

Модуль контроля параметров безопасности не является изолированным продуктом и представляет собой решение, которое наследует все сильные стороны базовой платформы Security Vision. Его польза проистекает из синергии с другими модулями: для управления активами и инвентаризацией (AM), уязвимостями (VM) со сканером (VS), инцидентами (SOAR) и SGRC. Эффективный контроль соответствия невозможен без полного, точного и постоянно актуализируемого реестра ИТ-активов: способность платформы обнаруживать, инвентаризировать и работать в разнообразных технических средах является её ключевой характеристикой (рис. 1).

Решение сочетает методы сканирования с использованием агентов и без них, а также проводит проверки как с использованием предварительно подготовленных УЗ, так и без них. Микросервисная архитектура позволяет организациям масштабировать отдельные компоненты (на-

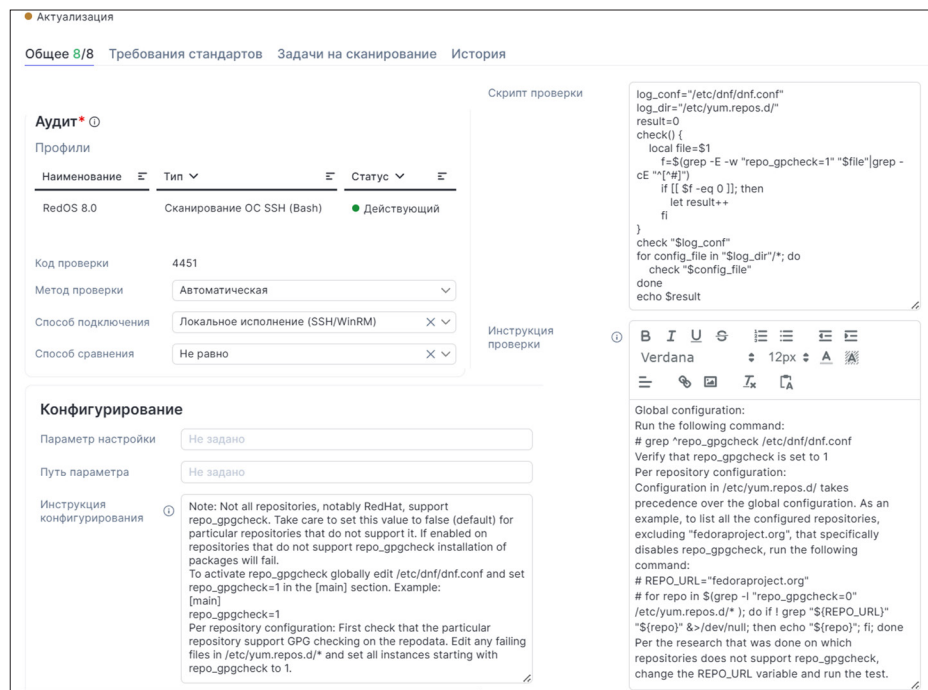


Рисунок 1. Настройки и автоматизация аудита конфигураций

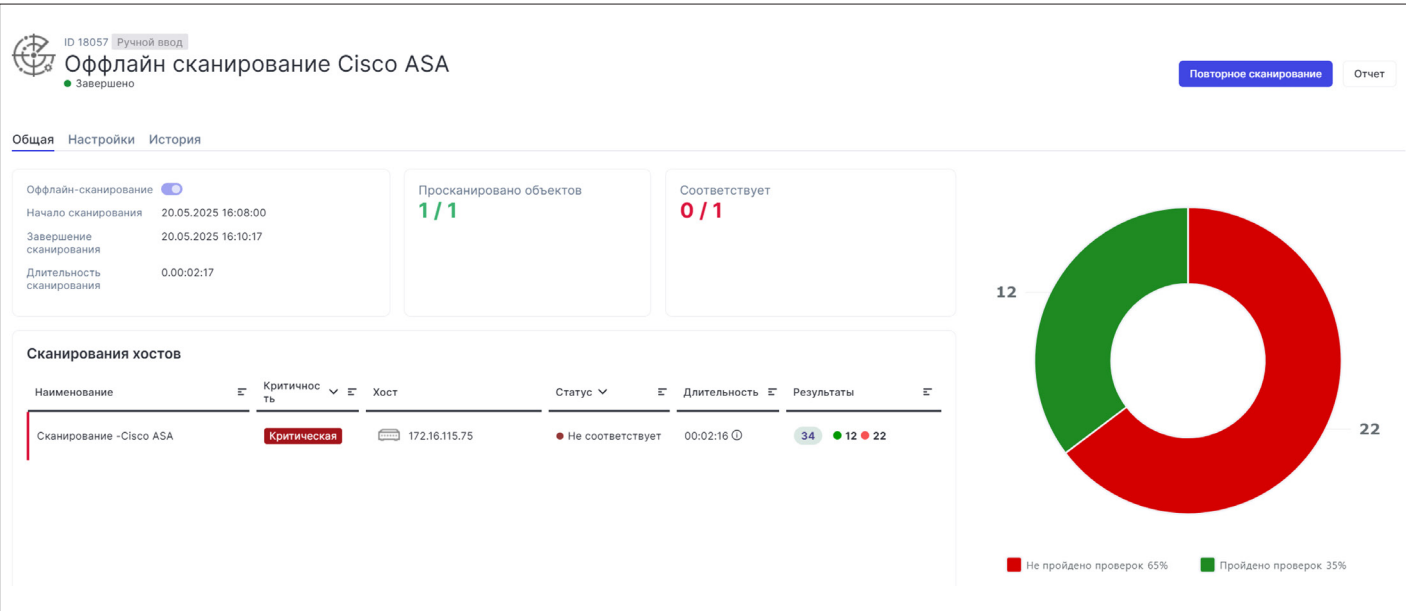


Рисунок 2. Результаты офлайн-сканирования

пример, сервис коннекторов для интеграции с внешними системами) по мере роста нагрузки и появления новых задач, что обеспечивает гибкость развёртывания и высокую отказоустойчивость.

ОСОБЕННОСТИ ПРОЦЕССА КОМПЛАЕНСА

Поскольку ни одна технология сканирования не может обеспечить 100% видимости данных, вендор-независимый подход Security Vision идеально подходит для компаний, где для обогащения данными применяются разрозненные системы от различных поставщиков. Low-code фреймворк-коннекторов позволяет агрегировать данные из внешних систем (служб каталогов, SCCM-, CMDB- и SIEM-систем, и других источников) вне зависимости от поставщика решения и без участия вендоров.

Офлайн-сканер позволяет определять степень соответствия параметров безопасности для любых сетей, включая применение в изолированных средах (рис. 2).

Автоматизация процесса, от обнаружения активов и технологических платформ до приведения к соответствию их настроек, позволяет освободить ресурсы аналитиков и ИТ-специалистов. В случае выявления несоответствия конфигураций активов эталонным значениям

значения при помощи коннекторов приводятся к заданным. Ведение профилей технологических платформ (например, операционных систем, СУБД, прикладного ПО), содержащих перечень релевантных проверок, можно проводить как вручную, так и автоматически по расписанию (рис. 3).

Security Vision SPC имеет встроенный движок управления бизнес-процессами (BPM) и позволяет создавать полностью кастомизированные рабочие процессы (для управления жизненным циклом активов, устранения несоответствий, обновления настроек и создания задач). Система может автоматически создавать задачи, на-

значать ответственных, контролировать SLA и интегрироваться с внешними системами Service Desk, такими как Jira, Naumen SD, Redmine и др.

Системы контроля соответствия регулярно (например, раз в сутки) сканируют хосты и сравнивают их текущую конфигурацию с эталонным «золотым образом».

Отдельным преимуществом является возможность самостоятельно собрать не только «золотой образ», но и требования, проверки, скрипты проверок с выполняемыми командами. Таким образом, сильно расширяются возможности кастомизации и подстройки под используемые в компании стандарты.

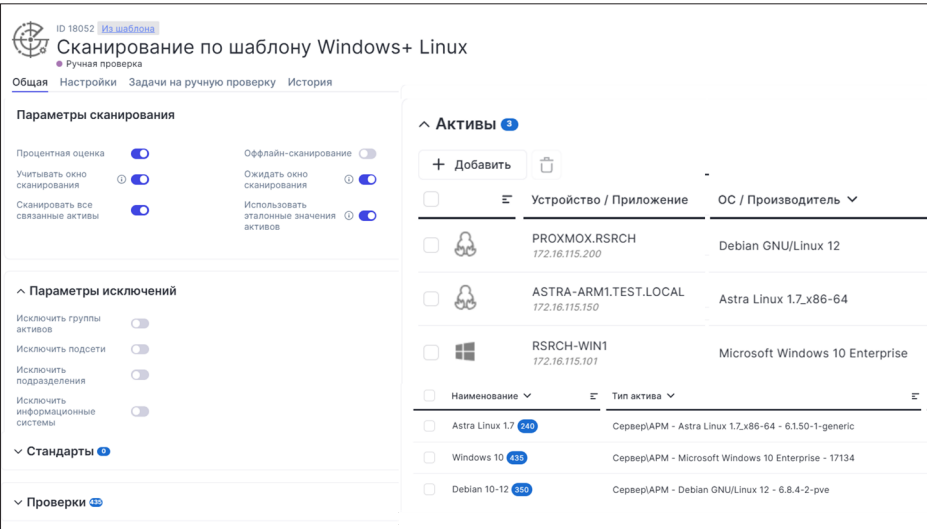


Рисунок 3. Гранулярные настройки контроля соответствия

РЕЗУЛЬТАТЫ И ВЛИЯНИЕ НА БИЗНЕС

Контроль конфигураций и соответствия профилям безопасности напрямую снижает поверхность атаки и повышает общую защищённость, делая системы более предсказуемыми, управляемыми и устойчивыми к взлому. Это достигается за счёт нескольких ключевых механизмов:

- ♦ устранение известных векторов атак (харденинг), приведение систем в соответствие с лучшими практиками безопасности (бенчмарками) и внутренними стандартами; этот процесс систематически закрывает распространённые лазейки;

- ♦ отключение ненужных служб и портов, потенциальных точек входа для злоумышленника: система находит и отмечает службы, которые не требуются для бизнес-функций, позволяя их отключить (например, если на веб-сервере не используется FTP, соответствующий порт (21) и служба должны быть отключены, что мгновенно убирает все известные уязвимости FTP-серверов из поля зрения атакующего до того, как он сможет их применить);

- ♦ проверка прав на выполнение системных команд или изменение кри-

тически важных файлов у обычных пользователей мешает горизонтальному перемещению по сети и повышению привилегий после первичного проникновения;

- ♦ неиспользуемое программное обеспечение (старые версии библиотек, тестовые утилиты) не обновляется, содержит уязвимости и может быть использовано для проникновения или повышения привилегий в системе. Функционал управления активами идентифицирует такое ПО для последующего (в т.ч. автоматического) удаления;

- ♦ выявление несоответствий парольной политике, мiskonфигураций и/или ошибок в различных файлах конфигов (для самых разных механизмов – от удалённого доступа и повышения привилегий до RAM и прочих);

- ♦ системы по умолчанию часто настроены на максимальную функциональность, а не на безопасность, поэтому контроль соответствия способен исправить сотни параметров: от отключения старых протоколов (SSL 3.0, TLS1.0) до установки корректных прав на системные файлы и каталоги.

Контроль соответствия профилям безопасности превращает реактив-

ный подход в проактивный, систематически устраняя слабые места и обеспечивая постоянную видимость реального состояния защищённости ИТ-инфраструктуры (рис. 4).

Любое отклонение (например, открытие нового порта, появление нового пользователя с правами администратора, изменение прав на файл) немедленно фиксируется и отправляется в виде оповещения команде безопасности. Это позволяет быстро обнаружить как случайные ошибочные изменения, так и вредоносную активность, значительно сокращая «окно», в течение которого система остаётся уязвимой.

ЗАКЛЮЧЕНИЕ

В будущем инструменты для работы с уязвимостями и конфигурациями будут включать в себя больше GRC-функций, а GRC-платформы – углублять свои технические возможности оценки. Выбор, сделанный организацией сегодня, определит её траекторию развития в этом меняющемся ландшафте. Он должен быть основан на глубоком понимании собственной организационной культуры, операционной зрелости и долгосрочной стратегии в области кибербезопасности.



Рисунок 4. Визуализация результатов для ресурсно-сервисной модели компании (выделенный контур)

ОБЛАЧНАЯ ЗАЩИТА ИЛИ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ?

КАК ПЕРЕСТАТЬ ВЫБИРАТЬ МЕЖДУ НИМИ



Юрий ГОРЯЧЕВ
менеджер
по продукту
компании
NGENIX

Экономика ведёт бизнес в облака. Высокая стоимость оборудования, сложность его обновления, дефицит квалифицированных специалистов и необходимость быстро запускать цифровые сервисы делают облачную модель привлекательной для одних компаний и

практически неизбежной для других. Однако для многих организаций, прежде всего из финансового сектора и других регулируемых отраслей, этот переход оказывается существенно сложнее.

ПОЧЕМУ ПУТЬ В ОБЛАКО ДЛЯ РЕГУЛИРУЕМЫХ КОМПАНИЙ СЛОЖНЕЕ

Для банков, финтех-компаний, страховых организаций, операторов персональных данных и участников платёжной инфраструктуры использование облаков невозможно рассматривать в отрыве от требований ФСТЭК, Банка России и платёжных систем.

Недостаточно просто формально соблюсти регуляторные требования — в текущих условиях используемые

технологии и средства защиты должны эффективно обеспечивать требуемый уровень безопасности. Тем временем, публичные веб-сайты, порталы и внешние API финансового сегмента сегодня постоянно подвергаются DDoS- и бот-атакам.

В результате компании вынуждены искать решения, которые одновременно выполняют задачи доступности и защиты веб-ресурсов и при этом не нарушают требования регуляторов. Соблюсти этот баланс не всегда легко.

ОСНОВНЫЕ ПОДХОДЫ К ЗАЩИТЕ ВЕБ-РЕСУРСОВ СЕГОДНЯ

На практике используется несколько подходов к защите веб-ресурсов от кибератак (см. таблицу 1).

	Построение DIY-решения Самостоятельная разработка ПАК/ПО, обеспечивающих защиту веб-ресурсов от DDoS-атак и ботов в составе оригинальной веб-инфраструктуры	Развертывание On-Prem решения Развертывание специализированных ПАК/ПО, обеспечивающих защиту веб-ресурсов от DDoS-атак и ботов в составе оригинальной веб-инфраструктуры	PaaS без раскрытия HTTP(S)-трафика Облачная услуга, позволяющая анализировать поступающий поток логов с оригинальной веб-инфраструктуры и формирующая списки нежелательных источников трафика для блокировки на оригинальной веб-инфраструктуре	PaaS с раскрытием HTTP(S)-трафика Облачная услуга, обеспечивающая обработку, анализ и блокировку нежелательного трафика на внешней инфраструктуре сервис-провайдера и экранирующая оригинальную веб-инфраструктуру
Капитальные затраты	Р Р Р Разработка ПО и закупка оборудования	Р Р Р Закупка специализированного оборудования	Р Р Р Закупка оборудования для интеграции с PaaS	О О О Отсутствует
Операционные затраты команды на поддержку	Р Р Р Разработка, поддержка и эксплуатация ПО и оборудования	О О О Поддержка и эксплуатация оборудования и ПО, за исключением обновления ПО	О О О Поддержка и эксплуатация оборудования, ПО и облачной услуги, обеспечивающей интеграцию с PaaS	О О О Эксплуатация облачной услуги
Затраты на аттестацию / периодическую аттестацию решения в составе ИС	Р Р Р Высокие, требуется полная перееаттестация ИС	Р Р Р Высокие, требуется полная перееаттестация ИС	О О О Решение не подлежит аттестации	О О О Аттестация в зоне ответственности PaaS-провайдера
Ответственность за работоспособность решения	Владелец веб-ресурса	Владелец веб-ресурса	Владелец веб-ресурса + PaaS-провайдер	PaaS-провайдер
Нагрузка на оригинальную веб-инфраструктуру	Р Р Р Вся нагрузка обслуживается оригинальной веб-инфраструктурой	Р Р Р Вся нагрузка обслуживается оригинальной веб-инфраструктурой	О О О Вся легитимная нагрузка, а также часть нелегитимной нагрузки обслуживается оригинальной веб-инфраструктурой	О О О Оригинальная веб-инфраструктура обрабатывает только часть легитимной нагрузки, нелегитимная нагрузка и легитимные запросы к кэшируемым данным обрабатываются в облаке
Масштабируемость и производительность решения	Р О О Веб-ресурс становится недоступен, если легитимная и/или нелегитимная нагрузка превысила ёмкость системы	Р О О Веб-ресурс становится недоступен, если легитимная и/или нелегитимная нагрузка превысила ёмкость системы	О О О Веб-ресурс становится недоступен, если легитимная нагрузка превысила ёмкость системы и/или оригинальная веб-инфраструктура не смогла передать поток данных для анализа	О О О Эластичное облачное решение с большим запасом ёмкости, автоматически масштабируемое под всплески легитимного и/или нелегитимного трафика
Эффективность решения	Р О О Высокий риск ложноположительных срабатываний	О О О Зависит от актуальной версии ПО	О О О Высокая задержка в принятии решения и ограниченность механизмов валидации	О О О Анализ запросов по множеству факторов и критериев с возможностью настройки дополнительных механизмов валидации
Time-to-market	Р О О Разработка и внедрение требует больших ресурсов	Р О О Нужна установка оборудования	О О О Сложная интеграция с PaaS-провайдером	О О О Простая интеграция через CNAME или A-записи в DNS

Таблица 1. Варианты построения защиты веб-ресурса от кибератак

Самый консервативный из них — построение собственной инфраструктуры и реализация на ней собственных мер защиты. Такой путь обеспечивает максимальный контроль, но требует значительных капитальных вложений, редких компетенций, длительных сроков внедрения, проверки соответствия, аттестации или переаттестации всей информационной системы. Для многих компаний это означает годы работы и десятки миллионов рублей затрат.

Близкий по логике вариант — развёртывание специализированных on-premise-решений. Он снижает нагрузку на команду разработки, но сохраняет высокие расходы на оборудование, эксплуатацию и обновление, а также полностью оставляет на владельце веб-ресурса ответственность за его работоспособность и соответствие требованиям. Масштабируемость таких решений по-прежнему ограничена физическими ресурсами инфраструктуры.

Еще один вариант — использование облачных сервисов защиты без раскрытия HTTP(S)-трафика. Формально он выглядит как компромисс между безопасностью и регуляторными требованиями, однако на практике имеет серьёзные ограничения. Анализ запросов строится на логах и метаданных, что приводит к задержкам в реакции на атаки, риску ложноположительных блокировок и высокой нагрузке на серверы оригинации в пиковые моменты (в начале атак).

С технической точки зрения наиболее эффективной считается облачная защита с расшифровкой и анализом HTTP(S)-трафика на стороне провайдера. Именно этот подход используют мировые лидеры рынка, поскольку он позволяет противостоять атакам на уровне приложений, снижать нагрузку на оригинальную инфраструктуру и автоматически масштабироваться под любые всплески трафика. Долгое время для российских компаний из регулируемых отраслей этот вариант был фактически закрыт из-за отсутствия провайдеров с аттестованной облачной инфраструктурой.

АТТЕСТОВАННОЕ ПУБЛИЧНОЕ ОБЛАКО КАК ИНФРАСТРУКТУРНЫЙ КОМПОНЕНТ

Пойдя по пути международных провайдеров, таких как Cloudflare и Akamai, NGENIX разработал аттестованное распределённое публичное облако на базе распределённой платформы с интегрированными сервисами защиты веб-ресурсов.

Платформа соответствует требованиям российских регуляторов и отраслевых стандартов: ФСТЭК России — в части защиты персональных данных, Банка России — для финансовых организаций, а также стандарту PCI DSS, обязательному для сервис-провайдеров, работающих с платёжной информацией. Это даёт заказчикам легальную основу для использования облачной защиты с полноценным анализом трафика на

узлах провайдера без нарушения регуляторных норм.

Для финансовых организаций (банков, микрофинансовых организаций (МФО), брокеров, страховых компаний) использование такого продукта означает выполнение требований Банка России по ГОСТ Р 57580 с существенным упрощением процесса аттестации. Для платёжных сервисов и интернет-магазинов — соответствие PCI DSS. Для операторов персональных данных — выполнение требований приказа ФСТЭК № 21 и возможность использовать облачную инфраструктуру в рамках требований 152-ФЗ по защите и обработке персональных данных.

АРХИТЕКТУРА И ПРИНЦИПЫ БЕЗОПАСНОСТИ РЕШЕНИЯ

Аттестованное публичное облако NGENIX построено на принципе «встроенной безопасности», при котором требования информационной безопасности учитываются на этапе проектирования. Инфраструктура размещена в трёх независимых аттестованных дата-центрах уровня надёжности Tier 3, что обеспечивает отказоустойчивость и высокую доступность критичных сервисов.

Взаимодействие между узлами платформы защищено ГОСТ-шифрованием с использованием сертифицированных аппаратных средств защиты. Многоуровневая система безопасности включает средства обнаружения и предотвращения вторжений (IDS/IPS), а также централизованный сбор и анализ событий в SIEM. Такая архитектура позволяет выполнять полноценный анализ HTTPS-трафика в облаке без нарушения требований регуляторов.

Использование аттестованного публичного облака позволяет защищать веб-ресурсы от DDoS-атак на сетевом и прикладном уровнях, а также от автоматизированного трафика (ботов). Также оно обеспечивает отказоустойчивость и защиту DNS и демпфирует пиковые нагрузки с помощью CDN. При этом заказчик получает готовую аттестованную часть ИТ-среды, которую можно учитывать при построении

Аттестованное публичное облако NGENIX построено на принципе «встроенной безопасности», при котором требования информационной безопасности учитываются на этапе проектирования, а инфраструктура размещена в трёх независимых аттестованных дата-центрах уровня надёжности Tier 3

собственной защищённой информационной системы.

Важно отметить, что речь идёт именно об аттестованном инфраструктурном компоненте, а не о подтверждении соответствия всей информационной системы заказчика.

ГДЕ ПРОХОДИТ ГРАНИЦА ОТВЕТСТВЕННОСТИ

Не все организации понимают, что использование аттестованного публичного облака не снимает с компании обязанности обеспечивать соответствие своей информационной системы требованиям регуляторов. Ответственность за приложения, бизнес-процессы и обработку данных остаётся на стороне заказчика, который отвечает за соответствие перед регулятором, платёжной системой или банком-эквайером.

Со стороны провайдера ответственность ограничена инфраструктурным уровнем. Например, в случае NGENIX инфраструктура и сервисы

аттестованного распределённого публичного облака соответствуют требованиям ФСТЭК России (приказ № 21, уровень защищённости УЗ-2), стандарту Банка России ГОСТ Р 57580.1-2017 и требованиям PCI DSS, предъявляемым к сервис-провайдерам. Аттестаты подтверждают, что используемый облачный компонент не нарушает установленных требований и может легитимно применяться в составе защищённой информационной системы заказчика.

Практическая ценность такого подхода заключается в том, что компания получает критически важный аттестованный компонент для защиты веб-ресурсов. Используя его, заказчик снижает регуляторные риски на уровне инфраструктуры, избегает капитальных затрат на создание и аттестацию собственной платформы и существенно сокращает сроки собственного подтверждения соответствия – по разным оценкам, на 6–12 месяцев. Именно в этом состо-

ит ценность аттестованного облака: не в формальном «соответствии», а в снижении издержек и упрощении выполнения обязательств перед регуляторами.

ВЫВОД

Рост потребления облачных сервисов российскими организациями в текущей макроэкономической ситуации неизбежен, и для регулируемых отраслей ключевым становится не вопрос «использовать ли облака», а вопрос доверия провайдеру и одновременно – соблюдение высоких стандартов безопасности. Аттестованные публичные облака формируют новый подход к защите веб-ресурсов, позволяя сочетать экономические преимущества облачной модели с соблюдением регуляторных требований. Опыт NGENIX показывает, что такой баланс сегодня достижим и может стать основой для дальнейшего развития облачных сервисов информационной безопасности в России.

ОРГАНИЗАТОР



Банк России

УРАЛЬСКИЙ ФОРУМ

КИБЕРБЕЗОПАСНОСТЬ В ФИНАНСАХ



Екатеринбург
18–20 февраля 2026

СТАНЬТЕ ЧАСТЬЮ
ПРОФЕССИОНАЛЬНОГО
СООБЩЕСТВА, ОПРЕДЕЛЯЮЩЕГО
СТАНДАРТЫ БЕЗОПАСНОСТИ

ИТОГИ ИСПЫТАНИЙ СТАТИЧЕСКИХ АНАЛИЗАТОРОВ ИСХОДНОГО КОДА ПРИ ОРГАНИЗАЦИОННОЙ И МЕТОДИЧЕСКОЙ ПОДДЕРЖКЕ ФСТЭК РОССИИ



Дмитрий ПОНОМАРЕВ

заместитель генерального директора — директор департамента внедрения и развития практик РБПО ООО НТЦ «Фобос-НТ», сотрудник ИСП РАН, преподаватель МГТУ им. Н.Э.Баумана

Одним из ключевых событий Открытой конференции Института системного программирования РАН им. В. П. Иванникова, прошедшей 9–10 декабря 2025 года, стало подведение итогов испытаний статических анализаторов, организованных при поддержке ФСТЭК России. В 2025 г. коллективы-участники испытаний и автор этой статьи посвятили организации и проведению испытаний значимую часть своего рабочего и личного времени. По итогам были получены интереснейшие и важные результаты, и одновременно с этим стало очевидно — мы только в начале пути. Приобретённый опыт позволит внести необходимые улучшения в ГОСТ Р 71207–2024, доработать тестовую базу и методологию испытаний, подойти к организации следующего цикла испытаний с существенно более точной оценкой ресурсозатрат. Наиболее подробную информацию о задачах и целях, ходе и результатах испытаний, с «человеческими» комментариями их непосредственных участников, вы можете получить, ознакомившись с «первоисточником» — видеозаписью подведения итогов на сайте Открытой конференции [1].

Дальнейшее развитие системы испытаний статических анализаторов (далее — СА) будет освещаться на портале РБПО.рф [2].

ОБОБЩЁННЫЙ ОПЫТ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ИСПЫТАНИЙ

Вместо предисловия важно отметить, что организация и модерация испытаний явились для меня личным вызовом, потребовавшим существенных затрат времени и нервов, в том числе на принятие решений в ситуациях, когда идеального решения не

существует, и от практически любого принятого решения обязательно останутся недовольные. Тем не менее итоги испытаний признаны успешными и полезными, работа будет продолжена. Поэтому я хочу выразить искреннюю признательность всем, принявшим участие в планировании, организации, проведении и всестороннем обеспечении испытаний, и особенно — лично Д. Н. Шевцову и И. С. Гефнер (ФСТЭК России), А. А. Белеванцеву (ИСП РАН), А. В. Кузнецову и А. И. Буркэ (НТЦ Фобос-НТ / ИСП РАН), Е. А. Погорелко (МГТУ им. Н.Э.Баумана) и Н. А. Костригину (Базальт СПО) — порой нам даже было весело (рис. 1).

Далее представлены наиболее значимые тезисы, описывающие полученный опыт:

1. Задуманный объём испытаний существенно превысил возможности коллективов по формированию комплекта тестов и последующей оценке и кросс-верификации результатов работы инструментов СА.



Рисунок 1. Порой нам даже было весело

2. Необходимо существенно повысить автоматизацию выполнения анализа и оценки результатов инструментов, что требует выработки более строгих критериев и правил (стандарта) формирования базы тестов.

3. Важно фиксировать все обсуждения и принятые решения в протоколах — особенно в отношении тех решений, которые теоретически могут повлиять на подчёркивание тех или иных сильных (и в особенности — слабых) сторон инструментов.

4. Добровольный формат участия в испытаниях предполагает нестабильную и не в полной мере прогнозируемую результативность работы различных групп участников. Получение официального подтверждения от организаций, принявших решение выступить в роли экспертов, оценивающих результаты работы инструментов СА, о выделении соответствующих людских ресурсов, представляется правильным для планирования дальнейших работ.

5. Использование в качестве тестовой базы исходного кода программных компонентов с открытым исходным кодом требует филигранной точности в определении числа и объёма кодовой базы компонентов. Слишком большое число срабатываний инструментов СА на выбранной для испытаний очевидно избыточной кодовой базе не позволило выполнить разметку и кросс-верификацию срабатываний в объёме, позволяющем считать данную выборку репрезентативной. По этой причине результаты разметки открытого кода не вошли в итоговую оценочную формулу.

Тем не менее определённая польза от данной активности была получена в любом случае. Помимо того, что ряд коллективов в ходе разметки выявил некоторые недостатки в своих инструментах СА, коллеги ИСП РАН самостоятельно выполнили «вдумчивую разметку» всего объёма срабатываний детекторов, соответствующих категории ГОСТ (рис. 2).

Результаты данной разметки представлены на портале Центра исследований безопасности системного ПО [6] и могут быть использованы в качестве «эталона» при сравнительном анализе в ходе выбора инструмента СА.

		Всего срабатываний	True Positive	TP без Won't fix	False Positive
C/C++	nginx	50	76,0%	30,0%	24,0%
	unbound	151	64,2%	41,1%	35,8%
Java	guava	220	93,2%	12,3%	6,8%
	netty	440	94,8%	7,3%	5,2%
	spring-framework	32	50,0%	46,9%	50,0%
C#	FluentValidation	20	100,0%	10,0%	0,0%
	SharpZipLib	349	85,7%	12,3%	14,3%
	SignalR	866	67,3%	29,8%	32,7%
Go	etcd	187	83,4%	36,9%	16,6%
	minio	953	96,3%	8,8%	3,7%
	nats-server	99	85,9%	69,7%	14,1%

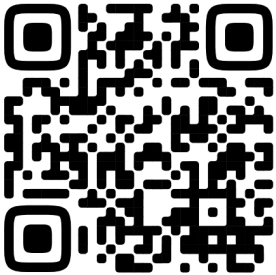


Рисунок 2. Результаты данной разметки представлены на портале Центра исследований безопасности системного ПО

6. ГОСТ Р 71207–2024 «Статический анализ исходного кода» требует внесения ряда доработок и уточнений, в том числе в терминах и определениях, для устранения неоднозначностей трактовок.

7. Необходимо выполнить более точный маппинг детекторов, реализованных инструментами СА, на методы анализа и типы ошибок, заявленные в ГОСТ. Эта кропотливая, но необходимая работа позволит повысить доверие к результатам последующих циклов испытаний за счёт минимизации коллизий срабатывания «не того детектора» в «том месте» кода, где заложена ошибка.

8. Необходимо точно и однозначно определить в методологии оценки перечни методов анализа, свойств инструментов и типов подлежащих обнаружению ошибок, подлежащие оценке в ходе испытаний.

9. Штатные особенности работы ряда инструментов анализа должны получить оценку «баг или фича» с целью либо верного учета данных особенностей при оценке результатов испытаний, либо — доработки инструментов до стандартного для методологии испытаний уровня возможностей.

10. Необходимо выработать и зафиксировать в ГОСТ единый, стандартизованный формат SARIF, который не только будет существенно способствовать повышению автоматизации последующих циклов испытаний, но и позволит стандартизовать обмен информацией с Центром исследований безопасности системного ПО в ходе выполнения сертификационных испытаний на соответствие требованиям ФСТЭК России.

11. Необходимо развивать подход, предполагающий создание комплексных тестов, позволяющих проверить корректность работы инструмента СА не только на простых атомарных тестах, но и на кодовой базе, по своей сложности сопоставимой с зубодробительными конструкциями и сложнейшими контекстами, порой встречающимися в реальном коде.

РЕЗУЛЬТАТЫ ИСПЫТАНИЙ

Данный раздел практически полностью состоит из слайдов с итоговыми количественными оценками (выборочно), без каких-либо пояснений, поскольку полноценный контекст их формирования слишком объёмен для текстового представления в рамках одной статьи. Всех желающих разобраться подробнее с принципами подсчёта результатов, а также ознакомиться со всем множеством результатов, я вновь приглашаю ознакомиться с материалами по ссылкам [1] и [4].

Зафиксирую единственный принципиально важный для восприятия результатов тезис-предупреждение — приведённые далее оценки следует трактовать в качестве приблизительных, в силу:

- ◆ неоднозначности трактовки результатов прохождения конкретными инструментами некоторых конкретных тестов;
- ◆ неполного выполнения процедуры разметки и кросс-верификации.

Для предоставленных цифр доверительный интервал оценивается в 7%, за исключением особо обозначенных случаев. Вся разметка выполнялась публично и была доступна для всех участников испытаний, все спор-

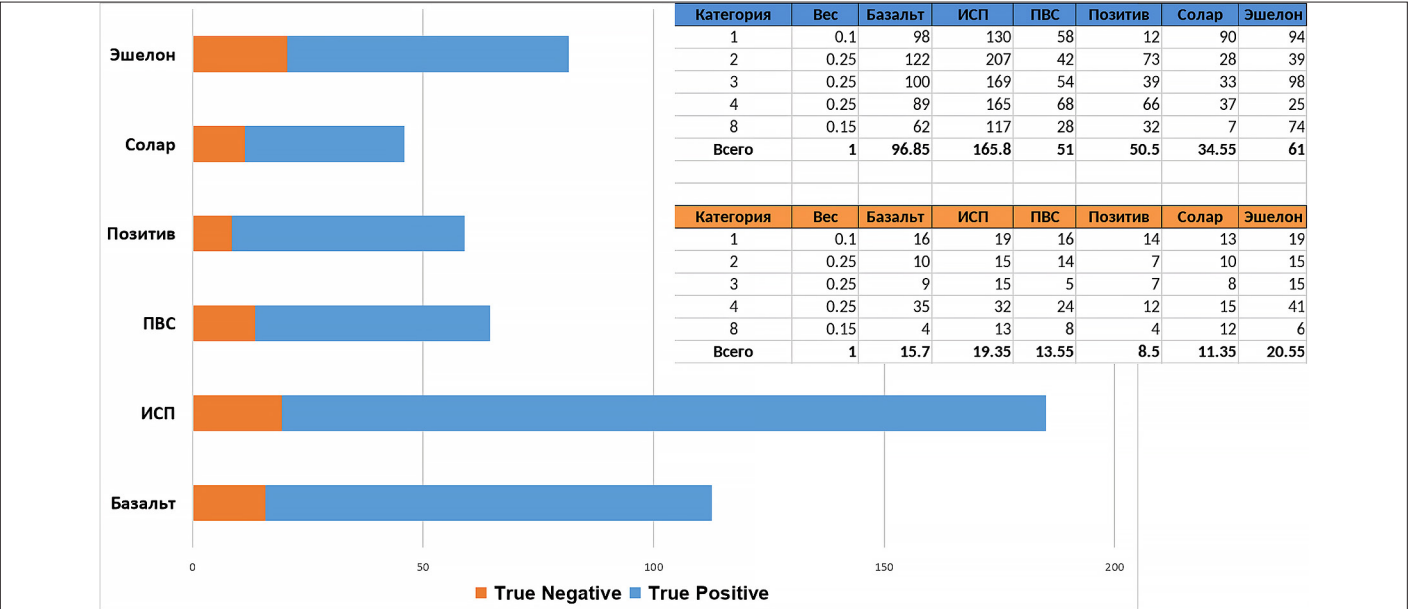


Рисунок 3. Результаты по основной формуле для языка программирования (ЯП) Си/Си++

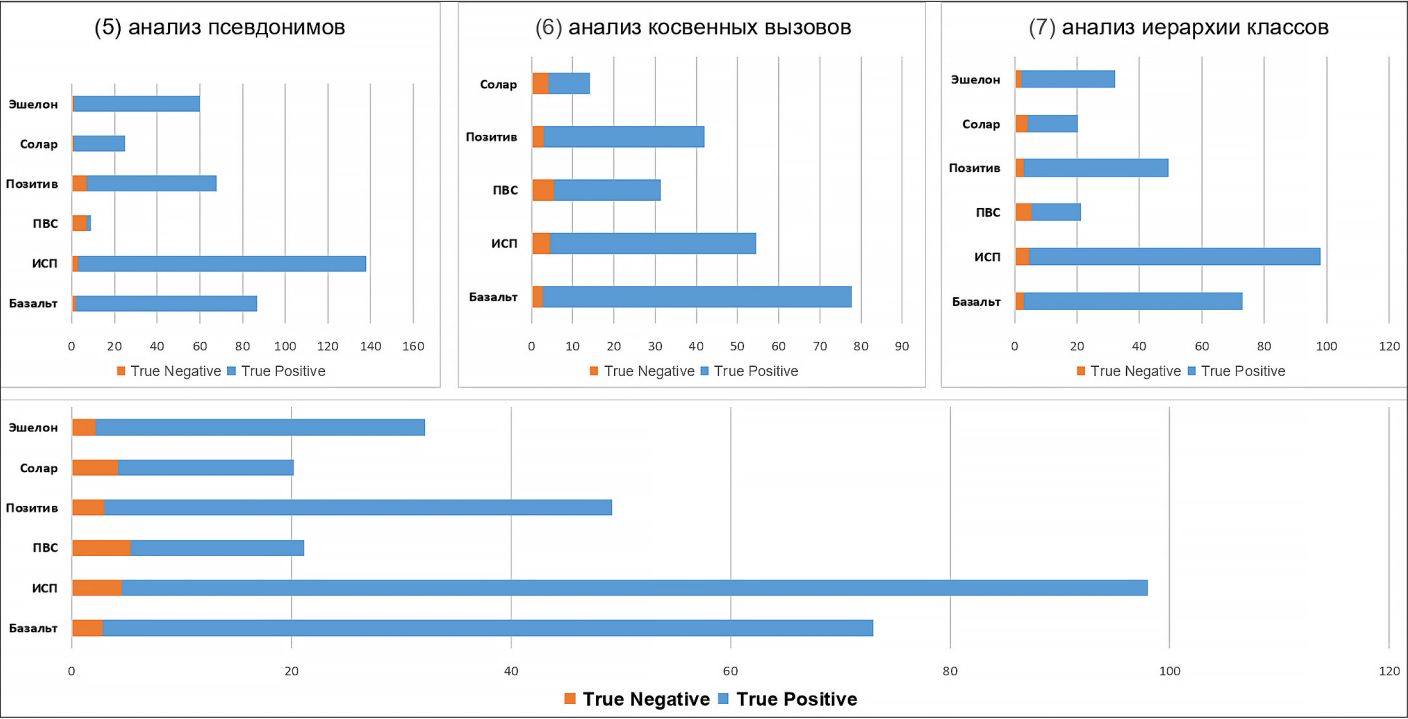


Рисунок 4. Результаты по дополнительной формуле для ЯП Си/Си++

ные вопросы разбирались участниками испытаний публично (рис. 3–6). В теории на рис. 6 показано заявленное участниками испытаний число срабатываний детекторов по ГОСТ. На практике:

- ◆ не все инструменты имеют механизмы фильтрации по типам детекторов;
- ◆ не все разработчики качественно отделили детекторы out-of-score от ГОСТ;

- ◆ некоторые инструменты действительно выдают очень много срабатываний.

ПЛАНЫ ПО ПОДГОТОВКЕ И ПРОВЕДЕНИЮ СЛЕДУЮЩЕГО ЦИКЛА ИСПЫТАНИЙ

Дальнейшие планы, озвученные И. С. Гефнер в ходе Открытой конференции, включают в себя:

- ◆ доработку и уточнение ГОСТ Р 71207-2024 «Статический анализ исходного кода»;
- ◆ доработку методологии испытаний и комплекта тестов с приоритетом создания «сложных», комплексных тестов, позволяющих испытывать инструменты в условиях, приближенных к «боевым»;
- ◆ разработку и стандартизацию формата представления результатов

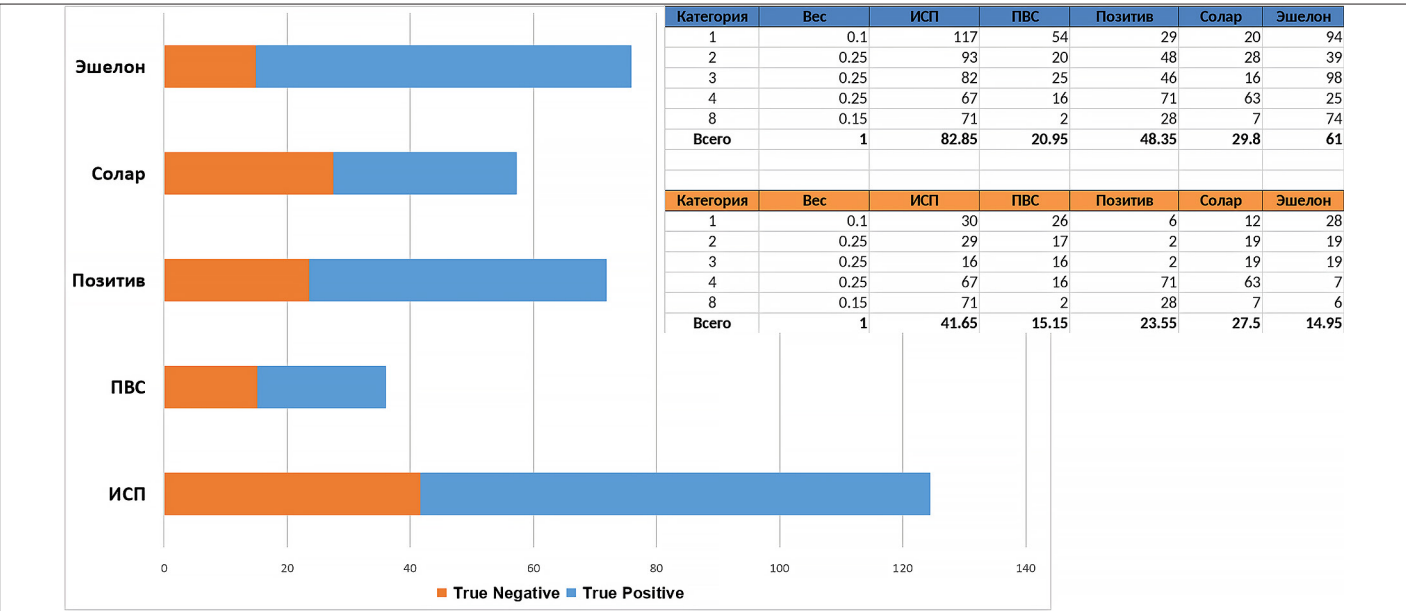


Рисунок 5. Результаты по основной формуле для ЯП Java

Пакет	ИСП РАН	Эшелон	Солар	ПВС	Позитив	Базальт
Cpython (C/C++)	414	88	813	2655	4882	3318
nginx (C/C++)	54	208	147	70	373	320
unbound (C/C++)	151	222	0	257	613	498
guava (Java)	224	317	3858	156	5519	0
netty (Java)	462	321	150491	144	61896	0
spring-framework (Java)	49	859	15078	353	1213	0
nats-server (Go)	104	25	24	0	2102	0
minio (Go)	994	58	221	0	724	0
etcd (Go)	198	22	3407	0	99	0
webpack (Go)	0	0	633	0	334	0
react (JavaScript)	6	0	1791	0	1	0
axios (JavaScript)	0	0	289	0	3	0
SharpZipLib (C#)	349	3	567	60	3553	0
SignalR (C#)	866	30	581	114	200	0
FluentValidation (C#)	20	0	1	2	551	0
Django (Python)	15	562	117	0	171	0
celery (Python)	3	61	2068	0	158	0
fastapi (Python)	0	103	1454	0	26	0

Рисунок 6. Общее число срабатываний детекторов для различных инструментов при анализе открытых компонентов

статического анализа (по аналогии с форматом SARIF);

♦ выработку механизма поддержки и развития репозитория комплекта тестов (действующий репозиторий [7] создан и поддерживается коллективом Базальт СПО),

♦ и, главное, подготовку и проведение следующего цикла испытаний в 2027 году.

ВМЕСТО ВЫВОДОВ.
ЛИЧНАЯ ПОЗИЦИЯ
МОДЕРАТОРА

Стратегической целью испытаний СА является создание и улучшение усло-

вий для развития отечественной научной-инженерной и производственной культуры создания сложных инструментов анализа.

Желания «перекрасить» и продавать открытый или даже проприетарный иностранный инструмент, либо взять опенсорс «as is» и, не вкладываясь в его развитие, получить коммерческий результат, понятны с тактической точки зрения конкретного бизнеса.

Но стратегический негативный эффект от таких действий для отрасли и государства противоречит поставленной Президентом РФ цели

достижения технологической независимости.

Испытания СА должны способствовать развитию и конкуренции отечественных школ создания инструментов СА и усложнять рыночную деятельность в указанных выше случаях – разумеется, за исключением случаев, когда открытый инструмент СА «из коробки» существенно лучше платного.

Поэтому я искренне рассчитываю, что органы по сертификации, аккредитованные в области сертификации процессов РБПО, будут опираться на методологию и результаты испытаний, в качестве минимально приемлемой, при оценке реализации процесса № 10 «Статический анализ исходного кода» (ГОСТ Р 56939–2024) разработчиками программного обеспечения и, в особенности, средств защиты информации.

ИСТОЧНИКИ

[1] <https://www.isprasopen.ru/>
Секция «Разработка безопасного ПО: качество, доверие, сообщество»
[2] <https://p6no.pf/news/rbpo-isprasopen-2025>
[3] <https://ib-bank.ru/rbpos>
[4] https://t.me/sdl_community/9420
[5] https://t.me/sdl_community/7859
[6] <https://clck.ru/3RSsMi>
[7] <https://altlinux.space/rbpo-community>

ЧТО НОВОГО В SVACE



Андрей БЕЛЕВАНЦЕВ

руководитель направления анализа и оптимизации программ ИСП РАН, доктор физико-математических наук, член-корреспондент РАН

Прошедший год для развития нашего статического анализатора Svace оказался очень продуктивным. Прежде всего хочется отметить прошедшие испытания статических анализаторов под эгидой ФСТЭК России и поблагодарить организаторов, площадку – МГТУ им. Н. Э. Баумана и отдельно кафедру ИУ10, коллег-вендоров, принявших участие. Для нас испытания стали поистине событием года, источником бесценного опыта, выразившегося в подготовке тестов анализаторов и изучении тестов, сделанных коллегами. Удалось увидеть множество деталей, которые раньше не всегда были сделаны на должном уровне. При этом надёжная основа в виде качественного масштабируемого межпроцедурного анализа, системы перехвата сборки, механизмов чувствительности к путям выполнения и других необходимых алгоритмов позволили Svace показать лучшие – с существенным отрывом – результаты для языков C/C++ и Java, полностью соответствующие ГОСТ Р 71207-2024.

Главное, на наш взгляд, что от испытаний выиграли все – организаторы, получившие обратные связи от сообщества вендоров анализаторов; сами вендоры, лучше узнавшие сильные и слабые стороны своих инструментов и обменявшиеся опытом с коллегами; пользователи, увидевшие объективную расстановку сил на рынке анализаторов и получившие более качественные инструменты.

Весь опыт, который мы вобрали в ходе испытаний, вошёл в последний релиз Svace 5.0. Помимо многочисленных улучшений анализа, мы отдельно выделили категорию детекторов, обнаруживающих критические по ГОСТ ошибки. Будем оперативно обновлять эту категорию по мере того, как будет дорабатываться и сам ГОСТ.

Отметим несколько важных новшеств анализа. Из новых языков Svace теперь поддерживает анализ программ на Lua, пока легковесный – на уровне универсального синтаксического дерева. Будем развивать его вместе с анализами других динамических языков – Python и JavaScript.

Продолжает развиваться интерфейс SvaceAPI для создания пользовательских детекторов. Его очень удобно использовать для поиска специфических ошибок, затрагивающих неизвестные анализу библиотеки или связанных с нарушением правил использования критических для безопасности компонент. При этом задействуется вся мощь основного движка анализа Svace. Мы сами использовали SvaceAPI для создания ряда специфичных детекторов для ГОСТ-ошибок и приглашаем пользователей активно его применять. Ваши обратные связи помогут нам развивать интерфейс в полезных для всех направлениях.

Серьёзно улучшен сервер удалённого анализа, позволяющий теперь работать с клиентами разных версий и конфигурировать различные дистрибутивы, гибко управляя пулом агентов анализа. Эта часть Svace востребована в крупных компаниях,

которые могут единообразно настраивать анализ для различных подразделений с учётом их специфики.

Появилось два новых режима анализа. Анализ «сверху вниз» позволяет находить ошибки, для которых естественно распространение информации от источников к приёмникам. Его комбинация с привычным анализом «снизу вверх» позволяет увеличить полноту (количество находимых ошибок) за счёт большего времени работы. Покомпонентный анализ позволяет анализировать независимые подпрограммы большой программной системы отдельно, сокращая потребление памяти; при этом выделение независимых модулей выполняется автоматически по данным графа компоновки – зависимые компоненты по-прежнему будут анализироваться вместе.

Активно развивается направление по применению в Svace алгоритмов машинного обучения. Уже можно попробовать ИИ-ассистенты, которые предсказывают истинность срабатывания по данным метрик программы (собранным Svace) и изнутри сервера работы с результатами Svacer. В будущем интерфейсы Svacer работы с ИИ-ассистентами будут позволять подключать различные модели, которые исследуются в ИСП РАН, в том числе разрабатываемую в настоящий момент функциональность предсказания истинности и объяснения предупреждений через специализированные большие языковые модели.

Следите за нашими обновлениями!

**Инструменты
анализа
ИСП РАН**



Блог Svace



УСКОРЕНИЕ И ТОЧНОСТЬ

КАК МЕНЯЮТСЯ SAST-ИНСТРУМЕНТЫ В ЭПОХУ БЫСТРОЙ РАЗРАБОТКИ



Антон ПРУСАК
руководитель
продукта
AppSec.Wave

Ускорение – важный тренд мировой разработки ПО, в том числе – российской. Объем российского ИТ-рынка, по прогнозам экспертов, в 2026 превысит 4,5 триллиона рублей. В условиях непрерывной интеграции и DevOps современным разработчикам ПО критически важно, чтобы инструменты статического анализа кода (SAST) отвечали требованиям бизнеса по скорости и удобству. Запрос 2026, пожалуй, можно обозначить как: еще быстрее и разложить по полочкам.

На первый план у ИБ-команд компаний-разработчиков вышли высокая скорость анализа, минимальное количество ложных срабатываний и интуитивно понятный процесс триажа. Однако сегодняшние запросы рынка идут дальше: ключевым ста-

новится требование к гибкости и адаптивности платформы. Именно эта потребность легла в основу амбициозной задачи по созданию для российского ИТ-сектора универсального SAST-решения, которое не только находит уязвимости, а органично встраивается в рабочий процесс, позволяя бесшовно интегрировать безопасность в цикл разработки. Совмещая скорость, качество и адаптивность, SAST-решения становятся естественной частью рабочего процесса, обеспечивая безопасность без потери темпа разработки.

Основной тренд последних полутора лет – активное внедрение в разработку генерируемого ИИ-кода. Массовое распространение вайб-кодинга требует серьезного ускорения и усиления кибербезопасности.

AppSec Solutions для этой задачи разработал универсальный SAST – AppSec.Wave, отличительной чертой которого является высокая скорость сканирования. Основные векторы развития AppSec.Wave – скорость анализа, качество и удобство триажа уязвимостей.

AppSec.Wave поддерживает множество языков программирования, включая JavaScript, Python, Go, C++, Java, PHP, Ruby, C# и другие. В 2026 планируется добавить и язык 1C, ши-

роко используемый отечественными компаниями.

Современная архитектура и агентская модель предполагают полный функционал и добавление любого количества агентов, это удобно для любого размера бизнеса. Менеджмент может подключить к процессу разработки 30+ команд, которым будет вполне комфортно работать совместно. Помимо этого, анализатор дает возможность добавлять кастомные правила, позволяя ИБ-команде настраивать SAST с учетом потребностей бизнеса. Система анализирует код не только по шаблонам, как опенсорс-решения статического анализа, но и использует усовершенствованный taint-анализ, который позволяет определить источник, например, SQL-инъекции, и проследить все части системы, на которые она повлияла.. Команда разработчиков будет работать над качеством анализа и прохождением всего AST-дерева для полноценного поиска уязвимостей. Также AppSec.Wave позволяет отключать предустановленные правила из комплекта поставки на усмотрение пользователя, а заниматься отладкой новых правил можно в самом сканере, не заполняя очередь реальных проектов. Также поддерживается импорт отчетов и правил из других сканеров, что важно при переходе с импортных SAST-инструментов на российское ПО.

Инструмент позволяет удобно группировать отчеты, а также импортировать их из сканеров других решений, чтобы собирать данные по уязвимостям воедино. История изменений при этом сохраняется. Среди функций: поддержка инкрементального анализа, групповая обработка результатов и интеграция с task-трекерами. Сейчас разработчики AppSec.Wave работают над возможностью интеграции инструмента с MCP-сервером, который позволит сканировать код с помощью языковых моделей.

Ключевой фактор, который влияет на скорость разработки — распространение вайб-кодинга. По оценкам экспертов, от 60 до 80% разрабатываемого в России ПО сгенерировано искусственным интеллектом. К примеру, совместное исследование IT_ONE, Фонда «Сколково» и «Сколтеха» показало, что 62% разработчиков в России применяли технологии ИИ при написании кода в 2025, а к 2028 эта цифра вырастет до 98%

ТРАНСФОРМАЦИЯ ОТЕЧЕСТВЕННЫХ ИНСТРУМЕНТОВ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Сас АРУСТАМЯН

директор Центра оценки
соответствия и тестирования
АО «НПО «Эшелон»

Чтобы отвечать вызовам современных угроз безопасности информации, инструменты разработки безопасного ПО должны не только существовать, но и доказывать свою эффективность на практике. Так в конце 2025 года завершились масштабные испытания статических анализаторов исходного кода, проведённые при поддержке ФСТЭК России. Эти испытания стали важным этапом в развитии отечественных средств анализа кода и позволили сформировать более прозрачное представление о текущем уровне инструментов статического анализа и их соответствии требованиям ГОСТ Р 71207-2024.

Для нашей команды участие в испытаниях стало возможностью получить независимую оценку ключевых характеристик анализатора на реальных тестовых наборах, а также сопоставить результаты с други-

ми решениями в рамках единых испытаний¹.

При оценке качества статических анализаторов использовались классические метрики, отражающие корректность их срабатываний.

- ◆ TP (True Positive) – ситуация, когда анализатор обнаружил дефект и этот дефект действительно присутствует в исходном коде. Высокое значение TP демонстрирует способность инструмента выявлять реально существующие ошибки в исходном коде.

- ◆ TN (True Negative) – ситуация, когда анализатор не выдал предупреждение и при этом в анализируемом участке кода действительно отсутствует дефект.

РЕЗУЛЬТАТЫ ПО C/C++

По основной формуле для языков C/C++ анализатор АК-ВС 3 показал следующие результаты:

- ◆ TN (True Negative) – 1-е место;
- ◆ TP (True Positive) – 3-е место;
- ◆ TN + TP – 3-е место.

¹ Сравнительный анализ и выбор статических анализаторов безопасности кода / Марков А. С., Антипов И. С., Арустамян С. С., Магакелова Н. А. // Вопросы кибербезопасности. 2024. № 5 (63). С. 79–88.

Первое место по показателю TN имеет особую практическую значимость, поскольку низкое количество ложных срабатываний напрямую снижает трудозатраты на анализ отчётов и повышает применимость инструмента в промышленных проектах с большими кодовыми базами.

РЕЗУЛЬТАТЫ ПО JAVA

Для языка Java результаты АК-ВС 3 распределились следующим образом:

- ◆ TN (True Negative) – 2-е место;
- ◆ TP (True Positive) – 5-е место;
- ◆ TN + TP – 2-е место.

Несмотря на более низкую позицию по показателю TP, суммарная метрика TN + TP демонстрирует второе место, что указывает на сбалансированное качество анализа в целом. Высокое значение TN подтверждает низкий уровень ложных срабатываний, что особенно важно для Java-проектов, использующих большое количество типовых библиотек, фреймворков и повторяющихся шаблонов кода.

При всём том, что результаты по части заявленных языков программирования (C#, Go, JavaScript, Python) не были озвучены, в совокупности результаты по C/C++ и Java показывают, что АК-ВС 3 демонстрирует высокие значения по ключевым метрикам.

РАЗВИТИЕ АК-ВС 3

Отдельную ценность представляет не только итоговая оценка, но и обратная связь, полученная в ходе испытаний. По сути, испытания стали источником данных о тех направлениях развития инструмента, которые требуют приоритетного внимания и способны дать наибольшую практическую пользу при реальном использовании.

Первое место по показателю TN имеет особую практическую значимость, поскольку низкое количество ложных срабатываний напрямую снижает трудозатраты на анализ отчётов и повышает применимость инструмента в промышленных проектах с большими кодовыми базами

Так, в рамках дальнейшего развития продукта планируется расширение перечня поддерживаемых языков программирования, включая Swift и Kotlin, что позволит применять инструмент при анализе более широкого круга современных программных проектов, включая мобильные приложения.

Особое внимание уделяется развитию модуля фаззинг-тестирования, нацеленного на существенное повышение эффективности динамического анализа². В частности, реализована поддержка всех основных режимов инструментации AFL++, что позволяет более гибко адаптировать процесс фаззинга к особенностям исследуемого программного обеспечения. Для оптимизации использования вычислительных ресурсов разработаны механизмы распределения ядер процессора между различными режимами фаззинга, а также предоставлена возможность создания пользовательских схем распределения. Автоматизирован процесс сборки проекта во всех режимах инструментации, и, что немаловажно, в отчёте по результатам фаззинга теперь доступны графики скорости фаззинга и детальная информация о достигнутом покрытии кода, позволяющие оценить эффективность проведённого тестирования. Параллельно развивается модуль полносистемного динамического анализа Код2, который обеспечивает запись, последующий анализ полносистемных трасс, а также позволяет автоматизировано определять поверхность атаки исследуемого ПО.

Дополнительно планируется разработка веб-интерфейса для IDE «Эшелониум», которая в настоящее время доступна в виде десктопного приложения. Так процесс просмотра, анализа и разметки результатов статического анализа станет ещё более удобным.

² Интеллектуальные методы фаззинг-тестирования в рамках цикла безопасной разработки программ / Арустамян С. С., Антипов И. С. В сборнике: Безопасные информационные технологии. Сборник трудов Двенадцатой международной научно-технической конференции. Москва, 2023. С. 11–15.

Не стоит забывать о том, что практики разработки безопасного ПО не ограничиваются статическим и динамическим анализом.

Всё большую роль играет управление рисками, связанными с заимствованными компонентами: библиотеками, фреймворками, сторонними пакетами

СЛЕДУЮЩИЙ ЭТАП В РАЗВИТИИ РБПО: КОМПОЗИЦИОННЫЙ АНАЛИЗ

Не стоит забывать о том, что практики разработки безопасного ПО не ограничиваются статическим и динамическим анализом³. Всё большую роль играет управление рисками, связанными с заимствованными компонентами: библиотеками, фреймворками, сторонними пакетами. Это находит отклик как в отечественных регуляторных требованиях, так и в международных практиках.

Если статический и динамический анализ уже реализованы и активно

развиваются в составе АК-ВС 3, то композиционный анализ выделен в отдельное направление.

В настоящее время в разработке находится инструмент CAT (Composition Analysis Tool) – средство композиционного анализа, предназначенное для:

- ♦ автоматической идентификации всех зависимостей проекта;
- ♦ формирования Software Bill of Materials (SBOM);
- ♦ анализа компонентов по базам уязвимостей (включая NVD и БДУ ФСТЭК России);
- ♦ автоматического формирования ППК (Прикладных программных комплексов);
- ♦ разметки уязвимостей;
- ♦ представления результатов в виде наглядной статистики.

Важно подчеркнуть, что CAT будет доступен как в виде самостоятельного продукта, так и в качестве модуля в составе АК-ВС 3, что позволит разработчикам выстроить конвейер РБПО, включающий сразу три вида анализа.

³ Вареница В. В., Марков А. С., Цирлов В. Л. [и др.]. Как избежать ошибок при безопасной разработке программного обеспечения / Москва: Квант-медиа, 2025. – 344 с. – ISBN 978–5–605–33861–1.

Арустамян С. С., Вареница В. В., Марков А. С. Методические и реализационные аспекты внедрения процессов разработки безопасного программного обеспечения // Безопасность информационных технологий. 2023. Т. 30. № 2. С. 23–37.



В завершение отметим, что всем, кто интересуется статическим анализом исходного кода, практическими примерами и новостями в этой области, будет полезно подписаться на Telegram-канал [@AK_BC_3](https://t.me/AK_BC_3).



Для приобретения знаний по особенностям внедрения процессов безопасной разработки программного обеспечения рекомендуем ознакомиться с **практическим пособием от экспертов «Эшелона»**.

БЕЗОПАСНАЯ АРХИТЕКТУРА

ОТ ПРИНЦИПА НАИМЕНЬШИХ ПРИВИЛЕГИЙ
ДО ВЫЗОВОВ ИИ И ТРЕНДОВ 2026 ГОДА



Евгений ТОДЫШЕВ

руководитель направления безопасной разработки УЦСБ

С чего начинается проектирование защищённого ПО? Как изменяются подходы к проектированию безопасности при разработке AI-систем? Прогноз на ближайшее будущее строим с руководителем направления безопасной разработки УЦСБ Евгением Тодышевым.

— Как на практике применять принцип наименьших привилегий и что такое безопасные настройки по умолчанию?

— Принцип наименьших привилегий — одно из основных понятий в безопасной архитектуре, но его часто реализуют формально. Суть

в том, чтобы выдавать права строго в соответствии с функцией. Это как пропускной режим: сотрудник отдела кадров не должен иметь доступ в серверную. То же самое применимо в разрезе сервисов и процессов. Например, служба для отправки почты не должна иметь полный доступ к базе данных (БД) пользователей. Для этого мы проектируем для каждого сервиса отдельные учётные записи с минимальным набором прав.

Безопасность настройки по умолчанию основана на принципе «запрещено пока не разрешено» и делает «сервис из коробки» максимально закрытым. Например, при создании новой учётной записи пользо-

вателя она по умолчанию не имеет привилегированных прав и доступ к программным интерфейсам (API) выключен. И только администратор системы должен сознательно их включать, понимая все риски. Также при первом входе система сама должна требовать смены пароля администратора, чтобы его нельзя было дальше использовать по умолчанию.

Все эти правила создают защитный слой: даже если злоумышленник получил доступ к какой-то части системы, его продвижение дальше будет затруднено, и он по цепочке привилегий не сможет добраться до самых ценных данных.

При проектировании прежде всего надо понять, какие основные бизнес-функции будет выполнять продукт. Ещё следует учитывать изменения, которые вносятся в софт, моделирование угроз для нового ПО, разработку ИБ-требований и различные рекомендации в адрес ИТ-архитектора и разработчиков.

— Как спроектировать систему разграничения прав в приложении?

— Ядром безопасности приложения является авторизация, и она должна быть централизованной. В системе необходимо создать единую точку принятия решения, которая фактически будет отвечать на вопрос, можно ли пользователю совершать определённое действие. Все запросы к данным должны проходить через неё, исключая разрозненную и противоречивую логику в разных подсистемах. За сами же решения должен отвечать отдельный сервис (или библиотека), в ко-

В системе необходимо создать единую точку принятия решения, которая фактически будет отвечать на вопрос, можно ли пользователю совершать определённое действие. Все запросы к данным должны проходить через неё, исключая разрозненную и противоречивую логику в разных подсистемах

тором и находятся непосредственно сами правила.

Для обеспечения гибкой модели доступа можно использовать связку RBAC и ABAC, то есть ролевой и атрибутной модели. Следует предусмотреть отказ от наследования привилегий по умолчанию и явно задавать разрешение для каждой новой сущности. Например, если создаётся новая папка, пользователь не должен на неё получить те же права, что и на родительскую, — это предотвратит случайное расширение прав. Кроме того, надо создать автоматические тесты на нарушение прав доступа, чтобы пользователю с низкими привилегиями не удалось выполнить действия администратора.

— **Атаки на цепочки поставок — один из ключевых вызовов последних лет. На что ещё, помимо Supply Chain Attack, стоит обратить внимание в 2026 году?**

— Я бы выделил три чётких направления. Во-первых, **безопасность мобильных приложений**. Их количество и зрелость растут, они работают с критичными данными и даже управляют инфраструктурой. Защита от компрометации устройства — must have.

Во-вторых, **API Security**. Количество API растёт лавинообразно, они становятся ядром цифровых продуктов. Необходимы централизованный контроль, анализ трафика и защита от злоупотреблений.

И главный тренд, который мы уже затронули чуть раньше, — **MLSecOps**. Компании массово внедряют модели машинного обучения (ML-модели) для автоматизации, но часто забывают про их безопасность. В ближайшей перспективе ожидается появление ГОСТа и усиление регуляторных требований к безопасности машинного обучения. Это станет отдельной дисциплиной.

Кстати, детально обсуждать тренды мы будем 19 марта **на квартирнике по безопасной разработке** в Москве. Приходите, будем рады пообщаться вживую с экспертами-практиками DevSecOps и все-

В AI-системах появляется фундаментальный класс неуправляемых или слабоуправляемых рисков, связанных с самой природой модели. Также появляются уязвимости, которые присущи данным: то есть атаки смещаются с кода на данные, и тут требуется другой подход к защите

ми, кто хочет глубже погрузиться в эту тему.

— **Какие проблемы возникают при проектировании AI-систем?**

— Проектирование AI-систем, особенно с точки зрения безопасности вообще, достаточно непривычная парадигма, которая порождает и новые вызовы. Если в традиционном софте мы имеем дело с детерминированной логикой и управляемыми рисками в виде известных уязвимостей и ошибок в коде, то здесь работаем с вероятностными моделями. И это вносит определённые корректировки в подходы. В AI-системах появляется фундаментальный класс неуправляемых или слабоуправляемых рисков, связанных с самой природой модели. Также появляются уязвимости, которые присущи данным: то есть атаки смещаются с кода на данные, и тут требуется другой подход к защите. Вдобавок модель сама по себе становится целевым активом и вектором атаки (к примеру, кража интеллектуальной собственности, инверсия модели и т.д.).

Задача архитектора по безопасности в данном случае — минимизировать риски утечек через саму модель. Ему приходится сталкиваться с проблемой чёрного ящика и проблемой тестирования. Сложные модели, например глубокие нейронные сети, часто не интерпретируемы. Недостаточно просто пройти отладчиком — необходимо решать задачу верификации и валидации данных.

Проблемы с цепочками поставок имеют место как при классической разработке ПО, так и в случае применения AI-компонентов. Мы используем какие-то готовые модели, фреймворки, датасеты, которые нужно уметь анализировать, видеть проблемы, находя уязвимости в зависимостях AI-компонентов.

— **Какова в идеальной модели роль специалиста по безопасности при проектировании нового ПО: консультант, куратор, диктующий условия, или часть команды?**

— Здесь могут быть разные подходы. В одном случае мы идём в партнёрском тандеме с разработчиками и помогаем друг другу повысить уровень защищённости ПО. Бывает и так, что приходится всё-таки диктовать условия и настаивать на требованиях к безопасности. В идеале хотелось бы органично сочетать в проекте все три роли: консультанта, блюстителя регуляторных требований и «своего парня».

Без регулярного общения с командой, с архитекторами приложения обойтись нельзя. Специалист по безопасности должен осуществлять и консультационную роль. Да, возможно, он часто не скажет, как лучше написать тот или иной кусок кода, но зато компетентно разъяснит, какие практики безопасности необходимо внедрять. Кроме того, эти практики необходимо составить, утвердить и согласовать как с бизнесом, так и с архитекторами, памятуя об универсальных и специфических условиях их внедрения.

ДЕВУШКИ В РБПО

В ПРЕДДВЕРИИ 8 МАРТА VIS JOURNAL БЕСЕДУЕТ
С ДЕВУШКАМИ, РАБОТАЮЩИМИ В СФЕРЕ РБПО



**Карина
НАПАДОВСКАЯ**
руководитель
Центра
сертификации
и соответствия
стандартам
АО «Лаборатория
Касперского»

— Ваш путь в РБПО?

— Если бы в школе и институте мне сказали, что я буду работать в ИТ-компании, да еще иметь отношение к РБПО, я бы сильно посмеялась. С компьютером и новыми технологиями я всегда была на вы. Получала себе спокойно специальность экономиста-управленца в автомобильно-дорожном университете и собиралась стать министром транспорта. Но в одночасье жизнь кардинально изменилась, на 5-м курсе института мне нужно было срочно выйти на любую работу, и по воле судьбы я устроилась в одну из испытательных лабораторий и стала заниматься сертификацией ПО. За несколько лет карьеры стало очевидно, что моя сильная сторона — это умение руководить проектами, управлять командой и выстраивать коммуникации. Так я оказалась в Лаборатории Касперского, где искали именно такого специалиста, и создала центр сертификации, который на сегодняшний день является образцово-показательным в отрасли. Ну и здравствуй, РБПО!

— Что Вы считаете важным для развития РБПО в отрасли?

— Всегда говорила, что самое важное — это осознание, принятие и про-

движение РБПО руководством компании. Без полной поддержки, как ресурсной, так и бюджетной, выстроить РБПО нельзя. Можно сделать пародию на РБПО, временно решить точечную задачу, но создать отлаженную машину — бесперебойно работающий механизм, коим и должна стать безопасная разработка в компании, — нельзя.

— Одна-две забавных истории из вашей карьеры?

— Когда в 2016 году активно начались разговоры про РБПО, появились соответствующий ГОСТ и инициатива ФСТЭК по внедрению РБПО вендорами, я понимала, что просто попросить команды разработки что-то сделать — очень плохой вариант. Нужен масштабный подход, правильная цель, полная поддержка. Соответственно, нужно не просто плыть по течению и делать что-то, как все, чтобы формально соблюсти требования по сертификации (важно заметить, что все начинали внедрять РБПО, чтобы не было проблем с получением сертификатов, не для реальной пользы в разработке продуктов!) — нужно возглавить это направление. Стать первыми. Показать реальный профит. Руководство компании поддержало эту позицию, ведь Лаборатория Касперского — это флагман в области защиты информации, чья миссия — спасать мир. Ну и безусловным преимуществом было то, что практики безопасной разработки в части анализа уязвимостей и отдельные другие уже были внедрены в компании на высоком уровне. Этот путь мы начинали не с нуля. Дальше нужно было культивировать эту историю (здесь мы вспоминаем, что я на вы с новыми технологиями, про РБПО я знала немного). И я создала многим известное мероприятие Certification Day, которое в этом году пройдет уже в 11-й раз. Цель — на единой площадке с вендорами, регуляторами, испытательными лабораториями, органами по сертификации обсуждать практические проблемы внедрения практик безопасной разработки. Многие, как и я, знали об этом немного (смеюсь). Мы учились, делились опытом, обсужда-

ли проблемы и подходы с регулятором, который слышал боль отрасли и корректировал нормативные документы таким образом, чтобы они были актуальными, полезными и жизнеспособными. Также мы обкатали на себе и первую методику ВУ и НДВ, продемонстрировав отрасли её выполнимость. Закрепили успех, переписав ГОСТ по безопасной разработке в команде с другими передовыми компаниями. За десять лет РБПО буквально переродилось. Это было рискованно. Ну а что, кто не рискует, тот не пьет шампанское, а шампанское я люблю.

— «Женский взгляд»?

— Женщины — уникальные существа. В нас уживается бесконечное множество противоречивых натур, и нам проще найти нужный ключик к сложной задаче, неоднозначному проекту, неразрешимому конфликту, нереальной цели. Важно оставаться женщиной в любой ситуации, на любой позиции, каждый день. Желаю нам всем не растерять свою суть, нести в мир, на работу и домой прекрасное, доброе и светлое — для этого мы и созданы!



Елена БЫХАНОВА
начальник
отдела аудито-
консалтинга
процессов РБПО
НТЦ «Фобос-НТ»

— Ваш путь в РБПО?

— «Оказалась в нужное время, в нужном месте» — так я пришла в РБПО три года назад, когда впервые встретила с евангелистом РБПО Дмитрием Пономаревым в МГТУ им. Баумана на студенческой секции. Я попала в сферу в отличное время — как раз в самый разгар набирающего популярность движения, а именно популяризации парадигмы безопасной и качественной разработки. Положительно сказывающиеся на развитии сферы события происходят одно за другим: нарас-

тает регулярность проведения тематических конференций, ведутся работы по созданию стандартов в техкоме (ТК362), начинают приглашать экспертов на интервью в журналы и подкасты. Тут же по стечению обстоятельств начинает приобретать востребованность аудито-консалтинг, который становится моим основным профилем. Считайте, что в РБПО мы с ним пришли в одно и то же время, так как набирать популярность эта услуга начала как раз за год до выхода ГОСТ Р 56939-2024.

— Что Вы считаете важным для развития РБПО в отрасли?

— В дискуссиях с коллегами по отрасли часто всплывает вопрос о том, что является важным для развития РБПО. Сперва на него хочется отреагировать обратным вопросом: «А кто спрашивает: регулятор, разработчик, потребитель?». Хотя, впрочем, это неважно, ответ один: «Не переставать видеть в этом ценность для России».

От потребителя должны исходить запросы, от разработчика — готовность и инициатива, от регулятора — неукоснительность и разумность. Развиваться будет то, на что есть спрос, что считается перспективным, в чем видят необходимость. А для того, чтобы РБПО было *тем самым*, требуется повышать уровень культуры всех заинтересованных сторон, демонстрируя ценность результатов для решения задачи повышения качества и конкурентоспособности отечественного программного обеспечения.

— Одна-две забавных истории из вашей карьеры?

— Что ж, их много, каждый день сплошные забавы :) А главная из них, даже не знаю, квалифицировать это в положительном или отрицательном ключе, следующая: «нет цели, есть только путь». Как аудито-консалтер, я должна постоянно наращивать собственные (и членов моей команды) компетенции в вопросах выстраивания процессов РБПО и их качественной оценки. При этом с годами я начинаю осознавать, что «чем больше я знаю, тем больше я

понимаю, что ничего не знаю». Для меня, специалиста, занимающегося распространением знаний об РБПО в массы и несущего ответственность за качество передаваемых знаний, важно всегда обладать актуальной информацией и высококлассной экспертизой в сфере, которая развивается невероятно быстро. Так что факт того, что сколько ты в этом РБПО ни развивайся, всё равно конца не увидишь, остается таковым — «забавным». Отсюда, дорогие читатели-разработчики, второй «забавный» факт: и вы тоже со временем приходите к такому осознанию и затем начинаете понимать, что требуется в рамках процесса №1 ГОСТ Р 56939–2024, а именно постоянный анализ, развитие, реализация ;)

— «Женский взгляд»?

— Как я понимаю, здесь надо написать «от женщины для женщин», ну тогда: «Берегите мужчин!». Поддерживайте тех, кто выше вас, и помогайте тем, кто ниже вас. Всем дамам в преддверии праздника желаю осознать свою ценность и применить навыки во имя общего Дела.



**Евгения
РЕМЕЗОВА**
начальник
отдела
технической
экспертизы
ООО НТЦ
«Фобос-НТ»

— Ваш путь в РБПО?

— Моя история в РБПО началась более пяти лет назад. Тогда это была еще небольшая региональная компания, основанная выпускниками Орловской академии ФСО России в городе Орле. Начав как технический писатель, я получила ценный опыт в сфере информационной безопасности, изучила сертификацию, специфику ИТ-компаний и важность качественной документации. Затем перешла в отдел технической экспертизы, где

занималась стандартизацией документации, участвовала в разработке нормативных документов по вопросам информационной безопасности и проведении аудитов на соответствие требованиям РБПО. Сейчас я возглавляю этот отдел, что позволяет мне не только решать конкретные задачи компании, но и формировать будущее отрасли, определяя стандарты и подходы к обеспечению безопасности ПО.

— Что вы считаете важным для развития РБПО в отрасли?

— Развитие практики безопасной разработки ПО является критически важной задачей для современных компаний. На мой взгляд, ключевыми факторами успешного внедрения РБПО являются три основных направления:

1. Стандартизация подходов. Крайне важна единая система стандартов и регламентов, регулирующих процесс разработки и эксплуатации ПО. Отсутствие четких критериев оценки, различие в понимании терминов — всё это ведет к разночтениям между разработчиками и регулятором. Единая терминология необходима для правильного понимания требований и корректного исполнения задач всеми участниками процесса. Стандарты должны охватывать широкий спектр аспектов, начиная от выбора инструментов анализа уязвимостей и заканчивая процедурами тестирования и контроля качества.

2. Развитие и улучшение существующих стандартов. Любые стандарты требуют постоянного обновления и совершенствования. Технологии развиваются стремительно, появляются новые угрозы и методы атак, соответственно, требования к защите должны регулярно пересматриваться и обновляться. Для этого необходимо тесное взаимодействие разработчиков с регулятором. Важно поддерживать открытый диалог, способствующий формированию наиболее эффективных рекомендаций и решений. Регулярные семинары, конференции и рабочие группы способствуют обмену опытом и созда-

нию единой базы знаний, необходимой для качественного развития стандарта.

3. Автоматизация процессов документирования. Одним из ключевых факторов повышения эффективности разработки является автоматизация процессов создания и поддержки технической документации. Инструменты автоматизированного документирования позволяют сократить временные затраты на рутинные операции, повысить точность информации и снизить вероятность человеческих ошибок. Все это способствует повышению прозрачности процессов и упрощению управления проектами.

— Одна-две забавных истории из вашей карьеры?

— Курьёзы случаются. Из последних: при проверке руководства пользователя на последней странице на всю ширину была подпись: «Этот раздел намеренно оставлен пустым». Я удаляю текст и оставляю страницу действительно пустой. Отправляю заявителю, на что приходит ответ: «Почему пропал мой секретный раздел?» Оказалось, что изначально этот раздел должен был содержать важную техническую информацию, но отдел разработки забыл заполнить его содержимым, решив временно вставить шутливую надпись.

В документации по одному из процессов РБПО, в разделе, где подробно должны были быть описаны методы проверки безопасности, встречается фраза: «Использованы лучшие практики безопасной разработки». Что, конечно, говорило о непонимании процесса и несерьезном отношении к документации и работе в целом.

— «Женский взгляд»?

— Цитируя слова песни It's a Man's Man's Man's World: «Этот мир создан мужчиной, но он был бы бессмысленным без женщин», хочу добавить, что будущее индустрии информационной и кибербезопасности зависит в первую очередь от профессионалов, готовых брать ответственность и создавать условия для дальнейшего развития отрасли. Так почему бы таким профессионалом не стать тебе?



**Елена
МАНЬЖОВА**
эксперт органа
по сертификации
ИСП РАН

– Ваш путь в РБПО?

– Мой путь в РБПО стартовал 10 лет назад, когда я начала заниматься сертификацией ПО в рамках систем сертификации средств защиты информации. Быстро стало очевидным, что один скромный абзац в техническом задании о соответствии разрабатываемого ПО требованиям по безопасности информации, расположенный где-то вдали от функциональных требований, – это только верхушка айсберга, под которой скрывается огромная глыба требований, способная привести к срыву работ. Выполнение этих требований без пересмотра подходов и процессов непосредственно разработки – затруднительно и очень затратно, особенно на последнем этапе.

– Что вы считаете важным для развития РБПО в отрасли?

Интересно, что в настоящее время, даже если организация не учитывает требования безопасности при разработке ПО, так как обязательная сертификация как будто бы не нужна, а разработчик не задумывается о безопасности кода, который пишет, или о безопасности заимствованных компонентов, которые использует, – это не освобождает их впоследствии от необходимости этим требованиям соответствовать. Ни одному уважающему себя заказчику не нужно небезопасное ПО. Терять выручку или доверие пользователей после компьютерного инцидента с использованием уязвимостей небезопасного ПО – вот что реально болезненно.

Наверное, осознание этого является наиболее важным для развития РБПО в отрасли. РБПО – это инвестиция в свою репутацию (или в

свое резюме), в качество и место на рынке. И это не так сложно, как кажется, но требует в первую очередь правильной мотивации, а во вторую – правильных проводников.

– Одна-две забавных истории из вашей карьеры?

– Из своего профессионального опыта хочется сказать следующее: чем быстрее удастся перейти из стадии отрицания в стадию принятия и начать перестраивать свои процессы с учетом концепции РБПО, тем лучше.

Иногда разработчики пытаются обосновать отсутствие необходимости в реализации некоторых процессов РБПО, проявляя удивительную смекалку: ссылаются на статьи гражданского кодекса или на тот факт, что разработка является коммерческой и «без обязательств», что их ПО не является средством защиты информации, приводят интересные толкования нормативной базы. Спойлер: это не помогает, когда начинают срывать сделки. Также ничем хорошим не заканчивается замалчивание, когда разработка ведется вне концепции РБПО, а разработчики приходят к соответствующим специалистам уже после выпуска продукта на рынок при возникновении проблем с реализацией.

Поэтому важно последовательно выстраивать культуру и процессы РБПО в организации в целом, с определенной очередностью и дифференциацией требований в зависимости от вида, назначения и области применения ПО.

– «Женский взгляд»?

– В преддверии праздника 8 Марта отдельно хочется сказать всем женщинам, которые занимаются вопросами информационной безопасности, сертификации и обеспечением безопасности разработки, – никогда не сомневаться в себе, с юмором относиться к предрассудкам и даже использовать их в свою пользу, ведь женщина способна добиться успеха там, где мужчины встречают сопротивление. Желаю всем легкой безопасности!



**Натали
ДУБОТЛКОВА**
руководитель
группы
обеспечения
безопасности
приложений
ООО Базис

– Ваш путь в РБПО?

– Я начинала свою карьеру как обычный инженер-программист.NET, но на стажировке выпала возможность дополнительно занять место Security Champion в проекте. На тот момент я даже не представляла, во что вписалась, и как это изменит мою карьеру. Именно там я впервые погрузилась в моделирование угроз и попробовала свои силы в проектировании безопасной архитектуры. Там же я впервые столкнулась с непониманием со стороны разработчиков необходимости усложнять и менять существующую устоявшуюся архитектуру. После стажировки я сознательно выбрала роль AppSec-инженера в той компании. И поняла: вот он, мой мир, где есть четкие правила, строгость и однозначность. Мне это оказалось гораздо ближе, чем творческая неопределенность в чистой разработке.

– Что вы считаете важным для развития РБПО в отрасли?

– Я очень рада, что сейчас всё больше и больше говорят о важности безопасности в жизненном цикле разработки. В целом для отрасли я считаю ключевым смещение фокуса с формальных показателей на суть. Нам нужна гонка за качеством и реальной безопасностью продукта, а не за красивыми сертификатами на стене или погоней за новыми функциями любой ценой. К сожалению, пока это часто остаётся мечтой о мире розовых единорогов.

– Одна-две забавных истории из вашей карьеры?

– Любовь к учёбе – мой конёк, бакалавриат и две магистратуры тому доказательство. Параллельно с рабо-

той специалистом по безопасности кода я изучала и другие направления информационной безопасности. Так я познакомилась с тестированием на проникновение и начала использовать разные сканеры для работы. Изучив простые виды уязвимостей, я переходила к более сложным и изощренным и, конечно же, искала именно такие на практике. Однажды мне выпала возможность провести свой первый реальный пентест на сайте внутренних услуг компании. Я, полная амбиций, сразу нырнула в недра сайта в надежде найти что-то «серьезное» и показать, на что я способна. Не найдя ничего «достойного», я уверенно отписала в заключении, что сайт безопасен. А через неделю пришло уведомление: на том самом сайте обнаружена обычная, классическая XSS. Та самая, куда можно вставить alert(1) — и это сработает. Сказать, что я была в шоке — ничего не сказать. История обошлась небольшим выговором и фразой «горе от ума», которая за мной закрепилась до конца работы в той компании. Зато с тех пор я твердо усвоила правило: проверку всегда начинать с самого простого и элементарного. Потому что иногда самое очевидное оказывается самым опасным.

— «Женский взгляд»?

Часто говорят про какую-то особую «женскую интуицию». Я бы назвала это скорее натренированным вниманием к мелочам. И особенно — к моментам, когда всё вокруг слишком идеально. Именно в такие периоды затишья у меня включается режим максимальной боевой готовности. Потому что опыт уже научил: самые критичные уязвимости и сломанные пайплайны появляются чаще всего в этой обманчивой тишине. Так что советую и себе прошлой, и всем, кто чувствует подобный внутренний звоночек, — прислушиваться к нему. Возможно, это просто голос вашего же опыта, который тихо подсказывает, куда смотреть. В безопасности нет мелочей, и такая интуиция — это ваш первый и самый важный сканер аномалий.

И ещё один момент, важный лично для меня. Говоря о «женском взгляде», я не сталкивалась с ситуациями, где мой пол создавал бы трудности. В безопасности, как я её вижу, нет «мужских» или «женских» ролей. Есть специалист, который либо видит архитектурные риски, уязвимости, угрозы и умеет их объяснить, либо нет. И я верю, что будущее именно за такой средой, где главный критерий — не кто ты, а что ты знаешь и как умеешь применять свои знания.



Анастасия КАЛУГИНА
руководитель направления безопасной разработки и инфраструктуры компании «ИнфоТекС»

— Путь в РБПО или из каких кирпичиков он строится?

— Мой путь в безопасной разработке начался вполне классически — с программирования. При техническом складе ума, родителях-программистах и активно развивающейся ИТ-отрасли у меня не было ни единого шанса. С профессией я определилась ещё в школе, выучилась по этому направлению и продолжаю получать новые знания в дополнение к базе, с которой все начиналось. Во время учёбы на программиста я нашла подработку с гибким графиком в области системного администрирования, поэтому практический опыт в ИТ начался с этого направления. Позднее к нему прибавилась работа по направлению backend-разработки.

Что примечательно — две ипостаси («Dev» и «Ops») «жили» у меня параллельно, практически не пересекаясь, около десяти лет. Аббревиатура DevOps уже появилась, опыт в обоих направлениях накопился немаленький, но не было комплексного понимания этого термина. А потом я поменяла работу. Пришла на очень интересный инновационный проект, где не существовало готовых решений,

и подход и механизмы для решения поставленных задач пришлось прорабатывать с нуля. Спустя какое-то время я поняла, что ранее абстрактный эпитет «DevOps» применительно к разрабатываемой системе перестал быть для меня сухой аббревиатурой и трансформировался во вполне определённую концепцию. И эта концепция сильно отличается от общепринятого определения. Для меня DevOps — это подход, где единственный критерий — оптимальность: если конкретную задачу эффективнее решить набором конфигураций или скриптов — автоматизируем, если лучше использовать приложение — кодируем. Хотя это уже скорее «DevArchOps», так как оценивать нужно архитектуру разрабатываемой системы в целом.

Понимание, как соединить разноплановые компетенции и какие это дает выгоды, выкристаллизовалось не сразу, но оно очень пригодилось для развития и обогащения знаний. И далее, формирование уже третьего направления до полноценного DevSecOps было для меня вполне осознанным. А потом активно стал развиваться подход разработки безопасного ПО (РБПО), и DevSecOps органично обогатился необходимостью:

- ♦ обеспечения безопасности в привязке к процессам разработки и на каждом этапе жизненного цикла ПО;
- ♦ обеспечения безопасности цепочки поставок;
- ♦ управления уязвимостями разрабатываемого и эксплуатируемого ПО;
- ♦ управления обучением сотрудников.

На мой взгляд, РБПО — на данный момент единственный системный подход для комплексного обеспечения безопасности разрабатываемого ПО. Нельзя выделить приоритетное требование или главный этап жизненного цикла ПО, только системный подход позволяет максимально обезопасить разработку продукта.

А теперь к теме женщин в РБПО. Еще пять лет назад я целенаправленно искала хотя бы пару девушек, чтобы разбавить коллектив из 40 мужчин-безопасников. Тогда результат был печальным — чтобы найти пер-

вую кандидатуру, потребовалось полгода интенсивных поисков. Девушки в ИБ просто не шли. Сейчас ситуация наконец выравнивается — отрасль безопасной разработки стала активнее развиваться, ее необходимость на рынке стала очевидно продвигаться, и женщины в безопасность стали приходить активнее. И это отлично! Когда над решением задачи работают специалисты с разноплановым опытом и подходами, когда привносят большее количество идей — это всегда позволяет достичь лучшего результата.



Альбина АСКЕРОВА
руководитель направления по взаимодействию с регуляторами Swordfish Security

— Ваш путь в РБПО?

— Мой путь, как это часто бывает, не был прямым, но вектор своего развития в ИТ я определила ещё в школе. У меня были прекрасные учителя математики и физики, которые показали «магию» точных наук и зажгли интерес на годы вперед.

Я поступила в технический вуз на направление сетей связи. Любимый Бонч (СПбГУТ им. проф. М. А. Бонч-Бруевича) стал важным этапом моего профессионального становления. На последнем курсе я уже работала по специальности, а ближе к защите диплома поняла, что задачи по защите информации увлекают меня сильнее. Сразу после выпуска поступила в магистратуру по информационной безопасности и начала работать в ИБ. И вот тут всё закрутилось!

Старт в отделе ИБ крупной госкомпании был классическим: политики, антивирусы, инциденты. Со временем пришло понимание, что мы чаще «латаем дыры», реагируя на проблемы. Это было объяснимо: молодой отдел, ограниченные ресурсы, мас-

штабная инфраструктура и множество регуляторных требований.

Постепенно команда выросла: выстроили процессы, начали автоматизацию, внедряли инструменты. Благодарна своим руководителям за доверие и пространство для развития.

Следующим этапом развития процессов уже моего Управления ИБ стала разработка — внутренний код и заказные решения. Это закономерно привело к погружению в мир практик безопасной разработки, а затем и в РБПО. Оглядываясь назад, понимаю, что сегодня стратегия была бы другой, но именно этот опыт дал мне прочную опору в текущих проектах.

Сложно переоценить, сколько сил, времени и души вкладывают люди, развивающие ИБ и РБПО в нашей стране, и я рада сегодня быть частичкой этого!

— Что вы считаете важным для развития РБПО в отрасли?

— На мой взгляд, ключевое — культура. Можно внедрить лучшие инструменты и стандарты, но без сдвига в отношении к созданию продуктов это упрётся в стену. Безопасность кода со временем должна стать частью профессиональной гордости и осознанной ответственности разработчика. Сейчас многое делается: развиваются сообщества, проводятся мероприятия, обновляется регулирование, меняются образовательные программы. Наверное, остаётся заложить основы безопасного ПО ещё в обучении в школе в инженерных классах, чтобы это стало естественной частью мышления будущих специалистов.

— Одна-две забавных истории из вашей карьеры?

— Один забавный случай произошел недавно. Я опаздывала с одной встречи регулятора на другую. Забежав в уже полный кабинет, заняла одно из последних свободных мест с краю стола. Оказалось, это место рядом с главой стола. Вошел инициатор встречи, и по законам жанра первые вопросы адресовали тем, кто сидел рядом, включая меня. Со временем начинаешь относиться к таким ситуациям с юмором и здоровым спокойствием.

— «Женский взгляд»?

— Убеждена, что ключ к успеху — любознательность и искренний интерес к своему делу. В технических сферах женщинам часто помогают качества: чуткость, умение работать в команде, гибкость, способность понимать не только слова, но и мотивы людей. Мы все разные, и в этом наша сила. Важно осознать и использовать свою индивидуальность, слышать друг друга и действовать сообща.



Нелли МАГАКЕЛОВА
руководитель группы Центра оценки соответствия и тестирования АО «НПО «Эшелон»

— Ваш путь в РБПО?

— Уже более четырёх лет моя профессиональная деятельность связана с информационной безопасностью. Мой путь начался с тестирования различных программ, преимущественно относящихся к банковскому сектору. Спектр задач был широким: от анализа кода и поиска уязвимостей до разработки документации. Этот опыт дал мне возможность не только находить слабые места, но и видеть, как команды реагируют на них, как принимаются решения и как устраняются проблемы в продуктах, которыми пользуются миллионы людей. Со временем пришло понимание, что безопасность — это не только про жизненный цикл уязвимости, но и про культуру команды. Позже мне удалось участвовать в полноценной разработке программного обеспечения с нуля, где мне приходилось быть одновременно разработчиком, аналитиком и архитектором. Этот опыт дал понимание того, как рождаются решения, какие компромиссы приходится искать для баланса между безопасностью и промышленной разработкой.

– **Что вы считаете важным для развития РБПО в отрасли?**

Что же действительно движет РБПО вперёд? На мой взгляд, ключ не только в регламентах и стандартах, а прежде всего в осознанности людей. Безопасность не должна быть обособленным этапом, про который обычно вспоминают перед релизом. Она должна стать способом мышления всей команды разработки. Не просто формальное выполнение требований, а постоянные вопросы в стиле: «Что будет, если злоумышленник попробует вот так?». Когда вопрос «Для чего нам РБПО?» становится общим языком разработчиков, аналитиков, тестировщиков и менеджеров, РБПО перестаёт быть бюрократией и превращается в инструмент создания качественных продуктов. И, что немаловажно, такой подход почти всегда оказывается экономически выгоднее, поскольку он снижает количество критических инцидентов, доработок и репутационных потерь.

– **Истории из карьеры?**

– Было немало случаев, когда даже продукт с высоким уровнем зрелости оказывался проблемным с точки зрения безопасности. Однажды с помощью одного отправленного вредоносного запроса удалось вывести из строя многопользовательский сервис с реальными клиентами. Как позже выяснилось, это произошло из-за неправильно настроенной инфраструктуры. Также об одном забавном случае рассказал слушатель нашего курса. При обсуждении фаззинг-тестирования в контексте непредсказуемости поведения программы коллега поделился историей, как оператор системы систематически выводил из строя программу из-за тремора рук, поскольку он отправлял запрос чаще, чем система могла бы обработать. Такие примеры демонстрируют, что порой аварийное завершение программы может возникнуть не только из-за ошибок, допущенных при разработке или проектировании, но и из-за банального человеческого фактора.

– **«Женский взгляд»?**

– Для девушек, которые думают об этом пути, хочется сказать следующее: не позволяйте стереотипам определять ваш выбор. История развития информационных технологий свидетельствует о том, что женщины всегда играли значимую роль в развитии этой области: Ада Лавлейс, Грейс Хоппер, Маргарет Гамильтон, Хеди Ламарр – и это лишь самые известные имена из тех, кто внёс огромный вклад в развитие компьютерных наук. Важно помнить, что в любой профессии ценится в первую очередь глубина мышления, любознательность, инициатива. Люди без индивидуальности – это всего лишь копии копий копий, а миру особенно нужны те, кто способен мыслить самостоятельно и видеть дальше шаблонов. Поэтому, если вас интересует мир разработки безопасного программного обеспечения, не бойтесь идти вперёд и создавать будущее, в котором технологии будут служить безопасно и надёжно.

БЕЗОПАСНОСТЬ ТЭК
ФОРУМ ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ ДЛЯ
ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА

КОМПЛЕКСНЫЕ СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТОВ ТЭК
 РОБОТОТЕХНИКА И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ
 ЦИФРОТЕХ
 НАВИГАЦИЯ И СВЯЗЬ
 ПОЖАРНАЯ БЕЗОПАСНОСТЬ
 ТЕХНОЛОГИИ СПАСЕНИЯ

12-13 МАРТА 2026
МОСКВА, ВДНХ, ПАВИЛЬОН 57

SFEXPO.RU

ОРГАНИЗАТОР
БИЗНЕС ОБЪЕДИНЕНИЕ ВЫСТАВОЧНЫХ КОМПАНИЙ

ЦИФРОВОЙ РУБЛЬ НА МАРШЕ

ИЛИ АНАЛОГОВЫЕ ПРОМПТ-ИНЪЕКЦИИ В РЕАЛЬНОЙ ЖИЗНИ



Андрей ЖАРКЕВИЧ
эксперт Start X,
ведущий рубрики

По данным ВЦИОМ, значительная часть россиян либо не слышала о цифровом рубле, либо затрудняется объяснить, что это такое. Похожие выводы делает и РБК, публикуя результаты опроса «Сравни.ру». При этом закон уже принят, пилот с реальными деньгами идёт, а массовое внедрение запланировано на 2026 год.

Получается парадокс: государство активно продвигает новую форму денег, а граждане не понимают, как она работает и где её искать. Это идеальная почва для мошенников — и они уже начали её осваивать.

Я решил проверить, насколько цифровой рубль реален для обычного клиента банка.

ЭКСПЕРИМЕНТ: НАЙТИ ЦИФРОВОЙ КОШЕЛЁК

Цель простая: найти в мобильном банке цифровой кошелёк или хотя бы понять, как его открыть. Взял четыре приложения — ВТБ, Сбер, Т-Банк и Альфа.

ВТБ. В поиске приложения вбил «цифровой рубль», «цифровой кошелёк», «ЦР». Ноль результатов. Написал в чат поддержки. Ответ через 12 минут: «На данный момент функционал цифрового рубля недоступен для клиентов. Следите за новостями».

Сбер. Поиск выдал раздел «Цифровые финансовые активы» — это платформа для покупки токенов на криптовалюты, какао и прочую экзотику. К цифровому рублю ЦБ это не имеет отношения. В чате уточнили: «Цифровой кошелёк пока недоступен».

Т-Банк. Ни в каталоге услуг, ни в поиске ничего похожего. Поддержка ответила шаблонно: «Когда появится — вы узнаете из приложения».

Альфа. Аналогично. Поиск пуст, в разделе «Счета» — только обычные рублёвые и валютные.

Итого: четыре крупнейших банка, ноль кнопок «Открыть цифровой кошелёк». При этом все четыре — участники пилота ЦБ.

Если мне, человеку с техническим и финансовым бэкграундом, приходится выдирать информацию по крупицам, что говорить о клиенте, который просто услышал в новостях, что «цифровой рубль вот-вот введут»?

КОШЕЛЁК ШРЁДИНГЕРА

В новостях цифровой рубль выглядит вполне живым. Есть Федеральный закон № 340-ФЗ, есть Положение Банка России № 820-П, есть пилот с реальными деньгами, в котором участвуют 13–15 банков и ограниченный круг их клиентов.

Но ключевые слова здесь — «ограниченный круг». В первых волнах туда попадали в основном сотрудники банков, позже — отобранные клиенты и компании. Это прямо следует из сообщений самого ЦБ о пилоте.

Для обычного же человека цифровой кошелёк сегодня — это:

- ◆ официальные обещания «вы сможете открыть его в мобильном приложении»;
- ◆ общие схемы в духе «будет удобно и безопасно»;
- ◆ и полное отсутствие кнопки «Открыть кошелёк» в реальном приложении.

Возникает парадокс, который можно назвать «кошельком Шрёдингера»: цифровой рубль одновременно есть и его нет. На уровне законов и документов — есть. На уровне повседневного интерфейса — его видела лишь небольшая группа участников пилота.

И здесь мы подходим к самой интересной части — человеческому фактору.

АНАЛОГОВЫЕ ПРОМПТ-ИНЪЕКЦИИ

В мире ИИ под prompt injection понимается приём, при котором злоумышленник подсовывает модели текст, переписывающий её исходные инструкции. Модель всё ещё «умная», но теперь действует по чужим правилам.

С людьми в финансовой сфере происходит то же самое — только «инъекция» делается не в нейросеть, а в голову клиента.

У любого осторожного человека есть внутренний свод правил:

- ♦ банк не просит данные карты по телефону;
- ♦ реквизиты контрагента нужно проверять;
- ♦ нельзя переходить по ссылкам из SMS «от службы безопасности».

Но дальше появляется новая история:

«У нас теперь цифровой рубль, всё меняется, вам надо срочно активировать кошелек / перевести средства / подписать согласие, иначе...»

И внутренний свод правил начинает давать сбой. Человек ещё плохо понимает, что такое цифровой рубль, зато отлично слышит слова «новый закон», «Центробанк» и «государство». Этого оказывается достаточно, чтобы переписать привычные ограничения.

Это и есть **аналоговая промпт-инъекция**: тщательно подобранный текст — звонок, SMS, «разъяснение» в мессенджере, — который переписывает человеческие правила безопасности так же, как вредоносный промпт переписывает системные инструкции ИИ.

ЛЕГЕНДА ЕСТЬ — КОШЕЛЬКА НЕТ. ИДЕАЛЬНАЯ СРЕДА ДЛЯ МОШЕННИКОВ

С точки зрения социальной инженерии цифровой рубль — подарок судьбы. Он:

1. Новый и непонятный. Большинство людей либо ничего о нём не знает, либо имеет смутное представление.

2. Официальный и «обязательный» на уровне риторики. Закон принят, ЦБ активно объясняет преимущества, в новостях звучат сроки массового внедрения и обязательность для банков.

3. Невидим в интерфейсе. Кошелек обещают открыть через мобильное приложение, но обычный клиент его не видит и не понимает, как он будет выглядеть.

На этом противоречии — «вроде бы есть, но руками потрогать нельзя» — и строятся мошеннические легенды. Массовых случаев пока не зафиксировано, но логика этих схем уже встречалась в других формах — в мошенничестве с «безопасными счетами»

и псевдокриптой. Ниже — сценарии, которые с высокой вероятностью появятся или уже появились в арсенале злоумышленников.

СЦЕНАРИЙ ПЕРВЫЙ: «ИНВЕСТИЦИИ В ЦИФРОВОЙ РУБЛЬ»

Людям предлагают «инвестиции в цифровой рубль» с регулярными выплатами и гарантированной доходностью «под крылом государства».

Логика простая:

- ♦ ЦБ запустил цифровую валюту — значит, это «новый инструмент».
- ♦ Новый инструмент — значит, на нём можно заработать больше, чем на старых.
- ♦ «Мы работаем официально, вот ссылка на личный кабинет — остаётся только перевести деньги...»

Психологически это продолжение старых схем с псевдокриптой. Отличие в том, что теперь легенда подкреплена реальным законом и пресс-релизами ЦБ.

Фактически цифровой рубль **нельзя купить как инвестиционный актив**: это не токен и не ЦФА, а просто ещё одна форма того же рубля, который уже лежит на счёте. ЦБ прямо подчёркивает это в своих разъяснениях.

Но когда кошелек существует только в описаниях, граница между «цифровым рублём ЦБ» и любым маркетинговым «цифровым чем-то-там» для клиента стирается.

СЦЕНАРИЙ ВТОРОЙ: «АКТИВАЦИЯ ЦИФРОВОГО КОШЕЛЬКА»

Звонки «из банка» или «из Социального фонда»:

«С 1 августа вступили в силу нормы закона о цифровом рубле, мы переводим ваши накопления в безопасный цифровой формат. Для активации кошелька подтвердите данные карты / продиктуйте код / установите приложение...»

Сюжет знакомый: классический социальный инжиниринг под видом защиты денег.

Разница в том, что ссылка на цифровой рубль звучит убедительнее абстрактного «нового законодательства»: закон действительно есть, пилот идёт, ЦБ об этом говорит.

Мошеннику даже не нужно объяснять, где именно в приложении находится кошелек. Достаточно сказать: «сейчас всё будет по-новому, вот ссылка — войдите и подтвердите».

СЦЕНАРИЙ ТРЕТИЙ: ЗАРПЛАТЫ В ЦИФРОВОМ РУБЛЕ

В новостях уже мелькали сообщения о первых зарплатах в цифровых рублях — в чис-

ле получателей фигурировали чиновники и участники пилота.

Дальше дело техники:

- ♦ фишинговое письмо от «службы персонала» или «банка»;
- ♦ ссылка на страницу-двойник с предложением «подтвердить согласие на получение зарплаты в цифровом рубле»;
- ♦ форма, собирающая логины, пароли, СМС-коды.

Для человека, который слышал, что «кто-то в Госдуме получал зарплату в цифровом рубле», такая легенда звучит правдоподобно.

И здесь снова работает аналоговая промпт-инъекция: старое правило «зарплатные реквизиты меняются только через кадровика» временно отключается, потому что «это же новый формат, тут всё по-другому».

СЦЕНАРИЙ ЧЕТВЁРТЫЙ: B2B-ФИШИНГ

Для корпоративного сегмента цифровой рубль тоже подаётся как будущее платёжной инфраструктуры: поэтапная обязательность для банков, сценарии для госконтрактов. Об этом писали и в релизах ЦБ о планах на 2026 год.

На этом фоне письмо от «контрагента» выглядит правдоподобно:

«В связи с требованиями Банка России наша компания с 01.10 переходит на расчёты в цифровой форме. Просим осуществлять платежи на следующие реквизиты...»

Это старая схема смены реквизитов, но с более солидным камуфляжем.

Если у компании нет жёсткого процесса верификации, бухгалтерия может среагировать по принципу: «всё равно всем придётся переходить». А дальше уже не важно, что цифровой рубль ещё в пилоте.

ЧТО ДЕЛАЮТ ЦБ И БАНКИ?

Нельзя сказать, что регулятор и банки бездействуют. Есть официальный раздел ЦБ «Цифровой рубль», есть разъяснения и FAQ, есть публикации о том, что кошельки автоматически открываться не будут.

Но проблема в другом: объяснено, что такое цифровой рубль, но не показано, как он выглядит в жизни.

Нет массовых скриншотов, нет воспроизводимого пользовательского пути: где в приложении будет кнопка, как выглядит чек, чем «перевод в цифровых» отличается от обычного перевода.

Пока этого нет, любой мошенник может нарисовать свой интерфейс цифрового рубля —

и никто не скажет, что «так не бывает», потому что практически никто ещё не видел, как «бывает на самом деле».

ЧТО МОЖНО СДЕЛАТЬ, ПОКА КОШЕЛЁК ЕЩЁ «НА ПОДХОДЕ»

С точки зрения ИБ и человеческого фактора у нас есть временной люфт — пилот расширяется, массовое внедрение растянуто на несколько лет. Этот люфт стоит использовать.

1. Чётко очертить границы нормального. Сказать простым языком:

- ♦ Банк никогда не будет звонить, чтобы «активировать цифровой кошелёк» или «перевести всё на безопасный цифровой счёт».
- ♦ ЦБ никогда не будет предлагать «инвестировать в цифровой рубль» с супердоходностью.

♦ Переход на цифровой рубль никогда не требует передачи кодов, паролей и реквизитов по телефону или в мессенджере.

2. Показать интерфейсы до того, как их покажут мошенники. Хотя бы в виде макетов и видеодемо: как выглядит цифровой кошелёк, где он в приложении, какие операции доступны. Тогда любая «альтернативная» версия в фишинговом письме будет выглядеть подозрительно.

3. Встроить легенду цифрового рубля в обучение. Симуляции фишинга для сотрудников банков и корпоративных клиентов должны включать сценарии «цифровой зарплаты», «перехода контрагентов на цифровой рубль», «активации кошельков».

Если мы этого не сделаем, эти сценарии за нас прогонят мошенники — только уже на реальных деньгах.

ВМЕСТО ПОСЛЕСЛОВИЯ

Цифровой рубль — красивый технологический проект. Централизованная платформа, строгая регуляторика, высокая степень контроля за операциями — всё это уменьшает риски на уровне инфраструктуры, о чём подробно пишет Банк России в описании платформы.

Но в ближайшие годы главным объектом атак будут не платформы, а люди.

Пока цифровой кошелёк живёт в документах и презентациях, любая ссылка «на цифровой рубль» превращается в удобный инструмент для аналоговой промпт-инъекции.

Вопрос в том, кто первым этим инструментом воспользуется: мы — чтобы внедрить в сознание людей простые правила безопасности, или мошенники — чтобы переписать эти правила под себя.

СОДРУЖЕСТВО НЕПРИЗНАННЫХ ГОСУДАРСТВ (СНГ-2)

ОБЗОР ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Александр
ВИНОГРАДОВ**
ФГУП «ЦНИИХМ»

Сергей МЕНЬШИКОВ
основатель Belarusian
InfoSecurity Community

Андрей СИТНОВ
независимый эксперт

Наталья КАЗАНЦЕВА
независимый эксперт

Содружество непризнанных государств (Союз непризнанных государств, СНГ-2) – объединение непризнанных и частично признанных государств на постсоветском пространстве, основанное в 1992 году. Состоит из Республики Абхазия, Приднестровской Молдавской Республики и Республики Южная Осетия.

Рассмотрим более подробно законодательство каждой из этих стран.



ПРИДНЕСТРОВСКАЯ МОЛДАВСКАЯ РЕСПУБЛИКА, ИЛИ ПРИДНЕСТРОВЬЕ

Непризнанное государство в Восточной Европе, провозглашённое на международно признанной территории Молдовы. Расположено преимущественно на левом берегу Днестра, включает в себя также несколько сёл и город Бендеры на правом берегу. Выхода к морю не имеет.

Столица – Тирасполь.

Официальные языки: молдавский, русский, украинский.

Законодательство о защите информации. Отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации, регулируются Законом Приднестровской Молдавской Республики от 19.04.2010 № 57-3-IV «Об информации, информационных технологиях и о защите информации».

Законом предусмотрены следующие виды информации: свободно распространяемая; предоставляемая по соглашению лиц, участвующих в соответствующих отношениях; подлежащая предоставлению или распространению; распространение которой ограничивается или запрещается.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

- ♦ на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- ♦ соблюдение конфиденциальности информации ограниченного доступа;
- ♦ реализацию права на доступ к информации.

В июле 2025 года в Закон внесены изменения, направленные на регулирование вопросов информационных систем, в том числе в части размещения серверов, оборудования и иных технических средств исключительно на

территории Приднестровской Молдавской Республики. Функции контроля создания, развития, использования и вывода из эксплуатации государственных информационных возлагаются на Министерство цифрового развития и органы госбезопасности. Внесение изменений в Закон направлено на усиление защиты персональных данных и государственной информации. Также появляется единый и понятный механизм контроля, а государство сможет быстрее выявлять и предотвращать нарушения в области защиты информации.

Законодательство о персональных данных. Вопросы обработки персональных данных в Приднестровской Молдавской Республике регулируются Конституцией, Трудовым кодексом, Законом от 16.04.2010 № 53-3-IV «О персональных данных», Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, принятым Постановлением Правительства ПМР 05.08.2014 № 210.

Персональные данные — любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных). Какого-либо исчерпывающего перечня таких сведений Закон не даёт, поэтому рассматривается это понятие в самом широком значении. Это информация, которая определяет субъекта как физическое лицо. Защиту такой информации гарантирует статья 24 Конституции Приднестровской Молдавской Республики, в которой в том числе говорится о невмешательстве в частную жизнь.

Любое лицо, которому передаётся такая информация, автоматически становится оператором персональных данных. В качестве оператора могут выступать физические и юридические лица, государственные и муниципальные органы. Операторы, обрабатывая персональные данные, должны иметь для этого согласие субъекта либо предусмотренное законом основание для обработки персональных данных без согласия. При этом, даже при наличии оснований, обработка персональных данных должна ограничиваться достижением конкретных, заранее определённых и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Функции и полномочия по определению государственной политики в сфере защиты

прав субъектов персональных данных осуществляет Министерство цифрового развития, связи и массовых коммуникаций. Данное министерство также осуществляет контрольно-надзорную деятельность в этой сфере, проводит плановые и внеплановые проверки операторов персональных данных по соблюдению требований правил действующего законодательства, рассматривает обращения субъектов персональных данных по нарушениям, реализует полномочия по пресечению правонарушений.

Административная ответственность за нарушение порядка обработки персональных данных установлена Кодексом об административной ответственности Приднестровской Молдавской Республики. Полномочия по возбуждению дел по данной категории возложены на Прокуратуру Приднестровской Молдавской Республики, дела рассматриваются судом. Задача Министерства цифрового развития, связи и массовых коммуникаций — выявить нарушения и уведомить об этом Прокуратуру.



РЕСПУБЛИКА ЮЖНАЯ ОСЕТИЯ, ИЛИ ГОСУДАРСТВО АЛАНИЯ

Частично признанное государство на Южном Кавказе, провозглашённое на международно признанной территории Грузии.

Вопрос о международно-правовом статусе Южной Осетии является спорным: независимость республики признана пятью государствами — членами ООН (Россия, Венесуэла, Никарагуа, Науру, Сирия) и тремя непризнанными и частично признанными государствами. В документах ООН рассматривается как территория Грузии.

Столица — Цхинвал (Цхинвали).

Официальные языки : осетинский, русский и грузинский.

Законодательство о защите информации. Вопросы защиты информации в Республике Южная Осетия регулируются

Законом от 12.02.2016 № 57 «Об информации, информационных технологиях и о защите информации», Законом от 29.12.2017 «Об обеспечении доступа к информации о деятельности органов государственной власти Республики Южная Осетия».

Информация представляет собой сведения (сообщения, данные) независимо от формы их представления. Условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за её разглашение устанавливаются действующим законодательством. Распространение информации осуществляется свободно при соблюдении установленных требований.

Обладатель информации, оператор информационной системы, в случаях, установленных законодательством Республики Южная Осетия, обязан обеспечить:

- ♦ предотвращение несанкционированного доступа к информации и (или) передачи её лицам, не имеющим права на доступ к информации;
- ♦ своевременное обнаружение фактов несанкционированного доступа к информации;
- ♦ предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- ♦ недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- ♦ возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- ♦ постоянный контроль за обеспечением уровня защищённости информации.

Особенности регулирования вопросов доступа к информации регулируются Законом «Об обеспечении доступа к информации о деятельности органов государственной власти Республики Южная Осетия».

К информации о деятельности органов государственной власти Республики Южная Осетия относятся законы, нормативные правовые акты, правовые акты, устанавливающие структуру, полномочия, порядок формирования и деятельности указанных органов и организаций, иная информация, касающаяся их деятельности.

Пользователи в отношении указанной информации имеют право получать достоверную информацию о деятельности государственных органов власти; отказываться от

её получения; не обосновывать необходимость получения запрашиваемой информации, доступ к которой не ограничен, и иные права.

В целях обеспечения права пользователей информацией на доступ к информации о деятельности государственных органов власти меры по защите этой информации принимают государственные органы власти Республики Южная Осетия.

Законодательство о персональных данных. Вопросы обработки и защиты персональных данных в Республике Южная Осетия установлены Законом Республики Южная Осетия от 11.06.2008 № 118 «О персональных данных».

К персональным данным Закон относит любую информацию, относящуюся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессию, доходы, другую информацию.

Для защиты персональных данных при их обработке оператор персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных устанавливаются Правительством Республики Южная Осетия.

Указом Президента Республики Южная Осетия от 11.08.2022 № 415 утверждено «Положение о персональных данных государственного гражданского служащего Республики Южная Осетия и ведении его личного дела».

Согласно Положению под персональными данными гражданского служащего понимаются сведения о фактах, событиях и обстоятельствах жизни гражданского служащего, позволяющие идентифицировать его личность и содержащиеся в личном деле граж-

данского служащего либо подлежащие включению в его личное дело.

При обработке персональных данных гражданского служащего кадровая служба государственного органа обязана соблюдать требования, в том числе по защите персональных данных гражданского служащего от неправомерного их использования или утраты, которая осуществляется за счёт государственного органа.

Учётные данные гражданских служащих хранятся кадровой службой государственного органа на электронных носителях. Кадровая служба обеспечивает их защиту от несанкционированного доступа и копирования.

Представитель нанимателя в лице руководителя государственного органа либо его представителя, осуществляющих полномочия нанимателя от имени Республики Южная Осетия, обеспечивает защиту персональных данных гражданских служащих, содержащихся в их личных делах, от неправомерного их использования или утраты.



РЕСПУБЛИКА АБХАЗИЯ

Частично признанное государство в Закавказье, провозглашённое на международно признанной территории Грузии в ходе грузино-абхазского конфликта.

Независимость республики признана пятью государствами — членами ООН, включая Россию. В документах ООН Абхазия рассматривается как территория Грузии.

Столица — Сухуми (Сухум).

Государственный язык: абхазский; русский язык, наряду с абхазским, признаётся языком государственных и других учреждений.

Законодательство о защите информации и персональных данных. В Республике Абхазия нет отдельных законов, регулирующих вопросы защиты информации и персональных данных.

Законом Республики Абхазия «О праве на доступ к информации» установлены отдель-

ные вопросы, касающиеся доступа к информации, основной целью которого является предоставление доступа к информации, обеспечение информационной открытости государства и осуществление общественного контроля за деятельностью органов государственной власти, иных государственных органов и организаций, органов местного самоуправления.

Основными принципами обеспечения прав на доступ к информации являются презумпция открытости и доступности информации; оперативность и своевременность предоставления информации; предоставление достоверной и полной информации; законность поиска, получения и передачи информации; защита права на доступ к информации.

При этом под защитой права на доступ к информации понимаются действия (бездействие) органов или организаций, их должностных лиц, нарушающие право на доступ к информации.

Отдельные вопросы персональных данных регулируются Законом Республики Абхазия «Об оказании государственных услуг». В частности, Законом установлено понятие персональных данных, к которым относятся документы или информация, представляемая в любой форме, подтверждающая личность гражданина либо иную информацию о нём, не запрещённую законодательством Республики Абхазия.

ЗАКЛЮЧЕНИЕ

Анализ законодательства Приднестровской Молдавской Республики, Республики Южная Осетия в области защиты информации, включая персональные данные, показывает, что по своему содержанию оно достаточно близко российским законам, регламентирующим аналогичные сферы. При этом существенным отличием является практика применения законодательства в каждой из стран, его восприятие обществом, готовность к исполнению.

Республика Абхазия имеет возможность, используя опыт различных стран, разработать законодательные акты, регулирующие вопросы защиты информации и персональных данных.

Надеемся, что данный обзор поможет не заблудиться в законодательстве стран СНГ-2. Мы постарались облегчить путь изучения и применения на практике нормативных законов и подзаконных актов в области ИБ.

«СТОИТ ВОООЩЕ ОТКАЗАТЬСЯ ОТ ИСПОЛЬЗОВАНИЯ ТЕРМИНА „ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ“»



СЕНАІ НЕ ОПРАВДЫВАЕТ ОЖИДАНИЙ.
ЧТО ЖДЁТ МИРОВУЮ ОТРАСЛЬ ИИ?

Пожалуй, только дети и неисправимые мечтатели ожидают от прихода нового календарного года неожиданных чудесных изменений. Однако, похоже, в области искусственного интеллекта случилось именно это — завершается история, за развитием которой следил буквально весь мир. Что приходит ей на смену? Об этом очередной разговор с Игорем Шереметом, академиком РАН.



Игорь ШЕРЕМЕТ
председатель
Научного совета РАН
«Информационная
безопасность», доктор
технических наук,
профессор, академик
РАН

— **Игорь Анатольевич, давайте подведём главные итоги развития мировой индустрии искусственного интеллекта (ИИ) в 2025 году. В первую очередь, что происходило с генеративным ИИ (GenAI), к которому, без сомнения, в последнее время приковано внимание как обывателей, так и профессионалов-математиков, а также государственных мужей в разных странах мира?**

— Конец 2025 года стал, без сомнения, знаковым периодом для мировой отрасли GenAI. Интересно, что целый ряд важных событий произошёл в 20-х числах ноября. Кратко перечислю их.

Во-первых, достоянием гласности стали экономические параметры компании OpenAI — мирового флагмана генеративного искусственного интеллекта: убыток за третий квартал 2025 г. — 11,5 млрд долл., выручка за первое полугодие — 4,3 млрд долл., то есть глубокий финансовый минус. И это при том, что затраты на создание дата-центров для поддержки больших языковых моделей (LLM) оцениваются на уровне 400 млрд долл. в год. Неудивительно, что ситуацию с этим строительством всё чаще стали называть «большим пузырьком искусственного интеллекта». Это второй знаковый момент в истории GenAI. Более того, сам Сэм Альтман, сооснователь и генеральный директор OpenAI, в интервью агентству Bloomberg 21 августа 2025 г. сказал: «Является ли искусственный интеллект пузырьком? Ответ положительный». Чуть позже Джеффри Безос, основатель интернет-компаний Amazon, создатель и владелец аэрокосмической компании Blue Origin, также подтвердил это мнение: «Искусственный интеллект — это своего рода промышленный пузырь».

Третий важный аспект — поведение крупнейших инвесторов в отношении развития GenAI. Так, в ноябре 2025 г. Питер Тиль, считающийся одним из самых грамотных, толковых и прибыльных инвесторов в сфере высоких технологий, продал свои акции компании NVidia. Напомню, что этот человек — инвестор таких компаний, как SpaceX, Airbnb и Spotify, а ещё учредитель широко известной в узких силовых кругах США компании Palantir, которая занимается технологиями интеллектуального анализа больших данных. Ну, и ещё Питер Тиль входит в круг серьёзных спонсоров американских консервативных политиков, в том числе президента США Дональда Трампа. Так вот, этот бизнесмен очень высокого полёта избавился от принадлежавших ему акций NVidia... Кстати, то же сделал SoftBank — одна из крупнейших в мире финансовых структур (японского происхождения), которая в течение многих лет и весьма успешно занимается инвестициями в высокие технологии. По сути, это ведущий банк во всём мире среди тех, кто занимается инвестициями в хайтек. То есть эти финансисты также посчитали, что инвестиции в Nvidia, связанные с ожиданием бурного роста индустрии дата-центров для LLM, больше не будут прибыльными.

ТОЧКА ПЕРЕЛОМА: НЕ ТОЛЬКО В БИЗНЕСЕ, НО И В ТЕХНОЛОГИЯХ GEN AI

— **С экономикой GenAI ситуация более-менее понятна. А что думают учёные-математики, которые с таким увлечением развивают технологии во всём мире?**

— Четвёртая группа знаковых событий в сфере GenAI как раз связана с именами самых видных профессионалов в этой области. Один из них — Илья Суцкевер. Тот самый Суцкевер, который вместе с Алексом Крижевски и будущим нобелевским лауреатом Джефффри Хинтоном опубликовал в 2012 г. статью ImageNet Classification with Deep Convolutional Neural Networks, которая сегодня входит в список самых цитируемых за всю историю науки. Там они описали нейросеть AlexNet, которая распознавала статические графические образы гораздо лучше других решений компьютерного зрения. Авторы

предложили свой оригинальный подход к анализу изображений на основе больших наборов данных, мощной вычислительной инфраструктуры на базе графических процессоров (GPU) и новой архитектуры нейросети. Именно эта модель обработки данных нейросетью положила начало эпохе глубокого машинного обучения (Deep Learning).

А в конце 2025 г. Суцкевер заявил в своих интервью и статьях, например, в журнале *Gerwin* в конце ноября, о том, что эпоха «масштабирования ИИ» (Age of Scaling), базирующаяся на простом наращивании вычислительных мощностей и объёмов данных, закончилась. Её сменяет новая «эпоха исследований» (Age of Research), наступает период фундаментальных исследований в области создания суперинтеллекта. Этим, собственно, и намерена заняться основанная им новая компания, которая так и называется — SSI, что означает Safe SuperIntelligence. И это будет не классическая коммерческая хайтек-компания, ориентированная на бизнес, а команда исследователей, сосредоточенная на развитии фундаментальной математической науки.

Масла в огонь подлил и Ян Лекун, ещё одна влиятельная фигура в мире генеративного ИИ, в недавнем прошлом — главный научный сотрудник компании Meta по искусственному интеллекту. С начала января он работает в основанной им новой компании Advanced Machine Intelligence Labs. Расставание с компанией Meta было достаточно громким и скандальным. В ноябре 2025 г. Лекун громко объявил о том, что LLM — это тупиковая ветвь искусственного интеллекта, он считает большие языковые модели принципиально ошибочными. Дальше последовали скандалы с манипулированием бенчмарками GenAI-моделей компании Meta, волна увольнений из подразделения ИИ, публичные взаимные обвинения Лекуна и Цукерберга.

Но, оказывается, проблемы накопились не только в компании Meta. Днём 24 ноября 2025 г. Сэм Альтман, глава OpenAI, разослал всем сотрудникам циркулярное письмо, в котором оповестил, что компанию ждут тяжёлые времена, возможно падение выручки до 10% в следующем году. Однако он призвал сотрудников не предаваться унынию, поскольку отныне OpenAI будет заниматься суперинтеллектом...

ОБЩИЙ ЗНАМЕНАТЕЛЬ — БУДУЩИЙ СУПЕРИНТЕЛЛЕКТ

— А что вместо GenAI?

— Интересно, что следующим этапом в развитии искусственного интеллекта по-

сле завершения «эпохи GenAI» все упомянутые профессионалы и бизнесмены от ИИ видят создание суперинтеллекта. Правда, у каждого из них — собственное представление о том, как этот суперинтеллект будет выглядеть.

Так, Илья Суцкевер (и его компания SSI) полагает, что суперинтеллектуальная программная система не только обладает энциклопедическими знаниями (это уже вроде бы достигнуто), но и способна «обучаться» новым знаниям в такой же манере, как это делает человек. С той лишь разницей, что у этой компьютерной системы не будет биологических ограничений в осваивании новых знаний и умений, свойственных мозгу человека. То есть она сможет бесконечно масштабироваться, но не в части вычислительной производительности, а в отношении «масштабирования знаний».

Компания Яна Лекуна Advanced Machine Intelligence Labs также делает ставку на дальнейшее развитие способностей компьютерной системы к обучению: она будет использовать не только тексты, но и другие типы данных (включая видео и пространственные данные) для того, чтобы понять, как устроен тот физический мир, в котором действует умная программная система. С этой целью такая система получит навыки самостоятельных рассуждений, планирования и анализа изменения данных во времени, а не в режиме диалога с человеком, как это происходит сегодня. Сам Ян Лекун называет этот подход продвинутым машинным интеллектом (Advanced Machine Intelligence, AMI), что отражено в названии компании.

Что именно подразумевает под будущим суперинтеллектом Марк Цукерберг, пока не раскрывается. Правда, можно сделать некоторое предположение, если учесть, что 24 ноября 2025 г. произошло ещё одно знаковое событие: президент США подписал указ о запуске проекта The Genesis Mission. Там он с присущим Дональду Трампу пафосом говорит о том, что Америка начинает новую эпоху в искусственном интеллекте. И те прорывы, которые планируется совершить в рамках этой инициативы, сопоставимы с Манхэттенским ядерным проектом.

— Как будут выглядеть эти прорывы в ИИ?

— Речь идёт о том, что будут получены прорывные результаты за счёт обучения того, что в указе называется domain-specific foundation models, то есть проблемно

ориентированных фундаментальных моделей. Эти модели будут обучаться на тех огромных наборах данных (датасетах), которые есть в распоряжении различных американских научных коллективов и сообществ. И в результате валом пойдут провалы и открытия...

То есть в американском Белом доме тоже понимают, что сегодняшний генеративный искусственный интеллект — это пузырь. Но публику нужно убеждать в победной траектории американских высоких технологий, а значит, нельзя допустить, чтобы этот пузырь лопнул у всех на глазах, и поддержать государственным финансированием. Очень похоже, что OpenAI уже нацелилась на этот «кусочек пирога», и Сэм Алтман в своём письме имел в виду именно тот суперинтеллект, который описан в проекте The Genesis Mission.

Кстати, можно уже наблюдать движение в данном направлении. В январе OpenAI объявила, что очередная версия их продукта ChatGPT решила несколько задач Эрдёша.

Напомню, что Пол Эрдёш — это талантливый «странствующий» математик венгерского происхождения. В пору своей активной научной деятельности во второй половине XX века он, подобно Давиду Гильберту в начале этого же века, сформулировал целый список математических проблем, которые в то время не поддавались решению учёных умов. И вот с осени 2025 г., в том числе в январе 2026 г., модели OpenAI начали находить решения математических проблем из этого списка Эрдёша. Видите, как всё красиво складывается?! Президент США 24 ноября 2025 г. подписал указ о создании суперинтеллекта, а уже к январю 2026 г. ChatGPT решил ряд фундаментальных проблем, над которыми безрезультатно бились лучшие умы человечества...

Тут и китайцы активизировались: опять-таки в ноябре 2025 г. компания DeepSeek представила свою модель DeepSeekMath-V2, которая ориентирована на решение сложных математических задач.

— Суперинтеллект The Genesis Mission в действии?

— Для непосвящённого человека это, действительно, может выглядеть как суперинтеллект: люди ведь не могли решить задачу, а нейросеть — смогла. Но на самом деле и DeepSeek, и ChatGPT — это не более чем инструменты, которые помогают в работе людям-математикам.

Если внимательно почитать текст указа о запуске The Genesis Mission, можно уви-

деть, что речь там идёт, во-первых, об огромном инфраструктурном проекте American Science and Security Platform — не случайно его исполнителем назначено Министерство энергетики США. Это министерство должно создать экспериментальную платформу искусственного интеллекта. Она объединит в единую сеть суперкомпьютеры национальных лабораторий, квантовые и другие экспериментальные установки, облачные среды для ИИ-решений, а также соберёт вместе массивы научных данных в рамках единой системы совместных научных исследований. На основе этой платформы будут создаваться и функционировать различные инструменты цифрового моделирования, теоретические модели из разных областей науки, будет обеспечиваться многоуровневый доступ к данным.

В списке промышленных партнёров проекта мы видим знакомые имена: Nvidia, AMD, Dell, HPE, Oracle, а также крупных провайдеров облачных сервисов и разработчиков GenAI, например, компанию Anthropic со своим продуктом — семейством LLM чат-ботов Claude.

В качестве приоритетных направлений прорывных исследований с помощью данной платформы названы: энергетика, материаловедение, биотехнологии, квантовые технологии, микроэлектроника и ядерные установки.

ДВИЖЕНИЕ К СУПЕРИНТЕЛЛЕКТУ ПО-АМЕРИКАНСКИ

— Сегодня ИИ преподносится публике как некая сверхидея любого развитого современного государства. Однако похоже, что в разных странах мира эта сверхидея понимается по-разному. Например, наш российский подход, который декларируется на высоких уровнях, предполагает в конечном итоге создание интеллектуальной цифровой экономики. А для США ИИ — это скорее инструмент обеспечения глобального влияния. А Вы как это видите?

— Что касается связки «США и ИИ», здесь нужно принимать во внимание несколько моментов. Прежде всего, безусловно, мериток — это одна из основ американского менталитета. Лозунг Make America Great Again — это оттуда. И в проекте The Genesis Mission все задачи нацелены на глобальное доминирование США в области ИИ: они начинаются с укрепления национальной безопасности, обеспечения энергетического превосходства, повышения производительности



труда и уходят в технологическое превосходство Америки и её глобальное стратегическое лидерство. Как говорится, написано чёрным по белому. Это определяет другие отличительные черты реализации сверхидеи США в области ИИ.

Для одной из этих черт у меня есть отличное название — термин, который я встретил в одной из публикаций: «рекламный балаган Альтмана». В самом деле, этот балаган на тему GenAI реально накрыл планету Земля! Иначе нельзя: мир должен верить в мессианскую идею глобального превосходства американского ИИ. И поэтому продолжается поток публикаций о том, что то одна, то другая GenAI-модель решила неразрешимую ранее проблему математики и т.п. И это вторая отличительная особенность движения США в области ИИ.

И, несмотря на то что Ян Лекун громко заявляет: «LLM — это тупиковая ветвь искусственного интеллекта», а Илья Суцкевер призывает заканчивать с бесконечным масштабированием LLM и соответствующим наращиванием количества GPU в дата-центрах, этот развесёлый пиар продолжается. Сэм Альтман, руководитель OpenAI: «Мы построим центр обработки данных на 10 ГВт!»

«А мы построим дата-центр на 5 ГВт!» — вторит ему Марк Цукерберг. Это третья отличительная особенность развития ИИ в США: позиции руководителей бизнеса и ведущих учёных могут быть диаметрально противоположными.

— **Как же они совмещаются в головах людей?**

— Всё достаточно просто. Бизнес в США — это отдельная история, уходящая корнями в рыночное саморегулирование. И возможности интеллектуальной обработки данных каждая компания использует как хочет. Но вот незадача — бизнеса на GenAI не получилось. Поставщики GenAI-услуг не смогли предложить рынку ни одного такого суперсервиса, который смог бы обеспечить возврат тех огромных инвестиций, что уже вложены в инфраструктуру LLM. И они не появятся, это сегодня уже понятно: бизнес не смог получить от GenAI никакого нового качества: сотрудник тратит время не на собственную работу по подготовке нужного документа, а на проверку той чуши, которую ему выдаёт чат-бот... В результате корпоративный спрос на сервисы LLM практически сошёл на нет: 95% корпоративных пользователей отказываются от них. И именно эти сервисы относятся к генеративному искусственному интеллекту и завершающемуся этапу развития ИИ, в отличие от следующей ступени — суперинтеллекта, где ИИ-инструментами будут пользоваться учёные и нести в остальной мир новые прорывные технологии и услуги. Теперь миру будут «продавать» следующий блестящий фантик — The Genesis Mission, «Манхэттенский проект» в сфере ИИ...

— **А что Вы скажете о только что объявленном намерении И. Маска создать орбитальный дата-центр из миллиона спутников?**

— Маску очень хочется стать первым в истории человечества триллионером... А если серьёзно, то это опять-таки вложения в инфраструктуру ИИ. То есть еще больший пузырь... Я не обсуждаю великое множество технических проблем, которые предстоит решить для достижения этой сверхамбициозной цели уровня «Звездных войн» Рейгана. Здесь приходят на ум слова нашего замечательного телеведущего Н. Н. Дроздова: «Давайте не будем им мешать и просто понаблюдаем за ними»... Не увидим ли мы за орбитальным дата-центром уши упомянутых «Звездных войн», только

на новой системотехнической и технологической основе?

А ЧТО У НАС?

— Кстати, Министерство энергетики Российской Федерации также озабочено созданием новых энергетических мощностей для центров обработки данных, где должны запускаться ИИ-решения. Этому вопросу недавно было посвящено специальное заседание Совета Федерации «Актуальные вопросы развития российских вычислительных мощностей». Там замминистра энергетики России Пётр Конюшенко сообщил, что до 2030 г. необходимо создать дополнительные энергопотребности для обслуживания задач ИИ на уровне 2–2,5 ГВт, и далее они должны наращиваться приблизительно на 20% ежегодно. И под эгидой Минэнерго РФ уже создана соответствующая рабочая группа, куда вошли представители госвласти, энергетических и хайтек-компаний.

— Знаете, я наблюдаю за тем, что происходит в области GenAI в нашей стране и мире, со смешанным чувством. С одной стороны, приятно, что всё, что я говорил в предыдущих интервью, сбывается. С другой стороны, я слышу разговоры о том, что надо выделить триллионы рублей на строительство новых электростанций, которые будут питать новые грандиозные центры обработки данных, начинённые мириадами графических процессоров, которые реализуют сервисы LLM.

И это несмотря на то, что ТАМ технологии генеративного ИИ списываются в утиль: в указе Launching The Genesis Mission аббревиатура LLM не встречается ни разу! Там есть domain specific foundation models (DSFM). Но это вовсе не domain specific LLM! Любая (!) фундаментальная математическая модель, разработанная для той или иной предметной области, может относиться к множеству DSFM. Мы по привычке, укоренившейся с 90-х годов прошлого века, наступаем на те же грабли, с которых Америка уже уходит, и выступаем промоутерами тупикового технологического направления...

В каком-то недавно опубликованном рейтинге степени внедрения искусственного интеллекта, который, надо полагать, формировался из цифр степени охвата населения стран LLM-чат-ботами, Россия находится где-то в районе 160-го места. По-моему, ниже Кении. Поверьте, это показатель не

отсталости, а здравомыслия! И нам совсем не надо стремиться обогнать Кению, как в стайерском забеге на 10 километров.

Я поддерживаю обеими руками то, что говорят у нас на высоком уровне про создание интеллектуального фундамента передовой цифровой экономики России, про умную роботизацию отечественной промышленности и т.п. Именно сюда надо бы направлять триллионы рублей, а не в «прожорливые» дата-центры для GenAI и электростанции, обеспечивающие их электропитание и охлаждение.

— Надо сказать, что существенная ограниченность GenAI понятна и российским специалистам в GenAI. Подводя итоги 2025 года, они отмечают, что в части реальных практических применений можно говорить только лишь о создании некоторых кусочков кода.

— К сожалению, понятна эта ограниченность далеко не всем. И у нас наблюдается расслоение как специалистов, так и лиц, принимающих решения, на здравомыслящих и продолжателей хайпа GenAI. И вторых ещё немало, даже в научной среде. «Давайте поручим искусственному интеллекту рецензирование научных статей, направляемых в журналы» — это один из реальных примеров. Есть деятели науки, которые всерьёз считают, что некий сервис GenAI обладает более широкими и глубокими знаниями, чем авторы статей. Значит, ему можно поручить и сами исследования? Ведь написание новых статей — это всего лишь оформление результатов исследований...

ДВИЖЕНИЕ К СУПЕРИНТЕЛЛЕКТУ ПО-КИТАЙСКИ

— А как обстоит дело с реализацией сверхидеи ИИ в Китае? Вы ведь регулярно бываете там и располагаете соответствующей информацией?

— Знаете, недавно я прочитал интересную статью на эту тему. И там встретилась фраза, которая мне очень понравилась: «Между генерированием слов и деланием дел — большая разница». Речь идёт о том, что объёмы производства промышленных роботов в Китае превышают американские показатели в разы. Американцы, которые занимаются тем самым «генерированием слов» посредством LLM, вряд ли смогут догнать по уровню развития китайские роботизированные производства. В этом они сами признаются после посещения производственных компаний в Китае.



Китай отличается комплексный подход к внедрению технологий ИИ (именно разных технологий ИИ, а не GenAI!). На современном этапе этого процесса наибольшее внимание уделяется киберфизическому промышленному производству, поскольку оно составляет основу конкурентоспособности КНР в мировой экономике. В декабре прошлого года я принимал участие в международной конференции, которая состоялась в Харбине. Вообще-то она была посвящена достаточно узкопрофессиональной теме — интеллектуальному интернету вещей (AI IoT). Но рассуждения экспертов можно описать так: наступает эпоха Post LLM AI, как нужно действовать?

И под эту большую текущую цель — создание китайской промышленности на основе AI IoT — подбираются наилучшие методы и технологии, включая передовые достижения в цифровизации управления. Все самые передовые технологии формирования управленческих решений и организации функционирования больших социотехнических систем там, естественно, реализуются. И всё это делается без какого-либо хайпа и громких публичных заявлений. Мне это известно, поскольку по роду деятельности приглашённого

профессора Харбинского политехнического университета я достаточно хорошо ориентируюсь в происходящих процессах.

— **То есть китайские товарищи прагматично относятся к технологиям и инструментам ИИ?**

— Предельно прагматично, здраво и спокойно. И это видно, в частности, в результатах развития оборонного комплекса и вооружённых Сил КНР. Я присутствовал 3 сентября 2025 г. в Пекине на военном параде в честь 80-летия победы над Японией и окончания Второй мировой войны. В числе приглашённых лиц наблюдал парад с трибуны дипкорпуса и видел очень близко всю военную технику, которая участвовала в параде. Это была наглядная демонстрация плодов спокойно-го, рационального проектирования поступательного развития такого большого современного государства, как Китай.

Там действительно нет того самого «генерирования слов», но есть «делание дел».

О РИСКАХ СВЕРХИНТЕЛЛЕКТА

— **Фанаты GenAI любят повторять страшилки о том, что генеративный ИИ, который уже разрешает математические проблемы, неподвластные человеческому уму, вот-вот перехватит управление над человечеством.**

— Если Вы верите тому, что сообщает ChatGPT, значит, он уже управляет Вами. И страшилка, которую Вы описали, — это реальность, а не потенциальный риск. Пусть человек на своём рабочем месте, скажем, управленца среднего звена должен создать некий документ. И он строит свою работу на информации, которую получает от ChatGPT. Затем отправляет готовый документ своему начальнику, а он тоже первым делом обращается к ChatGPT. В результате всё приходит к человеку-исполнителю, который должен точно выполнить всё, о чём сказано в документе, имеющем для него силу приказа. Кто в этой истории управляет целыми рабочими процессами? ChatGPT, пресловутый генеративный искусственный интеллект.

И как тут не вспомнить статистику самой компании OpenAI: до 27% ответов ChatGPT — это галлюцинации. Вдумайтесь только! 27%! Мы в технических системах бьёмся за две девятки, три девятки после запятой, а тут 27%, и это нисколько не смущает апологетов передачи управления генеративному ИИ. Кстати, сам Сэм Альтман запретил использовать ChatGPT в медицинских и юридических услугах: сервис, дескать, не даёт меди-

цинских и правовых рекомендаций, а просто ведёт беседы о здоровье и правовых аспектах. Стало быть, глава OpenAI что-то знает насчёт того, что ChatGPT на самом деле никакой не интеллект, а статистический аппроксиматор речи.

— **Однако в середине января появилась новость о том, что нейросеть Grok от Илона Маска официально станет частью военной платформы GenAI.mil, создаваемой для Министерства войны США. Все 3 миллиона сотрудников Пентагона всех уровней будут объединены в единый контур мониторинга и управления на основе некоторой «нейростратегии». А есть ещё критические технические системы: атомные электростанции, нефтехимические предприятия со своими рисками промышленных катастроф. Как это согласуется с 27% галлюцинаций?**

— Это уже просто конец человечества. Полагаю, что людей, которые в нынешнее время в разных странах настроены принимать решения по продвижению, финансированию и развитию такого рода средств, нужно переориентировать на осмысленные подходы к интеллектуализации таких чувствительных государственных сфер, как госуправление, вооружённые силы, промышленность. Иначе человечество получит техносферу, которая в кратчайшие сроки принесёт ему столько проблем, что поставит его на грань выживания.

— **Но ведь человечество давно занимается вопросами безопасности в критически важных сферах?**

— Да, это так. Но мы всегда работали в классической парадигме информационной безопасности. Есть корректно функционирующая система, спроектированная на основе адекватных математических и естественнонаучных моделей, которая в отсутствие деструктивных внешних воздействий не то что не является источником угроз используемому ее социуму, но содействует ему в решении стоящих перед ним задач - для этого она и создавалась. Разрабатываемые механизмы и средства нейтрализации упомянутых воздействий направлены на исключение возможности некорректного функционирования системы вследствие деятельности потенциальных злоумышленников (нарушителей). Однако то, что система при отсутствии таковых работает разумно и не во вред пользователям, сомнению не подвергается. И когда кибербезопасники говорят о доверенном

(trusted) искусственном интеллекте, то имеют в виду защищенность средств ИИ от деструктивных воздействий на эти средства (а также на их инфраструктуру и обучающие датасеты) на этапах их создания (разработки) и эксплуатации. При этом опять-таки модели и методы, реализуемые указанными средствами, считаются безупречными - «жена цезаря вне подозрений».

В случае LLM ситуация принципиально иная: система спроектирована на основе ущербной теоретической модели и поэтому сама по себе служит источником угроз в глобальном масштабе, хотя авторы ChatGPT, DeepSeek, BERT, Claude, Gemini, Qwen и т.д., вне всякого сомнения, не являются злоумышленниками в смысле упомянутой классической парадигмы, а наоборот, движимы благородной идеей - принести людям ощутимую пользу. Такое положение дел настойчиво требует от нас расширения области понятия «доверенный ИИ» на упомянутые модели и методы. Об этом же говорил мне не так давно президент РАН Г. Я. Красников. И, следуя его рекомендации, мы будем осознанно расширять сферу ответственности нашего научного совета «Информационная безопасность», в который входят специалисты всех отделений РАН, что создает благоприятные исходные условия для рассмотрения вопросов адекватности моделей и методов ИИ применительно к самым разным приложениям.

С другой стороны, одно из направлений деятельности нашего совета - информационно-психологическая безопасность. Число судебных исков к OpenAI растёт, в том числе в связи с психическими заболеваниями и даже суицидами после длительного общения с ChatGPT. Но и это не самое главное. Важно видеть очевидное: человечество никогда не было так легко манипулируемо! Рекламный балаган Альтмана привёл к тому, что аудитория ChatGPT уже достигла 800 миллионов человек. Представьте себе эту цифру: 800 миллионов людей, которые доверяют этому сервису решение своих задач! И они не только рисуют с помощью GenAI картинки для личных telegram-каналов. Они, например, разрабатывают клоны ChatGPT, помогающие писать диссертации и при этом обходить механизмы контроля Диссернет. И не только не понимают, что наносят вред российской науке, но ещё и гордо заявляют об этом, рассылая пресс-релизы. Потому что, с их точки зрения, они создали суперинтеллект, способный создавать тексты диссертаций. Сотрудникам «Диссернет» приходится срочно браться за дело и учиться отлавли-

вать и такие «результаты жизнедеятельности» GenAI.

А сколько студентов используют эти инструменты для изготовления курсовых работ, дипломов? Думаю, эта цифра гораздо ближе к 100%, чем к 0%... Ещё раз хочется повторить мысль из статьи китайского автора: давайте делать дела, а не генерировать слова.

ЖИЗНЬ ПОСЛЕ GENAI: КАК ЕЁ ОРГАНИЗОВАТЬ?

— Давайте... Как Вы полагаете, что стало главной причиной неудачной истории GenAI? Может быть, была сделана ставка не на ту математическую «лошадку»? Впрочем, нейросетевое направление само по себе продолжает развиваться, регулярно появляются новые достижения, скажем, в области видеоаналитики.

— Как всегда, причин несколько. Одна связана с терминологией. На мой взгляд, стоит вообще отказаться от использования термина «искусственный интеллект», поскольку он открывает широчайшие возможности для всевозможных словесных манипуляций и дезориентации человечества. В рамках бытовой, повседневной логики искусственный интеллект — это что-то типа искусственной кожи, то есть тоже человеческий мозг, только сделанный из другого материала.

История с LLM прекрасно нам показала: неадекватные модели приводят к неадекватным результатам. Мы стремимся сделать нечто, подобное природе, и на этом пути создаем множество теоретических и практических моделей, причем, каждая из них природоподобна по-своему и в своей степени адекватна реальному объекту (явлению). Помните, как в фильме Андрея Тарковского «Андрей Рублёв» монах приделал себе крылья и сиганул с колокольни? И пока летел, размахивал этими крыльями и радостно кричал: «Лечу!» И был в этот момент подобен птице — субъекту природы. А с другой стороны, самолёт — он тоже природоподобен, по-своему реализует функцию перемещения по воздуху. А планер — по-своему. А дирижабль — по-своему....

В этом смысле и систолические структуры, и клеточные автоматы природоподобны. И те, и другие — структуры с массовым параллелизмом, как, кстати, и нейросеть. Но начиная с модели перцептрона Розенблатта, считается, что именно модель нейрона МакКаллока-Питтса 1943 года лучше всего описывает то, как реально устроен и функционирует человеческий мозг. А это очень примитивное представление: нейрон есть пороговый эле-

мент, который срабатывает по результатам взвешенного суммирования по всем его входам. Физиологи сегодня говорят о совершенно иных принципах функционирования человеческого мозга, согласно которым нейрон — это весьма нетривиальный компьютер, а функции памяти реализуются глиальными клетками.

Плюс к этому идея, положенная в основу технологии LLM, — тоже очень примитивная: предсказание следующего слова, исходя из предыдущих. Но даже этот примитивный механизм можно было реализовать на любой другой математической и технологической базе, и это могло быть дешевле и эффективнее, но почему-то используется модель нейросети МакКаллока — Питтса, реализация которой приводит к дата-центрам с миллионами графических процессоров. То есть получилось, что на один примитивный подход наложили другой, тоже крайне примитивный, а в результате получили то, что получили... Насколько я понимаю, именно это Джеффри Хинтон пытался объяснить своим молодым коллегам, но это ему не удалось. И в 2023 году он покинул Google. А в 2024-м стал нобелиатом....

— То есть нужны иные математические основания для создания интеллектуальных систем?

— Нужно разрабатывать технологии, ориентированные на те задачи, решение которых мы хотим получить от компьютерных систем. Именно под целевую задачу нужно создавать модель представления знаний, а затем под неё конструировать соответствующую компьютерную архитектуру, которая, в числе прочего, обеспечит минимизацию избыточного перебора при наличии комбинаторных задач. И вот тогда, возможно, мы придём в научных исследованиях к лучшему пониманию того, как работает человеческий мозг.

— А на практическом уровне разработок ИИ от чего следует отталкиваться?

— Как минимум вместо термина «искусственный интеллект» (Artificial Intelligence, AI) использовать более работоспособные и корректные термины: HI (Human Intelligence, человеческий интеллект) и CI (Computer Intelligence, компьютерный интеллект). Мне очень нравится термин «ассистивный», иногда употребляемый в сочетании с «ИИ». Ассистивный, то есть помогающий, содействующий, ИИ-ассистент. А это и есть CI. В рамках такого подхода работу интерактивной интеллектуальной системы можно

представить как взаимодействие человеческого интеллекта, который при необходимости формулирует конкретные задачи, и компьютерного интеллекта, который их решает. Естественно, ИИ постоянно обучает СИ (в последнее время среди специалистов по ИИ получил хождение термин *Learning-on-the-Job*, то есть обучение в процессе работы). И в этом случае удастся избавиться от плутоватого хайпа на тему того, что некая GenAI-модель решила ещё одну проблему Эрдёша. Потому что будет очевидно: проблему решал человек, используя СИ в качестве инструмента реализации некоторых функций, которые ИИ несвойственны. И устроители «рекламных балаганов» перестанут дурачить непосвящённых людей, ставя знак равенства между ИИ и СИ, поскольку будет очевидно: Computer Intelligence по своей структуре, алгоритму функционирования и способам реализации вовсе не претендует на то, чтобы имитировать человеческий интеллект. А служит надёжным и эффективным помощником в решении сложных интеллектуальных задач.

Вот такое сочетание человеческого и компьютерного интеллекта и есть, собственно, суперинтеллект, состоящий из двух гармонично сотрудничающих компонентов: Human Intelligence и Computer Intelligence.

О ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ COMPUTER INTELLIGENCE

— С этой точки зрения какие технологические основы, на ваш взгляд, наилучшим образом подходят для создания Computer Intelligence? Вряд ли стоит говорить только о классическом ИИ, тем более что он тоже появился на свет не вчера, по возрасту недалеко ушёл от модели нейрона МакКаллока — Питтса...

— В моём понимании все задачи, которые традиционно относились к сфере исследования операций, экономической комбинаторике, — это и есть Computer Intelligence. Потому что человеческому мозгу в принципе не под силу поиск наилучшего решения в большом пространстве решений. Но человек выступает в тандеме с СИ как коуч, который, предварительно обучив СИ логике поиска решений, формулирует для него комбинаторные задачи.

Отличный пример такого подхода — SIEM-системы в кибербезопасности, которые обеспечивают распознавание кибератак на максимально ранних стадиях их подготовки. Здесь мы видим правильное сочетание человеческого и компьютерного интеллекта: человек закладывает в систему некие умо-

заклучения (причинно-следственные связи), которые позволяют распознавать признаки готовящихся или уже осуществляемых кибератак. А компьютерный интеллект реализует это распознавание в соответствии с теми знаниями, которые он получил от коуча.

В принципе, приблизительно то же самое делает и учёный, занимающийся своим исследованием: формирует цель и логику мысленного эксперимента, а компьютер этот эксперимент реализует, то есть, в конечном итоге, помогает перебирать миллиарды возможных ситуаций и предоставлять результаты перебора, которые удовлетворяют критериям, заданным ученым-организатором эксперимента. Только в этом случае задача исследователя иного уровня — добытие новых знаний.

— Вы упомянули, что один из основополагающих элементов разработки сверхинтеллекта, понимаемого как сочетание Human Intelligence и Computer Intelligence, — это создание модели представления знаний, отвечающей поставленной задаче в её актуальной постановке и с учётом всех известных рисков. На какие наработки прошлого имеет смысл опираться? Системный анализ, исследование операций или только классический логический искусственный интеллект?

— В моём понимании, исследование операций — это одна из наиболее полезных и глубоко разработанных областей применения компьютерного интеллекта. Хотя этот вид математики никогда не причисляли к ИИ в силу того, что там не было логического вывода в явном виде, на самом деле он там есть. Просто те учёные, которые разрабатывали, например, симплекс-метод, задачи исследования операций формулировали, не обращаясь к формализмам математической логики. Только и всего. А на самом деле это один из частных случаев решения комплекса логических задач, которые объединены единственной целью — оптимизация при ограничениях. По сути, это один из языков для решения задач оптимизации в условиях ограничений, который оперирует привычными математическими объектами: векторами и матрицами. В отличие от того ИИ, который реализуется в ранних экспертных системах и называется слабым. А слабый он лишь потому, что оперирует высказываниями, некими вербальными конструкциями, которые могут и не иметь прямого отображения в виде математических объектов.

Но и там, и там есть аксиоматика — правила вывода, применение которых обеспечивает построение новых объектов, начиная от аксиомы, соответствующей исходным данным, — и в итоге получение решения задачи, если оно существует. И все они составляют пространство Computer Intelligence, где есть сегменты и исследования операций, и системного анализа, и много других научных направлений. В частности, популярная сегодня технология мультиагентных систем, которая, впрочем, известна с 80-х годов прошлого века. Но все это, подчеркну еще раз, базируется на своих специфических моделях представления знаний. Как бы странно ни прозвучало, но, в частности, языки дифференциального исчисления и представления химических реакций — именно такие модели. А их фундаментом в конечном итоге является математическая логика, на которую опирается инженерия знаний как область исследований и практической деятельности, направленная на создание и применение эффективных средств CI и интерфейсов HI-CI.

— Итак, любая модель представления знаний непосредственно связана с решаемой задачей. Давайте возьмём для примера задачу интеллектуального управления цифровой экономикой страны. Что можно взять из прошлого научного опыта, а что нужно создавать впервые?

— Чудес не бывает! Нужно создавать проблемно ориентированный CI, предназначенный для решения экономических задач. При этом, как мы уже выяснили, есть полезный вариант компьютерного интеллекта, который называется исследованием операций. Но изначально этот математический аппарат был создан на архаичной матрично-векторной основе с сопутствующими ограничениями, в первую очередь в части размерности матриц. Разрабатывая новую модель представления знаний для решения сложных задач предсказательного моделирования и управления в больших социотехнических системах — мультимножественные грамматики и метаграмматики — я как раз и пытался совместить в одном инструментарии достоинства исследования операций и инженерии знаний.

— Что достигается в результате?

— В рамках одной модели представления знаний может работать и инженер на конкретном объекте, и математик из профильного НИИ, занимающийся макроэкономическими исследованиями.

Поскольку все решаемые задачи описываются в системе понятий предметной области, больше не нужно возиться с огромными матрицами. Скажем, нужно произвести пять автомобилей, четыре самолёта и два корабля, и далее все изделия раскрываются — опять же в терминах производства — до уровня самого последнего чипа в бортовой системе управления. База знаний, наряду с этим, включает сведения о возможных производителях каждого конкретного изделия (субэлемента, компонента), стоимостных и временных параметрах их производственных циклов, текущей и перспективной загрузке, а также о текущем состоянии ресурсной базы системы. А система логического вывода, или интерпретатор знаний (inference engine), обеспечивает построение рационального плана работы системы по выполнению заказа и движения финансовых средств в пределах кооперации. Этот план в современной экономической терминологии есть не что иное, как смарт-контракт.

Рациональность предложенного подхода подтверждается его применимостью не только к экономическим, но и к естественнонаучным задачам (например, из области инженерии химических реакций), что делает его основой для создания истинно интеллектуальных систем сквозного планирования деятельности больших производственных систем — от «руды» до сбыта высокотехнологичной готовой продукции на основе доступной логистической инфраструктуры.

— Получается современный инструмент моделирования народно-хозяйственных процессов?

— Нет, это не только моделирование. Моделирование здесь — не самоцель, а средство. Это средство планирования функционирования любой социотехнической системы: есть цель, ресурсы, и система построит маршрут достижения этой цели с учётом имеющихся ресурсов. А опора на данные реально имеющихся ресурсов даёт возможность реализовать ситуационное реагирование на воздействие разного рода непредсказуемых внешних факторов.

Собственно, это то, что в экономической теории называется программно-целевым планированием с обратной связью. Но на базе проблемно ориентированного Computer Intelligence для области экономики актуализация базы знаний и пересчёт ресурсов, планов, процессов осуществляется весьма оперативно. То есть трудоёмкость тех действий, которые сегодня называются обучением ис-



кусственного интеллекта и являются критической точкой ИИ, при таком подходе может быть радикально уменьшена.

А это значит, что Computer Intelligence действительно становится реальным помощником Human Intelligence, опираясь при этом на точные, верифицированные, юридически значимые данные и знания о том, что происходит с субъектами экономики. В этом контексте мне очень импонирует активность руководителя фонда «Кристалл роста» А. С. Галушки, который предпринимает серьезные усилия по воссозданию в современных российских

реалиях и на новой технологической основе процессов программно-целевого планирования в нашей стране. Возможно, на пересечении этих двух потоков интеллектуальной энергии — «Кристалла роста» и моей — возникнет синергия, которая и обеспечит давно ожидаемый рывок России в светлое будущее

— **Суперинтеллект в действии?**

— Не будем вступать в гонку броских лозунгов. Надежный и эффективный компьютерный интеллект для решения социально значимых задач.

Вопросы задавала
Елена Покатаева

kaspersky активируй
будущее



Защита организации
от сложных и целевых
атак

Kaspersky Anti Targeted Attack

с модулем NDR

ДиалОгНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

ПРОРЫВ К СОВРЕМЕННОЙ МАТЕМАТИКЕ

ТРУДНЫЙ ПУТЬ ОТ «НИКТО ПОЧТИ НИЧЕГО НЕ ПОНЯЛ» К «ЭТО СОЧИНЕНИЕ ДОСТАВИТ ВАМ ИСКЛЮЧИТЕЛЬНОЕ НАСЛАЖДЕНИЕ»



**Борис
СТОЛПАКОВ**
историк
криптографии

200 лет назад, 11 (23) февраля 1826 года, на Учёном совете Императорского Казанского университета состоялся доклад Николая Ивановича Лобачевского «Сжатое изложение начал геометрии». Ныне, много лет спустя, рядовое, казалось бы, событие оценивается иначе.

Эту дату в научном мире принято считать временем рождения неевклидовой геометрии. Немало и приверженцев того мнения, что именно так впервые заявила о себе современная математика.

«МЫ НЕ УШЛИ В ЭТОМ ВОПРОСЕ ДАЛЬШЕ, ЧЕМ ЕВКЛИД»

Аксиома о параллельных прямых известна нам со школы: в плоскости через точку, лежащую вне прямой, можно провести лишь единственную прямую, параллельную данной. Её ввёл Евклид, хотя прежде он пытался доказать её справедливость как теоремы. Да и современникам Лобачевского эта аксиома не давала покоя. Так, Ламберт искал теоремы, справедливые без её использования, а Лежандр при многочисленных переизданиях своего учебника геометрии всякий раз делал новую попытку доказательства аксиомы о параллельных и позже обнаруживал ошибку.

Итожа эти труды, Гаусс (1777–1855) писал: «В области математики найдётся мало вещей, о которых было бы написано так много, как о проблеме в начале геометрии при обосновании теории параллельных линий... И всё же, если мы хотим говорить честно и открыто, то нужно сказать, что, по существу, за 2000 лет мы не ушли в этом вопросе дальше, чем Евклид».

В 23 ГОДА — ПРОФЕССОР

Н. И. Лобачевский (1792–1856), молодой и даровитый профессор математики, читавший студентам Казанского университета курс геометрии, вероятно, особенно внимательно прорабатывал все материалы, готовясь к лекциям. Представим себе этого молодого человека. В 23 года — профессор, в 27 лет — декан физико-математического факультета, в 34 — ректор университета. Николай Иванович учился и трудился в то время, когда складывалась и пожинала первые плоды российская система образования. Да он и сам был её плодом. Сначала его воспитывали в недавно созданной Казанской гимназии, затем он поступил в только что открывшийся Казанский университет. Там в числе его педагогов был и М. Бартельс, друг и учитель К. Гаусса.

Сменив Бартельса на посту декана в 1820 году, Лобачевский по-прежнему много преподавал. Один из его лекционных курсов назывался «Элементарная геометрия с высшей точки зрения». В 1823 году Лобачевский представил свои лекции в печать, но они остались неопубликованными. Академик П. Н. Фусс, правнук Л. Эйлера, дал тогда отрицательный отзыв, указав на чрезмерный отход от Евклидовой традиции. Бартельс, к которому Лобачевский обратился за советом, тоже не поддержал его новшества.

НОВАЯ ГЕОМЕТРИЯ И ОБНОВЛЕНИЕ УНИВЕРСИТЕТА

Как мы знаем, Лобачевский постепенно уверился в недоказуемости аксиомы о параллельных, но на этом не остановился. Следующим его шагом стало развитие теории, основанной на всех аксиомах Евклидовой геометрии, кроме постулата о параллельных, который он заменил на его отрицание: «Через каждую точку плоскости, не лежащую на прямой, можно провести по крайней мере две прямые, не пересекающие данной прямой». Разумеется, в новой геометрии сразу обнаружились факты, совершенно непривычные для восприятия. Например, сумма углов любого треугольника меньше 180 градусов. Поэтому, когда Лобачевский в феврале 1826 года выступил с докладом на Учёном совете университета со своей «воображаемой геометрией», естественной реакцией большинства присутствовавших были молчание и недоумённый вопрос: «зачем всё это?»



Иллюстрация 1. Портрет Н. И. Лобачевского

Впрочем, административный и общий авторитет Лобачевского были так высоки, что уже в 1827 году тайным голосованием его избрали ректором университета и затем переизбирали на новый срок шесть раз. Именно при Лобачевском Казанский университет был заново отстроен, хорошо оснащён и превратился в украшение центральной части Казани (илл. 2).

«Я РАЗДЕЛЯЮ ТЕ ЖЕ ВЗГЛЯДЫ»

Добиваясь понимания своих идей, Лобачевский развивал теорию неевклидовой геометрии и одновременно пытался чётко и систематично излагать достигнутые результаты в России и за рубежом. Первый его доклад отдельно не был опубликован, но вошёл в «Мемуар о началах геометрии», напечатанный в «Казанском вестнике» в 1829–1830 гг. В 1835 г. вышла отдельным изданием «Воображаемая геометрия» (илл. 3), вскоре напечатанная в Берлине на французском языке. В 1840 году Лобачевский опубликовал на немецком языке свою книгу «Геометрические исследования по теории параллельных», два её экземпляра получил Гаусс – «король математиков». В письме своему другу и ученику астроному Г. Шумахеру Гаусс высоко оценил труд Лобачевского: «Вы знаете, что уже 54 года я разделяю те же взгляды; таким образом, я не нашёл для себя в сочинении Лобачевского ничего фактически нового. Но в развитии предмета автор следовал не по тому пути, по которому шёл я сам; оно выполнено Лобачевским мастерски, в истинно геометрическом духе. Я считаю себя обязанным обратить Ваше внимание на это сочинение, которое, наверное, доставит Вам совершенно исключительное наслаждение».



Иллюстрация 2. Университет в Казани. Гравюра 1832г.



Иллюстрация 3. Издание «Воображаемой геометрии», 1835 г.

Но, несмотря на все попытки, без ясного ответа оставались два важных вопроса: как доказать непротиворечивость представленной теории? какую пользу может принести новая геометрия? Ответов не знал даже Гаусс.

В петербургском журнале «Сын отечества» в 1834 году отметили: «Для чего же писать, да ещё и печатать, такие нелепые фантазии? <...> Если не учёность, то по крайней мере здравый смысл должен иметь каждый учитель, а в новой геометрии нередко недостаёт и сего последнего. <...> Новая геометрия написана так, что никто из читавших её почти ничего не понял».

ДОЛГІЙ ПУТЬ К ПРИЗНАНИЮ

На похоронах Лобачевского в 1856 г., воздавая ему должное как замечательному администратору, учёному и человеку, никто не упомянул о его неевклидовой геометрии, считая её плодом больного воображения. Ведь даже такой крупный математик, как академик М. В. Остроградский, ученик О. Коши, отозвался о первом изложении новой геометрии в 1826 г. на французском языке следующим образом: «Книга господина ректора Лобачевского опорочена ошибкой, она не заслуживает внимания».

Действительно, очень трудно было воспринять «воображаемую геометрию» Лобачевского, настолько противоречила попытка отказа от аксиомы о парал-

лельных устоявшимся представлениям о допустимом в геометрии. Кроме того, непротиворечивость новой геометрии не была убедительно обоснована. Поэтому удивительно упорство Лобачевского в отстаивании своих выводов. Даже великий Гаусс не решился обнародовать свои мысли, во многом сходные с идеями Лобачевского, и запрещал другим что-либо публиковать по этим вопросам. Лобачевскому он не написал ни слова, но в 1842 г. по предложению Гаусса Лобачевский был избран членом-корреспондентом Гёттингенского учёного общества.

Полное признание и широкую известность геометрия Лобачевского получила через 12 лет после его смерти. В 1868 г. итальянский математик Э. Бельтрами в своём мемуаре «Опыт толкования неевклидовой геометрии» показал, что геометрия Лобачевского столь же непротиворечива, как геометрия Евклида. Появились и её наглядные модели.

Признание геометрии Лобачевского пришло к его столетнему юбилею, а в 1895 г. Петербургская Академия наук учредила международную премию его имени, в 1896 г. в Казани ему установили памятник.

ВРЕМЯ ПРОРЫВА

Теперь нам привычно, что математика XIX столетия заметно отличается от математики предыдущих веков. С той поры новые математические теории стали возникать не только в результате непосредственных запросов естествознания или техники, но также из внутренних потребностей самой математики. Примером такой теории и явилась «воображаемая геометрия» Лобачевского.

По мнению А. Н. Колмогорова, в XIX веке произошла перестройка всего склада математического мышления. Если прежде, например, введение в употребление отрицательных или комплексных чисел и точная формулировка правил действий с ними требовали длительной работы, то теперь математики сознательно и свободно стали создавать новые числовые и геометрические системы, новые «алгебры» и т.д. Поэтому с идейной стороны так значимо среди математических открытий XIX века появление неевклидовой геометрии Лобачевского.

Физика, естествознание тоже предъявляли свои запросы к математике. Отметим здесь, что крупнейший французский математик А. Пуанкаре (1854–1912), формулируя в 1897 г. математические задачи для первоочередного решения, связал их с двумя основными, по его мнению, проблемами: «Создать математическую основу для квантовой физики и для теории относительности».

ПЕРЕСТРОЙКА РАСШИРЯЕТСЯ

К концу XIX века сложился и современный стандарт требований к логической строгости. И этот стандарт существенно использовал развитую к тому времени теорию множеств Г. Кантора. Аппарат и



Иллюстрация 4. Д. Гильберт

результаты теории множеств оказались очень удобными для систематизации математических знаний, но рассмотрение бесконечных множеств вызвало много протестов. Ещё Аристотель различал потенциально бесконечные множества, то есть множества, которые можно неограниченно достраивать, и актуально бесконечные множества, то есть множества «в готовом виде»: «Бесконечное имеет потенциальное существование... Актуально бесконечное не существует». Против актуальной бесконечности выступали Коши и Гаусс, Гаусс писал: «В математике бесконечную величину нельзя использовать как нечто окончательное. Бесконечность — не более чем манера выражаться, означающая предел».

По мнению А. Пуанкаре: «Грядущие поколения будут рассматривать теорию множеств как болезнь, от которой они излечились». У немецкого математика Д. Гильберта было иное отношение: «Никто не изгонит нас из рая, созданного Кантором».

К концу XIX века многим казалось, что возможности математики как важнейшего инструмента естествознания не ограничены. На волне такого энтузиазма в 1898 г. в Цюрихе состоялся первый математический конгресс. А уже спустя два года в Париже собрался второй Международный конгресс математиков. С докладом «Математические проблемы» выступил Д. Гильберт (1862–1943) (илл. 4).

Доклад Гильберта — уникальное явление в истории: ни до него, ни после математики не выступали с научными сообщениями, охватывавшими проблемы математики в целом. В докладе Гильберт говорил о целостном характере математики как основе всего точного естествознания и представил свой основной тезис — о разрешимости в широком смысле слова всякой математической задачи.

ПРОБЛЕМЫ ГИЛЬБЕРТА

Далее он сформулировал 23 проблемы, начиная с теории множеств и обоснования математики: «1. Проблема Кантора о мощности континуума. 2. Непротиворечивость арифметических аксиом».

Первая проблема — это проверка континуум-гипотезы Кантора: мощность континуума (то есть множества всех вещественных чисел) есть первая мощность, превосходящая мощность множества всех натуральных чисел.

Затем Гильберт перешёл к геометрии, теории чисел, алгебре и завершил своё изложение проблемами задачами анализа.

В начале прошлого века учёный мир с энтузиазмом воспринял предложенную программу исследований. Правда, уже скоро неожиданно возникли новые проблемы. А именно: обнаружились парадоксы, связанные с теорией множеств. Так, в 1902 г. английский философ и математик Б. Рассел обнаружил парадокс, основанный на самом определении множества.

Как известно, парадокс Рассела разнообразно популяризировали уже в начале XX столетия. Особенно распространённая форма была предложена самим Расселом в 1919 г.: «один деревенский брадобрей объявил, что он бреет тех и только тех жителей деревни, которые не бреются сами». Бреет ли он себя? Попробуем рассуждать логично. Если бреет, то, согласно его словам, себя не может брить, то есть не бреет; если не бреет, то, опять по его же словам, должен брить, то есть бреет. Таким образом, бреет тогда и только тогда, когда не бреет. Иными словами: и бреет, и не бреет.

ЗАДАЧА: ПРЕОДОЛЕТЬ КРИЗИС!

Попытка выхода из наметившегося кризиса с помощью ограничения теоретико-множественных методов исторически привела к возникновению новой области математики — алгоритмической теории и практики.

Гильберт тоже предложил программу выхода из кризиса. Она состояла из двух частей. Первая часть заключалась в формализации арифметики, анализа и теории множеств. Предполагалось создать особый символический язык, на котором математические утверждения записывались бы формулами, положить в основу математики некоторое множество аксиом-формул и указать правила вывода одних утверждений-формул из других. Во второй части программы предполагалось доказать непротиворечивость построенного формального исчисления, то есть невозможность вывода в нём какого-либо утверждения вместе с его отрицанием. При этом требовалось, чтобы все рассуждения, используемые для доказательства непротиворечивости, носили настолько элементарный характер, что их правильность не вызывала бы сомнений.

Программа Гильберта и его энергичная деятельность дали мощный толчок развитию формальных логико-математических теорий. Казалось, успех был близок. Для арифметики оставалось: 1 — показать, что в рамках формализованной арифметики можно сформулировать и доказать все утверждения классической арифметики; 2 — доказать непротиворечивость созданной теории.

НЕОЖИДАННЫЕ РЕЗУЛЬТАТЫ

Как теперь известно, обе эти задачи оказались невыполнимыми в принципе. Уже в 1931 г. появилась работа молодого австрийского математика Курта Гёделя (1906–1978), в которой содержались две теоремы, получившие общее название теоремы Гёделя о неполноте. Гёдель доказал, что если формальная система арифметики непротиворечива, то она не полна, то есть в ней существует утверждение-формула, которую нельзя ни доказать, ни опровергнуть в данной системе. При этом Гёдель доказал неполноту гильбертовой формальной системы, то есть обнаружил внутри системы ряд «неразрешимых» проблем — одной из них как раз и оказалась проблема непротиворечивости. Тем самым Гёдель продемонстрировал неосуществимость первой и второй частей программы Гильберта. Заодно был получен ответ на вторую проблему Гильберта (о непротиворечивости арифметических аксиом).

Гёдель внёс важный вклад в решение и первой проблемы Гильберта (проблема Кантора о мощности континуума). В 1935 г. он доказал, что континуум-гипотеза не может быть опровергнута средствами теории множеств. Окончательный ответ был получен в 1963 г. американским математиком Полом Козеном. Он сумел доказать, что и отрицание континуум-гипотезы невозможно опровергнуть теоретико-множественными средствами; то есть континуум-гипотезу невозможно ни доказать, ни опровергнуть. При этом мало кто сомневается в её справедливости. Впрочем, как и в том, что через точку плоскости, не лежащую на заданной прямой, можно провести лишь единственную прямую, параллельную заданной. Хотя математики утверждают, что мы живём в пространстве Лобачевского.

«ЕСЛИ БЫ НЕ БЫЛО ТЕОРЕМЫ ГЁДЕЛЯ...»

Отметим, что, по мнению некоторых математиков, в математической среде присутствует какое-то сожаление о несостоявшейся полной формализации математики. Так, П. Козэн однажды высказался следующим образом: «Если бы не было теоремы Гёделя, то жизнь была бы приятнее».

Возражая ему, другой известный математик, академик Российской академии наук Алексей Николаевич Паршин, написал в своей статье

«Размышления над теоремой Гёделя»: «Если бы не было теоремы Гёделя, жизнь не только не была бы приятнее, её просто бы не было».

Итак, далеко не всё в математике подвластно формализму и логике, то есть рациональному мышлению. Поразительная эффективность математики как инструмента естествознания тоже вряд ли будет когда-нибудь рационально объяснена.

«ТОЛЬКО МАТЕМАТИКА СУМЕЛА СТРОГО ДОКАЗАТЬ, ЧТО ОСНОВАНА НА ВЕРЕ»

Интересные исследования психологии математического творчества проводили в разное время такие корифеи, как Пуанкаре и Адамар. Оба они отмечали, что одним из наиболее фундаментальных, внелогических компонентов открытия в математике является так называемая вспышка озарения. Это ощущение знакомо и многим из нас, достаточно вспомнить наше обучение езде на велосипеде. При первых детских попытках езды на велосипеде мы никак не могли понять, как же можно сохранить равновесие и не упасть. Но в какой-то момент это понимание неожиданно приходило к нам, и мы уже легко катились на велосипеде, даже не задумываясь о равновесии.

По мнению А. Н. Паршина, и теорема Гёделя говорит о каком-то фундаментальном, глубинном свойстве мышления и, может быть, жизни вообще. Он также предположил, что в биологии должен быть верным факт, подобный теореме Гёделя. А именно: этот факт должен показывать невозможность полного описания живых организмов в чисто генетических терминах.

В связи с теоремой Гёделя приведём ещё интересную мысль, высказанную в статье «Непротиворечивость и полнота» из математического журнала *American Mathematical Monthly* 1956 года. По мнению её автора, до теоремы Гёделя все научные дисциплины, кроме математики, следовало бы признать основанными в той или степени на вере, независимо от того, чем эта вера вызвана. Одна математика представлялась строго формальной наукой. Теперь же после обнаружения утверждений, недоступных ни доказательствам, ни опровержениям, оказалось, что и математика основана на вере. Хотя по-прежнему она занимает особое положение среди научных дисциплин. Ведь только математика сумела строго доказать, что основана на вере.

Заметим, что провал в обосновании математики мало кого смущает, гораздо важнее поразительная эффективность математических методов в познании природы. Математика по-прежнему современна и многообещающа.

ЦВЕТЫ ДЛЯ АНИ

Продолжаем публиковать футуристические рассказы (или фельетоны) Андрея Жаркевича на актуальные темы. Сегодняшнее произведение иллюстрирует материал автора в традиционной рубрике «Социальная инженерия» на стр. 65.

У Ани был день рождения, и Серёжа хотел купить ей цветы. Казалось бы, что может быть проще. Они встречались три месяца, она любила пионы, он знал магазин на Покровке, где их продавали. Задача для первоклассника.

Но первоклассники не жили в 2027 году.

Цветочный на Покровке закрылся ещё весной — не прошёл сертификацию по новому регламенту «О допустимых эмоциональных триггерах в розничной торговле». Владелец, говорят, теперь работает консультантом по озеленению в муниципальном парке. Там триггеры одобренные.

Серёжа открыл приложение «ГосБукет» — единственный легальный агрегатор цветов в радиусе МКАД.

«Выберите повод», — предложил интерфейс.

Варианты: День Победы, День народного единства, День семьи, любви и верности, выписка из роддома, похороны (расширенный пакет).

Дня рождения в списке не было. Серёжа ткнул в «Другое».

«Укажите причину покупки (для персонализированной рекомендации и корректного налогообложения)».

Он набрал: «День рождения девушки».

Система думала секунд пятнадцать. Потом выдала:

«Статус отношений с получателем не подтверждён. Для покупки подарков категории „Романтика“ необходимо верифицировать союз через портал „ГосОтношения“. Хотите начать процедуру?»

Серёжа вздохнул и нажал «Да».

Портал «ГосОтношения» запустили два года назад — для упорядочивания демографической статистики. Идея была простая: если государство знает, кто с кем встречается, оно может точнее прогнозировать рождаемость и распределять льготы.

На практике это означало анкету на сорок страниц.

«Дата начала отношений (приблизительно)».

«Количество совместных ночёвок за последний месяц».

«Планируете ли вы совместное проживание в течение ближайшего года?»

«Есть ли у вас разногласия по политическим вопросам? Если да, кто из партнёров придерживается более патриотичной позиции?»

Серёжа добрался до двадцать третьей страницы и остановился на вопросе: «Опишите ваши чувства к партнёру (минимум 200 символов, использование иностранных слов снижает рейтинг заявки)».

Он написал: «Я её люблю».

Система выплюнула красное: «Недостаточный объём. Минимум 200 символов».

Он дописал: «Очень сильно».

«186 символов. Добавьте описание».

«Она смеётся, и у меня внутри что-то происходит. Не знаю, как это назвать. Просто хочу быть рядом».

«247 символов. Принято. Внимание: фраза „не знаю, как это назвать“ может указывать на эмоциональную незрелость. Рекомендован курс „Осознанные чувства“ (бесплатно для рейтинга выше 700)».

Серёжа закрыл приложение.

Аня работала дизайнером — вернее, «специалистом по визуальной гармонизации контента». Раньше она рисовала логотипы и иллюстрации для разных клиентов. Теперь — только для тех, кто в реестре одобренных заказчиков.

Список заказчиков обновлялся каждый вторник. В прошлый вторник из него пропала сеть кофеен, где Аня делала меню. Причина — владелец оказался «лицом с неоднозначной лояльностью» (перевёл пятьсот рублей фонду помощи бездомным животным, а фонд оказался связан с организацией, которая оказалась связана с человеком, который когда-то лайкнул что-то не то).

Аня осталась без проекта. Её рейтинг упал на пять баллов — «косвенное содействие неблагоприятным структурам».

— Я просто рисовала им чашки с паром, — сказала она Серёже по телефону. — Чашки. С паром.

— Пар — это же водяной конденсат, — мрачно пошутил он. — Облака. Облака бывают над разными странами. Возможно, над недружественными.

Она засмеялась. Он услышал, как на её стороне пискнул браслет.

Потом Серёжа чуть было не купил цветы у бабки возле метро.

Бабка сидела на перевёрнутом ящике, перед ней — ведро с астрами. Откуда астры в ноябре — загадка. Но бабки возле метро существовали вне системы: слишком старые для браслетов («медицинские противопоказания»), слишком бедные для цифровых кошельков («льготная категория, переходный период»).

— Сколько? — спросил Серёжа.

— Триста, — сказала бабка.

Он протянул браслет. Бабка посмотрела на него как на идиота.

— Сынок. Триста рублей. Деньги.

— У меня нет наличных.

— Тогда иди откуда пришёл.

Серёжа стоял и смотрел на астры. Фиолетовые, лохматые, неправильные. Аня любила пионы, но пионы были летом, а астры — сейчас. Живые. Настоящие.

— Подождите, — сказал он. — Я найду.

Наличные нашлись у коллеги Паши. Паша был странным: ездил на работу на велосипеде («экономия на углеродном лимите»), носил механические часы («не отслеживают пульс»), иногда расплачивался бумажками, которые доставал из носка.

— Триста? — переспросил Паша. — Легко. Но завтра вернёшь пятьсот. Цифрой.

— Это же грабёж.

— Это рынок, Серёженька. Свободный. Помнишь такое слово?

Серёжа не помнил.

Он взял три мятые сотни и побежал к метро.

Бабки уже не было. Вместо неё стоял молодой человек в форме — «Контроль торговли в неустановленных местах».

— Гражданин, вы что-то ищете?

— Нет. Просто... гулял.

Контролёр посмотрел на него с подозрением. Потом — на браслет.

— Ваш пульс повышен. Всё в порядке?

— Опаздываю на свидание.

— Свидание зарегистрировано в системе?

— Мы... в процессе.

Контролёр кивнул. Видимо, «в процессе» было знакомым статусом.

— Хорошего вечера. Не нарушайте.

Аня открыла дверь и увидела Серёжу — без цветов, без подарка, с красным лицом и бешеным пульсом.

— Ты чего?

— Я хотел купить тебе цветы, — сказал он. — Но для этого нужно было зарегистрировать отношения, описать чувства в двести символов, найти наличные у Паши, добежать до бабки, но бабку забрали, и вот.



Аня смотрела на него молча.

— В общем, — закончил он. — С днём рождения. Подарок — это я.

Она засмеялась. Он засмеялся. Два браслета синхронно мигнули.

«Зафиксирован совместный смех. Возможно: начало романтических отношений. Рекомендация: зарегистрируйте союз для получения налоговых льгот».

Аня сняла браслет и положила на тумбочку экраном вниз.

— Заходи, — сказала она. — У меня есть торт. Нелегальный. Подруга испекла. Без сертификата. Серёжа переступил порог.

Где-то в дата-центре система отметила, что гражданин Сергеев С. А. провёл в квартире гражданки Морозовой А. И. четыре часа семнадцать минут. Статус отношений: неопределённый. Рекомендация: повторный запрос через 14 дней.

Но система не знала, что торт был с вишней. Что они смотрели старый добрый и очень романтичный фильм с ноутбука через VPN, купленный у того же Паши. Что Аня положила голову Серёже на плечо и сказала: «Спасибо, что пытался».

Система много чего не знала.

И это, пожалуй, было единственной хорошей новостью.

декабрь 2025

ВСЕ ЮЗВЕРИ РАВНЫ, НО НЕКОТОРЫЕ РАВНЕЕ

ЗАМЕТКИ БЕЗОПАСНИКА



Александр ИГОНИН
эксперт BIS Journal,
ведущий рубрики

Сегодняшняя заметка навеяна парочкой свежих инцидентов, попавших на радар вашего покорного слуги. Первый – копирование ИТ-подрядчиком большого массива данных из корпоративной БД на рабочий ноутбук (вероятно, безо всякого злого умысла). Второй – несанкционированная установка специалистом техподдержки на свой ПК программы для удалённого администрирования, доступ к которой, похоже, каким-то образом «утёк» за пределы организации. Предлагаю читателям взять полминуты

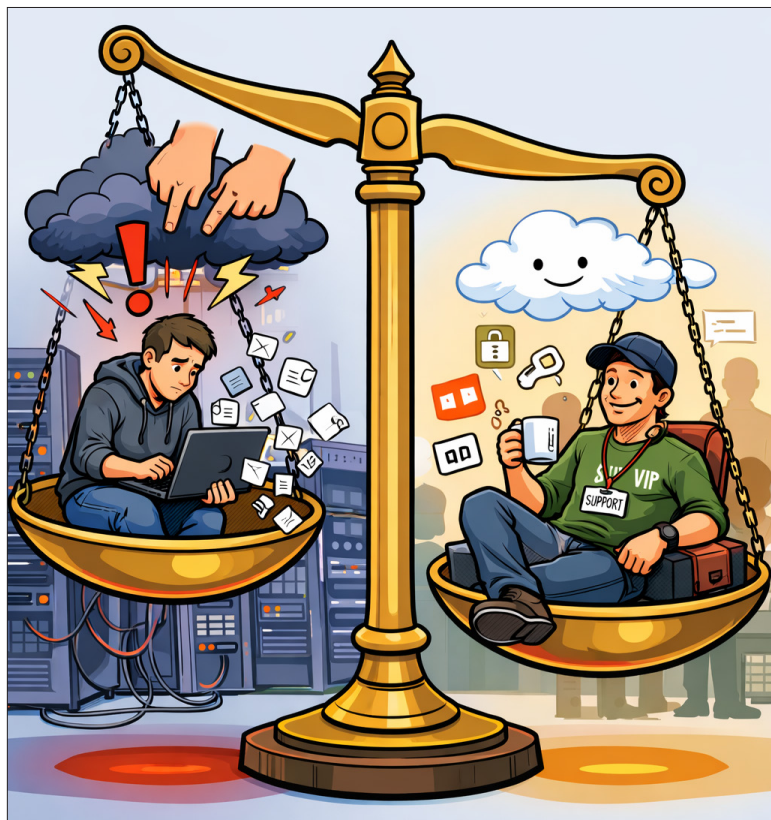
на раздумья и решить, что из этого серьёзнее и какие меры вы бы приняли к сотрудникам в описанных ситуациях. Проверим, сойдутся ли ваши предсказания с корпоративной реальностью.

Итак, в первом случае специалист получил очень жёсткий (чуть ли не до крика) выговор, с привлечением менеджмента и всех кар небесных. Думаю, я на месте бедолаги как минимум месяц боялся бы компьютер даже включать. Даже просто в розетку. С другой стороны, персонажа из второй истории лишь добродушно пожурили, и всё. Откуда же такая разница в подходах? А разгадка проста: «герой» второй истории – это ИТ-специалист, выделенный для поддержки VIP-пользователей, и все-рьёз его отчитывать просто побоялись из-за его потенциальных знакомств.

А вот ещё одна история: в ней ИБшники обнаружили в интернете информацию о внутреннем API компании и пошли предъявлять претензии подрядчику, отвечавшему за разработку этого API. Тот стал разбираться и достоверно выяснил, что утечку допустил не он, а (бывает же!) сотрудник самой команды ИБ. Получился буквально оживший анекдот о самой главной вещи в ходе любого расследования. Дело очень быстро спустили на тормозах...

Причины такой разной реакции вроде бы понятны: спорить с начальством и его приближёнными зачастую просто неразумно, выносить мусор из своей избы (точнее, его там подметать) – неприятно и утомительно. Но должен сказать, что мне как технарю наблюдать за подобным довольно грустно. Злоумышленникам всё равно, чья ошибка или оплошность открыла им ворота в периметр. Более того: если она допущена сотрудником ИБ или высокопривилегированным сотрудником ИТ, ущерб может даже увеличиться.

Какой из всего этого я бы сделал вывод? Политики безопасности в организации должны применяться как законы в по-настоящему правовом государстве: одинаково для всех, с минимумом необходимых исключений. Очень жаль, что и в бытовой, и в корпоративной жизни этот постулат часто не работает, тогда как конечная цена такого беззакония может быть очень и очень велика. Давайте будем стремиться к политике ИБ равной, не кровожадной, но применяемой одинаково ко всем, включая самих себя. И даже в первую очередь – самих себя.





ФОРУМ

РОССИЯ 20²⁶

15 17

сентября



XXIV

**международная
конференция**
по проблематике
инфраструктуры
открытых ключей
и электронной
подписи

г. Санкт-Петербург
Отель «Коринтия»



pki-forum.ru



Kaspersky
Security для
почтовых серверов

KSMS Plus — расширенный уровень защиты корпоративной почты

kaspersky активируй
будущее

