BIS JOURNAL

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА

№2 (61) 2026

Герман КЛИМЕНКО
Фонд развития цифровой экономики
«Цифра – она как кукушонок!» → 39

Юрий ШАБАЛИН
Swordfish Security
Как защитить ИИ-решения? → 38

ГосСОПКА — всё под контролем!
→ 5

Защита данных. В эпоху Zero Trust → 46

РБПО. Триаж секретов → 78

Алексей МАРТЫНЦЕВ
Норильский никель
«След атаки ведет в ловушку» → 5

Сергей ЛЕБЕДЬ
Сбер
«Сбер плюс ГосСОПКА – удар по фишингу!» → 6

Роман ШАПИРО
АО «Почта России»
«Не ждите проверок – инициируйте диалог» → 8

PKI 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

Сергей ПАЗИЗИН
научный редактор
BIS Journal

14–15 апреля 2026 года состоится долгожданное событие — в Москве в кластере «Ломоносов» пройдет Форум ГосСОПКА, организованный Национальным координационным центром по компьютерным инцидентам, посвященный тематике обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

В условиях продолжающейся фрагментации мировой экономики и нарастающего противостояния в киберпространстве рассчитываем, что данный форум станет не только площадкой для освещения вопросов противодействия компьютерным атакам, но также будет способствовать эффективному взаимодействию между регуляторами, ИБ-компаниями и субъектами критической информационной инфраструктуры.

«Противодействие кибератакам» — основная тема этого номера. Также в журнале представлена наша постоянная рубрика «Разработка безопасного ПО» и тема «Защита данных», включая вопросы идентификации и аутентификации, организации управления учетными записями и доступом к данным.

В интервью номера с Германом Клименко рассматриваем острые вопросы перехода к цифровой экономике в сфере управления, поднимаем проблемы замены человека машинами. В отдельной статье анализируем зарубежный опыт регулирования сферы информационной безопасности, включая тему безопасности «искусственного интеллекта».

В репортаже нашего обозревателя мы знакомим читателей с публичной информацией о ходе работы над новой Доктриной информационной безопасности Российской Федерации. Со времени утверждения действующей доктрины в 2016 году произошли значительные технологические, политические и экономические изменения. Предпринимаемые в отношении России попытки технологической изоляции требуют скоординированных, максимально эффективных и активных действий с целью достижения независимости в вопросах обеспечения функционирования и безопасности критической инфраструктуры. Каждый из компонентов классической триады — люди, процессы и технологии — критически важен для обеспечения информационной безопасности государства и должен получить соответствующие скоординированные планы развития.

BIS JOURNAL
ИЗДАЁТСЯ С 2010 ГОДА

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 (Роскомнадзором) как «BIS Journal — Информационная безопасность банков».

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

Подписан в печать 27.03.2026. Тираж 7000 экз.
Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

 16+

АКТУАЛЬНОЕ ИНТЕРВЬЮ

5 Алексей Мартынцев (Норникель)
«Взаимодействие с ГосСОПКА интегрировано в ИБ „Норникеля“»

6 Сергей Лебедь (Сбер)
«Объединение технологических возможностей Сбера и административного ресурса ГосСОПКА было бы полезно для защиты российских организаций от фишинга»

8 Роман Шапиро (Почта России)
«Не ждите проверок — инициируйте диалог»

ТЕМА НОМЕРА — ПРОТИВОДЕЙСТВИЕ КИБЕРАТАКАМ

10 Андрей Курило (ФБК, FBK Cyber Security)
Приоритеты защиты

14 Алексей Батюк (Positive Technologies)
Киберполигоны и непрерывная киберустойчивость

16 Иван Прохоров (Positive Technologies)
Почему компании со зрелыми системами ИБ всё равно теряют деньги из-за киберинцидентов

ТЕМА НОМЕРА — ПРОТИВОДЕЙСТВИЕ КИБЕРАТАКАМ

19 Василий Севостьянов (Доктор Веб)
По горячим следам

22 Даниил Бориславский (Контур.Эгида)
Простые шаги в верном направлении

26 Павел Пугач (СёрчИнформ)
Не стать долгостроем

28 Илья Одинцов (NCR Softlab)
SIEM вместо IRP

29 Роман Душков (Security Vision)
Security Vision AM, КИИ и ГосСОПКА

32 Николай Омланд, Максим Ильин (SolidLab Group)
Как не стать плацдармом для атак на цепочку поставок

34 **Кого и как атаковали в 2025 году**

38 Юрий Шабалин (Swordfish Security)
Appsec.AIGate

ИНТЕРВЬЮ НОМЕРА

39 **Цифровая экономика**
Герман Клименко (Фонд развития цифровой экономики)
«Цифра – она как кукушонок!»

ТЕМА НОМЕРА 2 — ЗАЩИТА ДАННЫХ

46 Илья Ткаченко (эксперт ИБ)
Всё на виду

50 Иван Писаренко, Сергей Попов (ВТБ)
Для чего нужны и как работают ID-провайдеры

53 Андрей Тархов (Актив)
Инфраструктура доверия

56 Евгений Бражников (Platform V IDM)
Сквозная идентификация пользователей

58 Андрей Арефьев (ГК InfoWatch)
Смотреть на данные через настройки и политики — это все равно, что наблюдать мир в замочную скважину

62 Николай Казанцев (SECURITM)
Управляйте процессами ИБ — экономьте время и деньги бизнеса!

РЕГУЛЯТОРЫ

64 **Парад законов**
Екатерина Рачкова (BIS Journal)
Квартальный отчёт

66 **Доктрина ИБ**
Усам Оздемиров (BIS Journal)
Продукт эволюции

69 **За рубежом**
Александр Першин (АРСИБ)
Ключевые структуры

РАЗРАБОТКА БЕЗОПАСНОГО ПО

78 **Процессы**
Александр Гадай (Swordfish Security)
Как организовать эффективный процесс безопасной разработки с подрядчиком

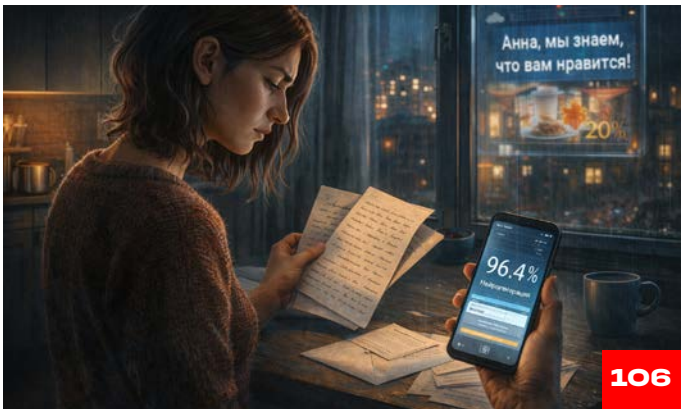
80 **Безопасность кода**
Дмитрий Ключников (CodeScoring)
Современная защита цепочки поставок

83 **Безопасность кода**
Александр Демидович (НПО «Эшелон»)
Триаж секретов

86 **Инструменты**
Антон Михайлов (SASTAV),
Дмитрий Поливанов (ДиалогНаука)
Принцип GIGO

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

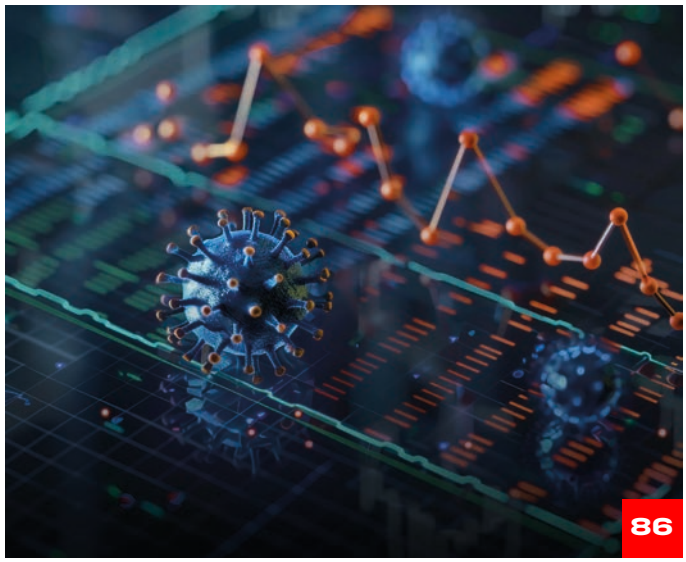
88 **ГосСОПКА**
Андрей Жаркевич (Start X)
ГосСОПКА и люди



106

ЗА РУБЕЖОМ

93 **Законодательство**
Александр Виноградов (ФГУП «ЦНИИХМ»),
Сергей Меньшиков (Belarusian InfoSecurity Community),
Андрей Ситнов (независимый эксперт), Наталья Казанцева (независимый эксперт)
Монголия


86

96

СУБЪЕКТЫ

96 **История**
Борис Столпаков (историк криптографии)
«От государственного канцлера графа Румянцева на благое просвещение»

102 **Лица ИБ**
Вероника Горячева
«Предпочитаю живых экспертов...»

106 **Рассказ**
Андрей Жаркевич
96,4 процента

108 **Заметки безопасника**
Александр Игонин (BIS Journal)
Зараза оптимизма? Так точно!

«ВЗАИМОДЕЙСТВИЕ С ГОССОПКА ИНТЕГРИРОВАНО В ИБ „НОРНИКЕЛЯ“»

Алексей МАРТЫНЦЕВ
директор департамента защиты информации и ИТ-инфраструктуры, Норильский Никель

— Алексей Сергеевич, расскажите, пожалуйста, о вашем опыте взаимодействия с ГосСОПКА?

— Взаимодействие с ГосСОПКА интегрировано в процесс реагирования на инциденты информационной безопасности «Норникеля». Мы реализовали возможность автоматизированного обмена информацией через Security Orchestration, Automation and Response (SOAR), а также проводим анализ поступающей к нам информации. Со всеми регуляторами в сфере информационной безопасности (ИБ) мы стараемся выстраивать партнерские взаимоотношения: уверены, что в конечном итоге это положительно скажется на отрасли в целом. Кроме того, на площадке Клуба «Безопасность информации в промышленности» (основанного «Норникелем» в 2017 году) мы регулярно обсуждаем особенности и нюансы обмена информацией через платформу ГосСОПКА, стараясь направить накопленную экспертизу на повышение эффективности взаимодействия бизнеса и государства.

— Что необходимо реализовать в первую очередь для эффективного решения задачи выявления компьютерных атак на начальном этапе?

— Чтобы решать эту задачу действительно эффективно, нужна выстроенная комплексная система информационной безопасности. У крупных компаний на это уйдут годы работы. Мы начали наш путь с определения элементов базовой защиты, т.е. процессов и систем безопасности, которые должны работать абсолютно везде: полное покрытие антивирусом, единые точки выхода в Интернет, анти-спам защита, контроль внешнего периметра. Далее последовало внедрение продвинутых средств защиты и сервисов ИБ, основанное на риск-ориентированном подходе. Такие средства защиты информации (СЗИ) в силу высокой стоимости или сложности реализации/поддержки целесообразно использовать только там, где они нужнее всего. Ну и, конечно, не обойтись без аудитов, проверок, практических тестирований, повышения осведомлённости — чтобы быть уверенными, что выявление атак работает не только на блок-схемах, но и в реальных условиях.

— Почему важно не только отражать атаки, но и проводить их анализ?

— Все очевидно: отраженная автоматизированными средствами атака — это хорошо, но это ничего не меняет для киберустойчивости вашей компании. А проведенный анализ и принятые меры могут эту устойчивость повысить. Давайте порассуждаем на бытовом примере: вы приходите домой и видите, что дверь в квартиру пытались вскрыть. Вряд ли просто порадуетесь тому, что попытка взломщиков оказалась неудачной, откроете дверь и как ни в чем не бывало продолжите жить в этой квартире. В голове сразу возникнет множество вопросов: «почему ко мне?», «как попали на территорию?», «что искали?», «а что, если бы удалось взломать дверь?» и т.д. Аналогичные вопросы следует задавать себе и про компьютерные атаки. Сложность в том, что таких автоматически отражённых атак на крупные российские организации — тысячи в день. Тут стоит определиться с подходом к процессу: что мы пытаемся выяснить, можем ли укрупнять информацию в тренды, все ли атаки стоит анализировать или можно договориться об определенных параметрах.

— Для чего необходим обмен информацией о компьютерных атаках?

— У этого процесса довольно много положительных эффектов: сокращение времени на реагирование, снижение объёма трудозатрат аналитиков Security Operations Center (SOC), более полная картина угрозы. Конечно, обмен информацией и ее анализ тоже требуют немалых ресурсов. Именно поэтому стоит дифференцировать процесс обмена: для общей массы компьютерных атак достаточно обмена техническими индикаторами компрометации — хешами файлов, IP-адресами, доменами. Однако в случае полноценных реализовавшихся компьютерных инцидентов гораздо важнее понимать тактики и инструментарий атакующих, векторы реализованных угроз и применяемую методологию. Обмен такой информацией позволит не только обнаружить следы атаки, но и выстроить проактивную защиту от аналогичных угроз. Таким образом, обмен сведениями об атаках нужен, чтобы максимально оперативно и эффективно использовать эту информацию для повышения защищенности всей отрасли.

«ОБЪЕДИНЕНИЕ ТЕХНОЛОГИЧЕСКИХ ВОЗМОЖНОСТЕЙ СБЕРА И АДМИНИСТРАТИВНОГО РЕСУРСА ГОССОПКА БЫЛО БЫ ПОЛЕЗНО ДЛЯ ЗАЩИТЫ РОССИЙСКИХ ОРГАНИЗАЦИЙ ОТ ФИШИНГА»

Сергей ЛЕБЕДЬ
вице-президент по кибербезопасности Сбера

— Сергей Васильевич, что, на ваш взгляд, структурно представляет собой фишинговая атака?

— Сегодня фишинговая атака — это многоступенчатая операция, структурно состоящая из сбора информации, создания инфраструктуры для атаки, доставки вредоносного контента и эксплуатации человеческого фактора. По сути, это настоящее социально-инженерное кибероружие.

В рамках модели Kill Chain фишинговая атака разделяется на этапы: разведка (Reconnaissance), подготовка (Weaponization), доставка (Delivery) с использованием различных каналов (электронная почта, мессенджеры или SMS), эксплуатация (Exploitation) и действия по достижению цели (Actions on objectives). Анализ фишинговой атаки в разрезе модели Kill Chain помогает понять последовательность действий злоумышленника, выявить проблемные зоны в защите, на которые необходимо обратить внимание, и выработать меры противодействия.

— Что необходимо сделать для повышения эффективности противодействия фишингу в отношении организаций?

— Чтобы системно и эффективно противодействовать фишингу, необходимо развивать взаимодействие всех заинтересованных структур: операторы связи, банки и другие организации. Необходимо активное подключение соответствующих государственных структур, которые будут координировать действия участников и вырабатывать общие правила. Ключевую роль, на мой взгляд, в этом взаимодействии должны играть регуляторы: НКЦКИ, Роскомнадзор. Важно усовершенствовать нормативно-правовую базу, чтобы проактивно выявлять и блокировать вредоносные ресурсы, а также привлекать к ответственности тех, кто их создаёт и распространяет.

Отдельное большое направление работы — обучение сотрудников организаций основам цифровой гигиены. Повышение осведомлённости снижает риск, что сотрудник станет жертвой фишинга, а значит, поставит под удар свою организацию.

Подробнее вопросы противодействия фишингу будут обсуждаться на пленарной сессии «Роль ГосСОПКА в противодействии преступлениям, совершаемым с использованием ИКТ» на Форуме «ГосСОПКА 2026». Приглашаю всех заинтересованных экспертов стать гостями сессии, на которой я буду выступать в роли модератора.

— Какой основной вызов в части противодействия фишингу вы видите и какая конечная цель борьбы с ним?

— Конечная цель в борьбе с фишингом — сделать его использование экономически нецелесообразным. Надо выйти на такой уровень противодействия, когда усилия мошенников по созданию и распространению фишинговых ресурсов не будут окупаться.

Достижение этой цели существенно осложняется тем, что мошенники активно используют ИИ для генерации фишинга. Это делает атаки гораздо более массовыми, а их подготовку дешевле. Сегодня можно достичь успеха в противодействии фишингу только с использованием инстру-

Наша внутренняя платформа киберразведки содержит модуль для работы с фишингом: так, мы обнаруживаем фишинговые домены, маскирующиеся под бренд Сбера, ещё до появления на них контента. Этот модуль мы успешно перенесли на нашу внешнюю платформу управления киберугрозами X-Threat Intelligence

ментов на базе искусственного интеллекта.

— Какие новые сервисы в части противодействия фишингу от ГосСОПКА были бы полезны рынку?

— Рынку было бы полезно, если проблемой фишинга займутся на уровне всей страны. В свете этого важно отметить инициативы ГосСОПКА, о которых мы поговорим на предстоящей конференции. В рамках этих инициатив можно организовать сервис с использованием инструментов ИИ по оперативному выявлению и разделегированию фишинговых ресурсов в российской доменной зоне и блокировке доступа к ним в иностранных доменных зонах.

Сбер всегда готов предложить свои наработки в этой области. Наша внутренняя платформа киберразведки содержит модуль для работы с фишингом: так, мы обнаруживаем фишинговые домены, маскирующиеся под бренд Сбера, ещё до появления на них контента. Этот модуль мы успешно перенесли на нашу внешнюю платформу управления киберугрозами X-Threat Intelligence. Наполнение платформы, включая реализованные нами алгоритмы борьбы с фишингом, бесплатно доступно всем российским компаниям. Подключённые к X-Threat Intelligence организации уже узнали о десятках тысяч фишинговых ресурсов, которые имитировали их бренд.

По сути, Сбер уже создал техническую основу для общероссийского сервиса, но у нас нет возможности и полномочий разделегировать домены и блокировать доступ к ним. Полагаю, что объединение наших технологических возможностей и административного ресурса ГосСОПКА было бы полезно для защиты российских организаций от фишинга.

Кстати, у профсообщества уже есть пример успешного взаимодействия в сфере противодействия телефонному мошенничеству. Ранее этой теме уделялось мало внимания, однако теперь проблема взята на контроль на высшем государственном уровне. Активно ведётся законодательная работа, банки развивают системы антифрода, блокируются мошеннические звонки в мессенджерах, принимается множество других мер. В итоге совместными усилиями нам удалось переломить тренд на рост хищений от действий телефонных мошенников — и работа продолжается. Противодействие фишингу надо организовывать, используя этот положительный опыт. Хотелось бы отметить работу НКЦКИ, который предпринимает конкретные шаги в этом направлении.

— Сергей Васильевич, расскажете о вашем опыте взаимодействия с ГосСОПКА?

— Мы активно обмениваемся с ГосСОПКА информацией, направленной на обнаружение, предупреждение и ликвидацию последствий компьютерных атак. Для Сбера это всегда было полезно. Отдельно отмечу нашу продуктивную совместную работу в рамках подготовки к форуму «ГосСОПКА 2026». Считаю очень правильным решением, что ГосСОПКА подняла тему противодействия фишингу на своём форуме и привлекла Сбер к участию в этом важном мероприятии.

«НЕ ЖДИТЕ ПРОВЕРОК — ИНИЦИИРУЙТЕ ДИАЛОГ»

Роман ШАПИРО
руководитель Блока по информационной безопасности
Дирекции информационной безопасности АО «Почта России»

— Роман, расскажите о вашем опыте взаимодействия с ГосСОПКА и как изменился подход к сотрудничеству за последние годы?

— С самого основания ГосСОПКА я наблюдал кардинальную трансформацию отношения к ней — от формального соблюдения требований к полноценному партнёрскому диалогу. Современная ГосСОПКА — это не нагрузка на подразделения информационной безопасности, а «коллективный иммунитет» национальной инфраструктуры, где каждый участник одновременно получает и вносит вклад в общую картину угроз.

Четыре года назад наше взаимодействие ограничивалось подачей отчётов и получением бюллетеней. Сегодня мы участвуем в рабочих группах по разработке методических рекомендаций, получаем оперативные данные об угрозах и видим реальное понимание специфики нашего бизнеса.

Зрелость сотрудничества с регулятором измеряется не количеством отправленных форм, а скоростью, с которой индивидуальные кейсы превращаются в защитные меры. У нас был показательный случай: мы с коллегами получили информацию об угрозах, связанных с действиями хакеров через цепочку поставок, практически одновременно, но мы среагировали мгновенно — и избежали расследования инцидента с неблагоприятными последствиями.

Рекомендация: не ждите проверок — инициируйте диалог. Регулярные консультации с экспертами ГосСОПКА позволяют заблаговременно подготовиться к изменениям и минимизировать риски.

— Какие средства обнаружения атак вы считаете обязательными для любой организации, и как выстроить эшелонированную защиту в условиях ограниченных бюджетов?

— Эшелонированная защита — это не количество решений, а правильная расстановка приоритетов: сначала полная видимость, потом оперативное реагирование. При ограниченном бюджете гораздо эффективнее обеспечить качественную инвентаризацию активов, обеспечить процесс управления изменениями и гигиенический минимум грамотно настроенных инструментов, нежели покупать десяток несвязанных продуктов за десятки миллионов рублей.

Главная ошибка, которую я регулярно вижу,— «синдром коллекционера». Организации приобретают множество решений, но ни одно не настраивают должным образом. В прошлом году я консультировал компанию, где SIEM генерировал гигантский объём событий, однако правила корреляции не были адаптированы под реальную инфраструктуру. Процент ложных срабатываний вырос настолько, что команда мониторинга просто перестала воспринимать алерты как реальные угрозы. Это уже не защита, а самоуспокоение.

Поэтому строим оборону по принципу «сначала самое ценное»: начинаем с анализа логов доменных контроллеров и критических серверов — это даёт высокий процент покрытия при минимальных инвестициях. Даже специалист без глубокого опыта, опираясь на актуальные методические документы ФСБ и ФСТЭК России, сможет получить эффективную систему обеспечения информационной безопасности.

Практический совет: оптимизируйте число инструментов под реальные возможности организации. Лучше три решения, которые вы полностью понимаете и используете, чем десять в режиме «установил и забыл».

— На какие критерии и метрики должны ориентироваться CISO при выборе конкретных решений для обнаружения атак среди представленных на рынке?

— Главным критерием при выборе далеко не всегда является чистая функциональность. Часто важнее интеграционная готовность решения к встраиванию в существующую экосистему. Нет смысла покупать электрический «Москвич», если все специалисты вокруг умеют обслуживать только машины до 1998 года выпуска, но делают это великолепно, да и запас запчастей есть только для таких машин.

Я рекомендую оценивать три ключевых параметра: эффективность

детектирования, эргономику эксплуатации и экономику владения (TCO). Многие коллеги фокусируются исключительно на первом и совершают ошибку. В одном из проектов решение продемонстрировало впечатляющие показатели на синтетических тестах, но в реальной инфраструктуре количество ложноположительных срабатываний превышало 60%.

TCO — это не только стоимость лицензий, но и интеграция, обучение персонала, техподдержка. По моему опыту, реальная стоимость владения превышает первоначальные инвестиции в 2,5–3 раза. Решение должно бесшовно встраиваться в SIEM, SOAR и тикет-системы, а специалисты — быть обучены работе с ним.

Важно также оценивать устойчивость самого производителя: за последние годы мы наблюдаем устойчивую тенденцию к закрытию вендорами проектов по дальнейшей разработке средств защиты информации.

Совет: проводите пилотные проекты длительностью не менее 90 дней обязательно на собственной инфраструктуре. Только так можно понять реальную эффективность в ваших условиях, а не в идеальных демо-условиях.

— Нужны ли России национальные стандарты для средств обнаружения атак, и как их разработка может повлиять на развитие отечественного рынка ИБ?

— Стандарты необходимы, но их ценность определяется методологией разработки. Они должны стать акселератором развития отечественного рынка ИБ, а не барьером. Оптимальная формула: базовые требования задают минимальный уровень безопасности и взаимодействия, а механизмы адаптации учитывают отраслевую специфику.

Сегодня рынок сильно фрагментирован: каждый вендор использует свои метрики эффективности, форматы интеграции и подходы к обнаружению. Это приводит к зависимости от конкретного поставщика и серьёзно затрудняет миграцию.

В моей практике два крупнейших российских вендора потратили более шести месяцев только на обеспечение совместимости двух своих продуктов в части передачи между ними данных для анализа.

Национальные стандарты должны унифицировать форматы данных, API-интеграции и метрики эффективности. При этом «стандарт, написанный без участия практиков, становится не картой, а лабиринтом». Ключевой фактор успеха — вовлечение в разработку действующих CISO, а не только коллег, прекрасно разбирающихся в теории создания таких стандартов, и представителей вендоров с очевидным конфликтом интересов.

Грамотные стандарты стимулируют конкуренцию по качеству, а не по маркетинговым бюджетам, упрощают обоснование закупок и снижают регуляторные риски.

Практический совет: активно участвуйте в публичных обсуждениях проектов стандартов и формируйте консолидированную позицию через профессиональные ассоциации. Регулятор слышит структурированную обратную связь — в этом я убеждался неоднократно.

ПРИОРИТЕТЫ ЗАЩИТЫ

КАК ИХ РАССТАВИТЬ

Андрей КУРИЛО
кандидат технических наук, доцент, ФБК и FBK Cyber Security

Сущность понятия «безопасность» определяется как состояние безопасности, покоя, отсутствия тревог и невозможности реализации угроз, защищённости для ценности, ценного актива, субъекта.

Безопасность в то же время можно определить как специфическое состояние, особое свойство, близкое к категории качества[1], которое возникает у объекта защиты при реализации на нём особых защитных мер. Как показывает практика, это свойство латентно, постоянно стремится к исчезновению, незаметному «испарению».

С другой стороны, мы видим, что для поддержания безопасности необходимо постоянно прикладывать к активу довольно существенные усилия, тратить ресурсы и энергию, в результате чего возникает аналогия с понятием «энтропия», использованным К. Шеноном в теории информации, то есть с мерой неопределённости в системе. Чем выше энтропия (защищённость), тем меньше хаоса, но тем больше энергии нужно затратить на достижение этой цели.

Информационную безопасность принято оценивать либо по шкале меры близости к некоему императивно заданному уровню, состоянию (уровень защищённости, уровень зрелости, полный или выборочный набор требований по защите), либо прямым тестированием путём имитации атак или сканирования уязвимостей.

Сложность вопроса обусловлена тем, что для измерения уровня защищённости доступны только косвенные методы измерения и оценки. Естественно, при этом возникают вопросы достоверности и точности измерений, ошибок оценки защищённости. А в случае, если используется метод прямого тестирования, например тестирование уязвимостей или обновлений, по полученным результатам можно сделать вывод только об отсутствии или наличии уязвимостей в системе защиты, которые могут быть проэксплуатированы для реализации атаки. Но в целом по этим результатам в целом оценить уровень защищённости объекта защиты невозможно.

Таким образом, нужно определиться, что же нас интересует в итоге: защищённость ценных для нас активов[2] от угроз, оценённая через наличие слабостей в системе, или уровень защиты информации в ней.

Следует уточнить, что мы понимаем под словом информация. А что это такое? Это «иная, отличная от материи и энергии сущность» (Н. Винер), обладающая совершенно отличными, специфическими только для неё, свойствами и характеристиками. Важнейшим свойством информации, оказывающим существенное влияние на развитие проблематики защиты информации и в целом на всю сферу информационной безопасности, является её абсолютная инвариантность к постулатам информационной безопасности, известным как CIA (доступность, целостность и конфиденциальность), которые, по сути, являются ограничительными мерами. А ведь именно эти постулаты положены в основу всех механизмов защиты информации.

Противоречие между невозможностью применить CIA к информации и необходимостью их использовать в своё время было разрешено достаточно просто: все требования по безопасности информации были применены не к информации как к объекту защиты, а к материальной среде, в которой хранятся, обрабатываются и передаются данные[3]. Таким образом, было принято первое допущение (1), которым было установлено тождество между защитой информации и защитой среды её обработки

$$З_и \equiv З_д \qquad (1)$$

Где $З_и$ – защищённость информации, а $З_д$ – защищённость данных в среде обработки.

Это позволило распространить на информацию постулаты CIA и установить критерии достаточности мер её защиты.

До середины 70-х годов прошлого века, когда программы (софт) были неотделимы от самого компьютера (хард), защищённость информации оценивалась исключительно радиотехническими методами, путём измерений радиоизлучений (так называемый ПЭМИН[4]) «харда». В качестве критерия защищённости рассматривалось хорошо известное в радиотехнике соотношение шум/сигнал на входе измерительного радиоприёмника. Это устраивало всех. Измерял – и спокоен, всё нормально. На этой

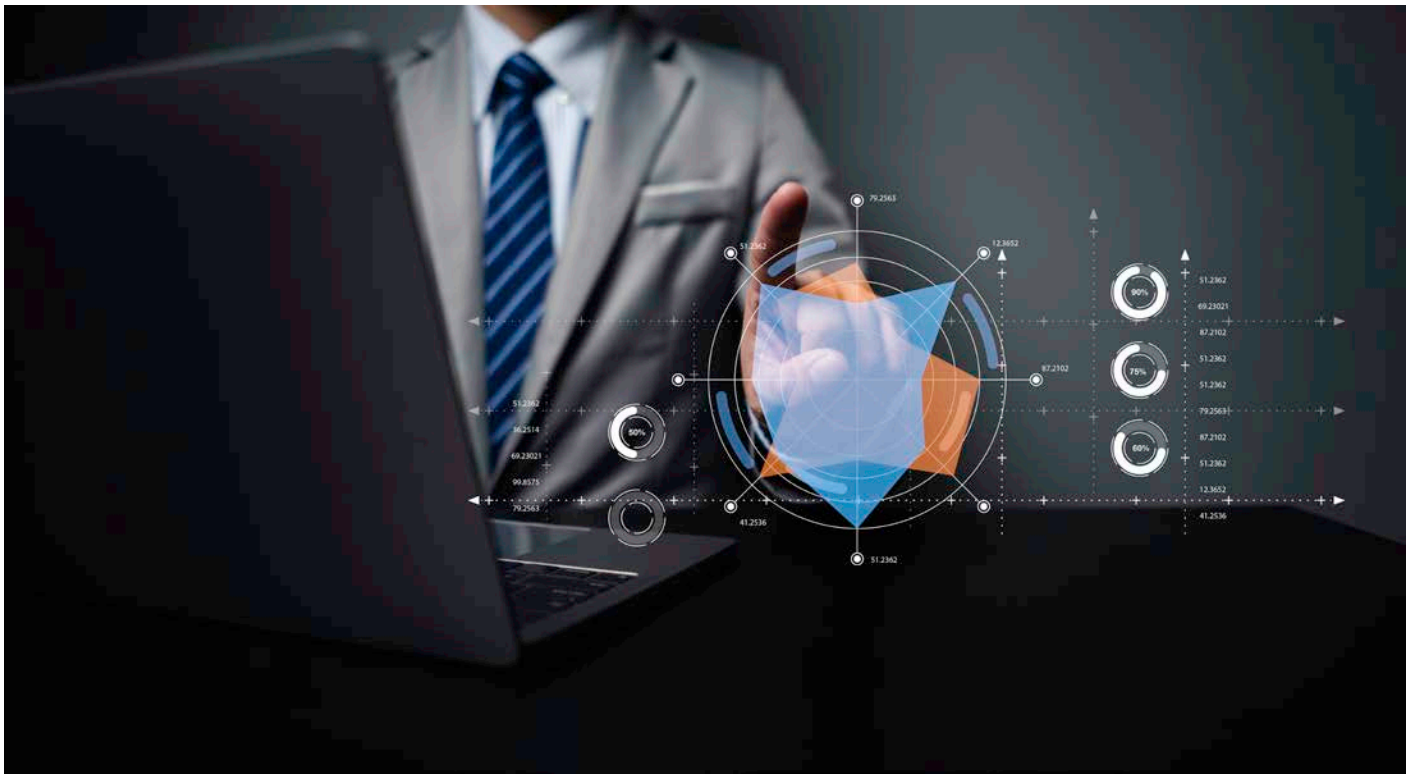
[1] В основе деятельности по обеспечению безопасности лежат стандарты управления качеством ISO 9000 и 9001, созданные на базе цикла управления деятельностью Деминга – Шухарта (PDCA).

[2] Что-либо, что имеет ценность для организации. [ГОСТ Р ИСО/МЭК 27000–2012].

Примечание. Имеются различные типы активов:
– информация;
– обеспечение программное;
– активы материальные, например компьютер;
– услуги;
– люди и их квалификация, навыки и опыт;
– активы нематериальные, такие как репутация и имидж.

[3] Данные – поддающееся многократной интерпретации представление информации в формализованном виде, пригодном для передачи, связи или обработки (ISO/IEC2382:2015).

[4] ПЭМИН – побочные электромагнитные излучения и наводки.



парадигме в сфере защиты информации возникла целая индустрия. Были вложены огромные средства в создание измерительной базы, проведение соответствующих измерений и в итоге – создание защищённых компьютеров.

Однако с развитием информационных технологий, отторжением «софта» от «харда», усложнением архитектур вычислительных систем, возникновением индустрии разработки ПО потребовалось усовершенствовать методику оценки защищённости информационных (автоматизированных информационных) систем, которые уже рассматривались как совокупность софта, харда, данных и пользователей, участвующих в работе системы и/или получающих от неё определённые сервисы и услуги. В середине 80-х годов прошлого века было принято второе допущение (2), при котором полагалось, что уровень защиты информации может быть оценён как результат выполнения набора специфических защитных мер, предъявленных к среде, в которой обрабатывается информация (данные).

$$К_{зи} = f(\sum М_{зи}) \quad (2)$$

Где:

- $К_{зи}$ – коэффициент защищённости системы, данных, данных, информации,
- $М_{зи}$ – защитная мера.

Этот подход позволил ввести шкалу для измерения уровня защищённости информации (данных). Критерием защищённости при этом считалось либо полное выполнение всего набора защитных мер (бинарный подход), либо соответствие императивно установленной мере близости к идеальному состоянию защищённой системы.

Это оказалось удобным для сертификации продуктов информатизации по требованиям безопасности в рамках ISO/IEC15408 Common criteria.

Однако попытки применения этого стандарта для решения задачи обеспечения информационной безопасности систем и крупных информационных комплексов оказались неудачными.

В эти же годы, когда компьютерная преступность ещё не развилась и не проявилась во всей своей красе и рассматривалась в теоретическом ключе, были разработаны системы оценки защищённости. При этом в требованиях по безопасности содержался довольно большой объём формальных требований, как оказалось, слабо влияющих на реальную защищённость систем.

В последнее время ситуация изменилась радикально и стало очевидным следующее.

Во-первых, выполнение на объекте защиты абсолютно всех требований по безопасности не позволяет достичь абсолютной защищённости и всегда существует определённая вероятность, риск «прокола» системы защиты и успешной атаки на данные или ПО, что мы и видим на практике:

- всегда или почти всегда может появиться новая, неизвестная атака, учесть которую было просто невозможно при проектировании системы защиты;
- вероятность срабатывания используемых защитных мер даже по известным атакам далеко не равна 100%, что существенно влияет на общую вероятность отражения атак системой защиты.

Во-вторых, ясно проявилось такое неприятное свойство информационной безопасности, как тенденция к «быстрому и незаметному испарению», резко повышающая вероятность успешной атаки на фоне фор-

мального соответствия требованиям по безопасности.

В-третьих, растущая сложность информационных систем увеличивает так называемую поверхность атаки, которая доступна злоумышленнику. За счёт неэффективного менеджмента постоянно возникающих уязвимостей эта «поверхность» ещё более расширяется, что повышает риск успешной атаки.

В-четвёртых, остро стоит вопрос качественного управления системой обеспечения информационной безопасности.

В-пятых, в проблематике защиты ясно обозначились две важные задачи, два этапа:

а) защита периметра, имеющая целью отразить, не пропустить атаку внутрь системы;

б) обеспечение безопасности внутренней структуры информационной системы, имеющее целью прежде всего предотвратить развитие атаки в случае её проникновения вовнутрь защищаемой системы.

Сформулированные и нормативно закреплённые требования по защите существенно различаются по следующим критериям:

- эффективности;
- вероятности срабатывания;
- скорости ослабления (деградации);
- затратам на реализацию.

Исходя из этого одни требования необходимо обязательно выполнять и строго контролировать как можно чаще, а лучше непрерывно, а другие — можно проверять с гораздо меньшей частотой. Это напоминает известное правило Парето: первоочередные 20% действий позволяют достичь 80% результата. Такой подход может существенно упростить и сделать более прозрачными процедуры контроля.

В-шестых, стало ясно, что задачу обеспечения защиты какого-либо приоритета информационной безопасности необходимо ставить не «вообще», а только на определённом отрезке времени. Например, в части отражения атак на отказ в обслуживании задача для службы безопасности может быть сформулирована следующим образом: не допустить реализацию атак через фишинговые письма или отразить DDoS-атаки с определённой плотностью в течение ближайших нескольких, трёх-пяти лет.

По истечении этого срока эти цели следует уточнять, но для этого, как правило, потребуется модификация системы защиты.

Наконец, киберпреступность не стоит на месте, а активно развивается и совершенствуется. В результате многолетнего, систематического и целенаправленного изучения информационной среды РФ «та сторона» постоянно приобретает новое, более детальное знание, намеченные к атаке системы детально и целенаправленно изучаются, улучшается планирование, растёт число успешных атак. Очевиден тренд на индустриализацию, промышленную разработку хакерских инструментов, интеграцию усилий, увеличение скорости атак за счёт внедрения искусственного интеллекта (ИИ). Обращает на себя динамика изменения и уточнения целей атак, а также оперативность внедрения в практику передовых наработок.

Всё изложенное вновь ставит вопрос о переосмыслении методического подхода к задаче обеспечения безопасности и способам её решения.

Очевидно, что на качество защиты самым существенным образом влияют:

- не только сам факт реализации требований по безопасности, но и в гораздо большей степени уровень зрелости процессов обеспечения безопасности объекта и управления ею, так как именно процессный подход позволит наиболее эффективно парировать деградацию защитных мер и поддерживать их на надлежащем уровне;
- оперативность, своевременность и качество принятия первоочередных мер, обеспечивающих прочность периметра и способность успешно отражать атаки, принятые во внимание при построении системы защиты, оперативность выявления и устранения «критических» уязвимостей системы защиты;
- наличие эффективного оперативного контроля и мониторинга работы основных защитных механизмов, обеспечивающих защиту внутренней структуры защищаемой информационной системы, а также выявления наличия в ней признаков атак;
- автоматизация управления работой системы обеспечения информационной безопасности и повышения, таким образом, скорости реакции системы защиты на атаку;
- существенное повышение требований к поставщикам услуг в части обеспечения информационной безопасности с целью разрушения каналов атаки «через поставщика».

Как следствие, оказалось необходимым повышать качество (уровень) защиты имеющихся объектов и рассматривать объекты и их подсистемы не выборочно, а в совокупности с поставщиками, подрядчиками и клиентами, как специфическую «экосистему информационной безопасности», имея в виду тот неоспоримый факт, что цепь всегда рвётся в слабом звене.

И тут снова встают вопросы: как измерять качество защиты, как соотнести его с вероятностью отражения атак или, наоборот, вероятностью успешных атак? Достаточно ли измерять уровень соответствия требованиям или необходим иной, более точный подход? Как выстроить эффективную систему управления информационной безопасностью в современных условиях? Как организовать эффективный мониторинг информационной безопасности? Какие задачи управления безопасностью необходимо автоматизировать, чтобы эффективно управлять рисками информационной безопасности?

Выделим главное.

1. Информационная безопасность системы, то есть её защищённость, устойчивость в условиях воздействия на неё компьютерных атак, обеспечивается качественной реализацией соответствующих (рекомендованных или предписанных) защитных мер, организационных мероприятий и контрольных мер.

2. Защитные меры, как уже было отмечено, имеют различную и не всегда стопроцентную эффективность. Но при этом напомним, что

первоочередные 20% действий достигают 80% результата. В нашем случае к таким действиям относится довольно ограниченный набор мер защиты периметра и веб-сервисов. Выполнить эти требования просто, а результат будет весьма заметен. Однако и все остальные защитные меры тоже должны быть реализованы.

3. Организационные требования запускают процессы обеспечения безопасности.

4. Процессы обеспечивают устойчивость защитных мер и существенно снижают вероятность их незаметного «испарения».

5. Управление системой обеспечения безопасности должно существенно уменьшить скорость её реакции на вторжения и инциденты и включать максимальную автоматизацию функций сбора информации, контроля работы подсистем, выявления признаков типовых атак и реакции на них.

6. Мониторинг основных защитных мер и состояния информационной инфраструктуры должен быть непрерывным.

7. Чем проще и яснее изложены требования по защите, тем выше результат.

8. Контроль должен включать:

а) оценку соответствия требованиям по безопасности (в форме аудита);

б) оценку уровня зрелости процессов обеспечения и управления безопасности (в форме проверок, самооценок с обязательной отчётностью);

в) оперативный контроль первоочередных мер защиты, в первую очередь периметра;

г) инструментальное тестирование, в первую очередь средств защиты периметра, включая электронную почту, и веб-сервисов, взаимодействующих с сетью Интернет, и в плановом порядке — внутренней структуры защищаемой информационной системы;

д) обязательную отчётность.

Если обратиться к вопросу анализа рисков нарушения безопасности, следует отметить, что при таком подходе риски нарушения ИБ могут быть существенно снижены за счёт организации эффективного управления и непрерывного контроля процессов. То есть будет осуществляться тот самый «менеджмент рисков».

Однако следует отметить, что на практике до уровня управления рисками дело пока не дошло.

ФСТЭК на протяжении нескольких лет в ходе проверок объектов критической информационной инфраструктуры (КИИ) фиксирует грубые примитивные нарушения требований защиты, например использование заводских настроек паролей, а число административных штрафов, вынесенных по результатам проверок в 2025 году, составило 1200 при 700 проверенных объектах. Лишь 36% всех проверенных организаций соответствуют минимальному уровню защищённости, установленному ФСТЭК. При этом минимальный уровень защищённости считается достигнутым, если выполнены все требования ФСТЭК, изложенные в нормативных документах[5]. Очевидно, что, пока эта первая, достаточно простая, но исключительно важная задача не решена, о менеджменте рисков думать рано.

Тем не менее с учётом последних изменений, происходящих в проблематике информационной безопасности, встраивается следующая схема управления безопасностью объекта и контроля.

1. Двухэтапная (1-й этап — защита периметра и веб-сервисов, взаимодействующих с сетью Интернет, 2-й этап — организация защиты внутренней структуры и управления ИБ) реализация требований нормативной базы по обеспечению информационной безопасности не только на объектах КИИ, но и на других, ценных для населения объектах, типа Владимирского хлебозавода, информационная система которого недавно подверглась разрушительной компьютерной атаке, что создало много реальных неудобств для населения крупного города и его окрестностей.

2. Контроль реализации требований по защите в виде аттестации или аудита ИБ.

3. Повтор аудита ИБ в виде оценки соответствия требованиям по информационной безопасности и оценки уровня зрелости процессов обеспечения безопасности каждые 3 года.

4. Оперативный контроль защищённости периметра, включая инструментальное тестирование каждые 6 месяцев, с одновременной оценкой уровня зрелости основных трёх-четырёх процессов управления и обеспечения информационной безопасности.

5. Централизованная обязательная отчётность перед госрегуляторами по результатам проверок.

6. Усиление административной и уголовной ответственности собственников (руководителей) организаций за непринятие мер защиты.

ЗАКЛЮЧЕНИЕ

Задача обеспечения информационной безопасности в нашей стране в современных условиях вышла на новый уровень, превратившись из формализованной системы требований, направленной на отражение «будущих» угроз, в задачу обеспечения устойчивости работы информационных систем в условиях информационного общества и наличия беспрецедентного и всё возрастающего числа и сложности компьютерных атак на них. Будет ошибкой думать, что эта ситуация изменится в лучшую сторону.

И выход из этой ситуации только один:

1. Постоянное улучшение защиты;

2. Оптимизация наборов требований, что продемонстрировало ФСТЭК приказом № 117 и новыми методиками контроля защищённости;

3. Повышение качества управления информационной безопасностью на объектах защиты;

4. Существенное повышение ответственности топ-менеджмента за реализацию деятельности по обеспечению информационной безопасности.

[5] Методический документ ФСТЭК от 11 ноября 2025 г. «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», пункт 3.

КИБЕРПОЛИГОНЫ И НЕПРЕРЫВНАЯ КИБЕРУСТОЙЧИВОСТЬ

СТРАТЕГИЯ, ТАКТИКА, МЕТОДОЛОГИЯ

Алексей БАТЮК
технический директор Positive Technologies по развитию государственного сектора

Возможно ли через практику использования киберполигонов усилить систему цифровой устойчивости критических инфраструктур и превратить оценку защищенности из периодической процедуры в постоянный процесс?

Современный ландшафт киберугроз развивается настолько быстро, что традиционная модель периодической оценки защищенности информационных систем постепенно теряет эффективность. Если раньше запрос на аудит безопасности или тестирование на проникновение возникал раз в год или раз в несколько лет, то сегодня этого уже недостаточно для понимания уровня защищенности организации.

Количество уязвимостей программного обеспечения ежегодно растет. В международной базе Common Vulnerabilities and Exposures (CVE) фиксируется более 25–30 тысяч новых уязвимостей в год, причем значительная их часть относится к критическим. Ежегодно это число будет возрастать, потому что злоумышленники активно используют автоматизированные инструменты поиска уязвимостей (уже нередко с использованием технологий искусственного интеллекта) и эксплуатации слабых мест инфраструктуры.

Параллельно увеличивается интенсивность компьютерных атак. Государственные организации и объекты критической инфраструктуры регулярно становятся целями сложных целевых кампаний, направленных на нарушение технологических процессов, уничтожение данных или вывод из строя информационных систем.

В результате возникает очевидный вызов: инфраструктура может становиться уязвимой значительно быстрее, чем проводится очередная проверка защищенности.

В этих условиях обеспечение киберустойчивости требует перехода от периодической оценки защищенности к модели непрерывной проверки устойчивости инфраструктур к актуальным сценариям атак.

Одним из наиболее эффективных инструментов реализации такого подхода становятся киберполигоны и киберучения.

КОГДА ПРОДАКШН — НЕ МЕСТО ДЛЯ ЭКСПЕРИМЕНТОВ

Проверять, как инфраструктура выдерживает реальные сценарии атак, прямо в рабочей среде зачастую невозможно. Особенно это касается объектов критической информационной инфраструктуры, где отдельные системы напрямую связаны с непрерывной работой технологических процессов.

В таких условиях проведение активных тестов может нести риски для функционирования организации.

Киберполигоны решают эту проблему за счет создания цифровых копий инфраструктуры: в виртуальной среде воспроизводится архитектура информационных систем, сетевые взаимодействия и логика работы ключевых сервисов.

Это позволяет безопасно моделировать сложные сценарии атак и регулярно проверять цифровую копию инфраструктуры на возможные векторы атак, оценивая эффективность средств защиты без риска для производственной среды.

Практика показывает, что подобное моделирование нередко выявляет проблемы, которые долгое время остаются незамеченными. Например, при построении цифровой копии инфраструктуры одного из клиентов мы воспроизвели сценарий атаки с компрометацией сервисного узла. В ходе моделирования выяснилось, что через доверительные связи злоумышленник мог получить доступ к сегменту, где располагалась система управления критическим технологическим процессом.

Такая архитектурная связка существовала много лет и воспринималась как техническая необходимость. Однако при реальной атаке она могла привести к остановке ключевого процесса организации. После проведения киберучений клиент пересмотрел архитектуру сетевых взаимодействий и внедрил дополнительные механизмы сегментации.

Подобные кейсы демонстрируют важную особенность киберполигонов: они позволяют выявлять не только программные уязвимости, но и архитектурные и организационные риски, которые сложно обнаружить традиционными методами аудита.

ОТ КИБЕРУЧЕНИЙ К КИБЕРИСПЫТАНИЯМ

Киберучения традиционно используются для подготовки специалистов мониторинга и реагирования. Для этого применяются киберполигоны — цифровые копии реальной ин-

фраструктуры, на базе которых можно регулярно проводить тренировки команд защиты. Такой подход позволяет отрабатывать сценарии атак в максимально реалистичной среде, не затрагивая рабочие системы.

Однако подготовка специалистов — лишь одна часть задачи. Для оценки защищенности самой инфраструктуры используются кибериспытания и программы поиска уязвимостей. Они проводятся уже на реальной среде и позволяют выявлять уязвимости и проверять, возможна ли реализация конкретных недопустимых событий.

Вместе эти подходы формируют систему непрерывной работы с киберустойчивостью: киберполигоны и киберучения помогают готовить команды к отражению атак, а кибериспытания и поиск уязвимостей позволяют регулярно проверять защищенность инфраструктуры.

Эффективность подобного подхода уже доказана в ряде отраслей. Программы багбаунти и кибериспытаний активно используются в банковском секторе, ретейле и технологических компаниях. Постоянное привлечение независимых исследователей безопасности позволяет выявлять уязвимости значительно раньше злоумышленников.

В контексте критической инфраструктуры речь может идти прежде всего о закрытых кибериспытаниях, проводимых в контролируемой среде по ограниченным спискам участников.

ПРИМЕНЕНИЕ УСПЕШНОЙ ПРАКТИКИ В НАЦИОНАЛЬНОЙ МОДЕЛИ КИБЕРУСТОЙЧИВОСТИ

В системе ГосСОПКА для субъектов критической инфраструктуры подобные испытания могли бы проводиться силами центров ГосСОПКА.

На первом этапе участие в закрытых кибериспытаниях могли бы принимать:

- специалисты центров ГосСОПКА;
- организации, имеющие лицензии ФСТЭК России;
- специалисты профильных исследовательских организаций.

Это позволило бы обеспечить необходимый уровень безопасности и доверия субъектов критической информационной инфраструктуры (КИИ) и регуляторов при проведении испытаний.

При этом оценивалась бы не только защищенность инфраструктуры, но и эффективность работы сил мониторинга и реагирования. Также появится возможность оценить способность сил центров ГосСОПКА проводить подобные мероприятия. Например, центры ГосСОПКА могли бы выставить собственную инфраструктуру, исследователями которой будут сотрудники других центров.

Фактически речь может идти о формировании системы оценки компетенций центров ГосСОПКА и создании рейтинговой модели участников национального взаимодействия — насколько эффективно они способны выявлять уязвимости, моделировать сценарии атак и организовывать мероприятия по оценке защищенности.

ЭКОСИСТЕМА АНАЛИЗА УЯЗВИМОСТЕЙ

Важным элементом подобных программ является триаж отчетов об уязвимостях.

Для обеспечения качества анализа этот процесс мог бы выполняться профессиональным экспертным сообществом специалистов по информационной безопасности, формируемым при участии Национального координационного центра по компьютерным инцидентам (НКЦКИ).

В отдельных случаях, особенно когда речь идет о критически значимых системах, триаж может осуществляться непосредственно специалистами НКЦКИ.

Такая модель позволила бы обеспечить баланс между эффективностью обработки отчетов и необходимым уровнем контроля.

ЭКОНОМИКА КИБЕРИСПЫТАНИЙ

Еще одним преимуществом кибериспытаний является экономическая эффективность.

Традиционная модель оценки защищенности предполагает оплату за проведение работ и подготовку отчетов. При этом результат таких работ не всегда напрямую связан с количеством выявленных уязвимостей или реальным повышением уровня защищенности.

Модель багбаунти и кибериспытаний предполагает иной подход: организация платит за результат — за найденные уязвимости и подтвержденные риски, а не за сам процесс проверки.

Это позволяет значительно повысить эффективность расходов на информационную безопасность.

Для государственных и бюджетных организаций такой подход может оказаться особенно актуальным. В этом случае средства направляются не на подготовку формальных отчетов, а на фактическое выявление и устранение уязвимостей.

ЗАКЛЮЧЕНИЕ. ОТ ПЕРИОДИЧЕСКИХ ПРОВЕРОК — К ПОСТОЯННОЙ КИБЕРУСТОЙЧИВОСТИ

Интенсификация киберугроз и постоянное появление новых уязвимостей делают традиционную модель периодических проверок все менее эффективной.

В этих условиях обеспечение устойчивости информационных инфраструктур требует перехода к непрерывной оценке киберустойчивости.

Киберполигоны способны стать технологической основой такого подхода. Они позволяют безопасно моделировать атаки на информационные объекты критической инфраструктуры, проводить кибериспытания и совершенствовать процессы мониторинга и реагирования.

В сочетании с механизмами обмена информацией в рамках ГосСОПКА это может создать основу для новой модели обеспечения безопасности критических информационных систем — модели, в которой защищенность проверяется не эпизодически, а постоянно.

Именно такой подход способен обеспечить устойчивость цифровых систем предприятий, отраслей и государства в условиях нарастающего киберпротивостояния.

ПОЧЕМУ КОМПАНИИ СО ЗРЕЛЫМИ СИСТЕМАМИ ИБ ВСЁ РАВНО ТЕРЯЮТ ДЕНЬГИ ИЗ-ЗА КИБЕРИНЦИДЕНТОВ

Иван ПРОХОРОВ
руководитель продукта MaxPatrol 360, Positive Technologies

За последние десять лет инвестиции бизнеса в информационную безопасность (ИБ) выросли многократно. Компании внедряют Security Information and Event Management (SIEM) — системы, средства обнаружения угроз на конечных устройствах, системы управления уязвимостями, анализа сетевого трафика, аналитику поведения пользователей и десятки других технологий. С точки зрения архитектуры такие инфраструктуры выглядят достаточно зрелыми. Однако статистика по инцидентам показывает парадоксальную ситуацию: даже компании с развитой системой защиты продолжают нести серьёзные финансовые потери из-за кибератак.

Согласно информации о расследовании киберинцидентов, основная доля финансовых потерь компаний связана не столько с утечками данных, сколько с операционными последствиями атак — остановкой сервисов, простоем инфраструктуры и вымогательством (ransomware-атаки). По данным отчета Sophos State of Ransomware 2024, большинство компаний, столкнувшихся с ransomware-атаками, испытывали серьёзные перебои в работе ИТ-систем и бизнес-сервисов. Такие атаки способны парализовать ключевые процессы компании, нарушить цепочки поставок и остановить цифровые сервисы, что напрямую приводит к финансовым потерям. Это означает, что даже при наличии современных средств защиты организации долгое время остаются уязвимыми после компрометации. Причина заключается в том, что наличие технологий ещё не означает эффективное управление безопасностью.

ЧЕМ БОЛЬШЕ ИНСТРУМЕНТОВ, ТЕМ СЛОЖНЕЕ УПРАВЛЯТЬ БЕЗОПАСНОСТЬЮ

Современная инфраструктура информационной безопасности в крупных компаниях состоит из множества специализированных решений. По данным исследований процессов в Security Operations Center (SOC), проведенных Splunk и Palo Alto Networks, более 70% команд ИБ используют более 10 различных инструментов, а почти половина организаций — более 20. В некоторых крупных компаниях стек средств защиты может включать 40–60 различных систем. Каждая из этих систем решает свою задачу: обнаружение вредоносной активности, анализ поведения пользователей, мониторинг сетевых соединений, управление уязвимостями, контроль доступа. Однако вместе они создают серьёзную операционную проблему — фрагментацию процессов ИБ.

Каждая информационная система имеет:

- интерфейс;
- модель данных;
- механизмы корреляции событий;
- сценарии реагирования.

В результате специалистам SOC приходится вручную сопоставлять информацию из разных источников, чтобы понять, что на самом деле происходит в инфраструктуре.

Исследование Splunk показывает, что 46% специалистов по ИБ тратят больше времени на управление инструментами, чем на анализ угроз. Вместо расследования инцидентов команды вынуждены заниматься настройкой систем, интеграциями и ручной корреляцией событий.

Чем больше инструментов используется в инфраструктуре, тем сложнее обеспечить согласованную работу всей системы безопасности.

Более 70% команд ИБ используют более 10 различных инструментов, а почти половина организаций — более 20. В некоторых крупных компаниях стек средств защиты может включать 40–60 различных систем

ПЕРЕГРУЗКА АЛЕРТАМИ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Одним из ключевых факторов неэффективности SOC остаётся перегрузка аналитиков уведомлениями о событиях безопасности. Каждый инструмент генерирует собственные

алерты: сигнатуры вредоносного ПО, аномалии поведения, подозрительные сетевые соединения, попытки несанкционированного доступа. В крупных инфраструктурах это могут быть тысячи и десятки тысяч событий ежедневно. Значительная часть этих уведомлений оказывается ложноположительной. В результате специалисты SOC сталкиваются с явлением, известным как alert fatigue — усталость от алертов.

Согласно исследованиям SANS Institute, аналитики SOC могут тратить до 25–30% рабочего времени на обработку ложных срабатываний.

При таком объёме событий риск пропустить действительно опасную активность существенно возрастает. По данным Devo Security Operations Report, более 70% специалистов по ИБ признают, что боятся пропустить реальную атаку из-за перегрузки уведомлениями. Это напрямую влияет на скорость реагирования и масштаб ущерба.

НЕДОСТАТОК КОНТЕКСТА ПРИ РАССЛЕДОВАНИИ ИНЦИДЕНТОВ

Даже когда подозрительная активность обнаружена, следующей проблемой становится недостаток контекста для принятия решений.

Аналитику необходимо понять:

- какой актив затронут;
- кто является владельцем системы;
- есть ли известные уязвимости;
- происходили ли похожие события ранее;
- связана ли активность с индикаторами компрометации.

Но эта информация обычно находится в разных системах: CMDB, системах управления активами, платформах Threat Intelligence, системах мониторинга.

Исследование процессов в SOC, проведенное Medium, показывает, что до 60–80% времени аналитиков может уходить на сбор контекста и корреляцию данных из различных источников, а не на непосредственное расследование угроз. В результате расследование инцидента может занимать часы или даже дни, хотя ключевые данные уже существуют в инфраструктуре — просто они распределены по разным системам.

ГДЕ НА САМОМ ДЕЛЕ ФОРМИРУЮТСЯ ФИНАНСОВЫЕ ПОТЕРИ

Распространённое заблуждение — считать, что основной ущерб от атаки возникает в момент проникновения злоумышленника. На практике большая часть финансовых потерь формируется после проникновения, в промежутке между обнаружением угрозы и её полной нейтрализацией.

Этот этап включает:

- расследование инцидента;
- локализацию атаки;
- восстановление инфраструктуры;
- анализ масштаба компрометации.

Именно здесь начинают накапливаться основные бизнес-риски:

- простой критически важных систем;
- распространение атаки на новые активы;
- повторные компрометации;
- необходимость срочного восстановления инфраструктуры.

Публичная статистика по расследованию инцидентов подтверждает масштаб проблемы. По данным практики реагирования на инциденты Positive Technologies:

- в 40% случаев обнаружение угрозы занимало более одного месяца;
- только 21% атак выявлялся в течение первых суток.

При этом устранение последствий инцидента также занимает значительное время:

- только 29% компаний полностью ликвидируют инцидент за неделю;

47% организаций тратят на это более месяца.

Таким образом, даже после обнаружения атаки компания может оставаться в состоянии кризиса длительное время, что напрямую приводит к финансовым потерям.

КИБЕРИНЦИДЕНТЫ ВСЕ ЧАЩЕ ВЛИЯЮТ НА БИЗНЕС-ПРОЦЕССЫ

Ранее кибератаки в основном рассматривались как проблема ИТ-инфраструктуры. Сегодня ситуация изменилась. Современные компании глубоко цифровизированы: бизнес-процессы, производственные системы, финансовые операции и взаимодействие с клиентами зависят от ИТ-систем. Поэтому последствия атак всё чаще выходят за пределы ИТ.

По данным расследований инцидентов, проведенных командой Positive Technologies ESC IR, доля проектов, в которых атака привела к нарушению внутренних бизнес-процессов, достигла 55%.

Это означает, что инциденты напрямую затрагивают:

- производственные процессы;
- логистику;
- клиентские сервисы;
- финансовые операции.

Дополнительным фактором риска становится расширение цифровых экосистем. Современные компании активно взаимодействуют с подрядчиками, облачными сервисами и партнёрскими системами.

В результате растёт доля атак, в которых использовались доверительные отношения с подрядчиками и партнёрами. По данным расследований, около 28% инцидентов связаны именно с такими сценариями. Чем шире цифровая экосистема компании, тем сложнее контролировать происходящее.

ГЛАВНАЯ ПРОБЛЕМА — НЕ ТЕХНОЛОГИИ, А ПРОЦЕССЫ

Современная информационная безопасность традиционно описывается через модель «люди — процессы — технологии». Однако во многих организациях основной фокус инвестиций сохраняется именно на технологиях.

При этом процессы реагирования на инциденты остаются фрагментированными:

- разные команды используют разные инструменты;
- отсутствует единая система управления инцидентами;
- детектирующая логика распространяется неравномерно;
- реагирование на события часто происходит вручную.

Особенно сложной задачей становится управление детектирующей логикой.

Правила обнаружения угроз постоянно обновляются: появляются новые индикаторы компрометации, изменяются техники атакующих, внедряются новые источники данных. Без централизованного контроля сложно добиться того, чтобы актуальная логика обнаружения использовалась одинаково во всей инфраструктуре. В результате часть атак могут оставаться незамеченными просто из-за несогласованных параметров систем безопасности.

ЧТО ИЗМЕНИТ СИТУАЦИЮ

Чтобы действительно снизить ущерб от киберинцидентов, организациям необходимо управлять всем жизненным циклом инцидента, а не только его обнаружением. Это требует перехода от набора разрозненных инструментов к платформе управления операционной деятельностью SOC.

Такая платформа объединяет:

- события безопасности из разных источников;
- процессы обнаружения инцидентов;
- процессы расследования инцидентов;
- сценарии реагирования;
- данные об активах и уязвимостях;
- аналитику и отчетность.

Единая операционная среда позволяет аналитикам SOC работать с инцидентами быстрее и эффективнее, а руководству — получать прозрачную картину происходящего.

Именно эту задачу решает платформа MaxPatrol 360 от Positive Technologies — единый центр управления расследованиями и операционной работой SOC.

MaxPatrol 360 объединяет события и инциденты в единую систему, снижает объём ручной работы, автоматизирует реагирование и обеспечивает прозрачный контроль безопасности.

ГДЕ ВОЗНИКАЕТ БИЗНЕС-ЭФФЕКТ

На первый взгляд внедрение платформы управления процессами в SOC может восприниматься как техническое улучшение. Но на самом деле эффект проявляется прежде всего на уровне бизнеса.

Централизованное управление инцидентами позволяет:

- сократить время обнаружения и реагирования (MTTD и MTTR);
- снизить масштаб инцидентов;
- уменьшить нагрузку на аналитиков SOC;
- повысить прозрачность процессов ИБ для руководства.

В результате компания решает одну из ключевых задач — повышает киберустойчивость своей инфраструктуры. А это означает не просто меньше атак, а меньше финансовых потерь, когда атаки всё-таки происходят. Именно способность быстро и управляемо реагировать на инциденты сегодня становится главным показателем зрелости информационной безопасности.

ПО ГОРЯЧИМ СЛЕДАМ

КАК DR.WEB FIXIT! ПОМОГАЕТ РЕКОНСТРУИРОВАТЬ КАРТИНУ АТАКИ

Василий СЕВОСТЬЯНОВ
начальник отдела технического сопровождения продаж компании «Доктор Веб»

В информационной безопасности не существует инструмента, способного решать любые задачи. Защита инфраструктуры складывается из множества элементов: технологий, настроек системного ПО, организационных мер и процедур реагирования.

Антивирусный вендор рассматривает кибербезопасность прежде всего через призму противодействия действиям злоумышленников. Когда речь идет о вредоносном ПО, фундаментом защиты остается антивирус. Он чаще всего предотвращает запуск вредоносных программ, блокирует заражение и мешает злоумышленнику закрепиться в системе.

Однако использование вредоносного ПО — лишь один из способов компрометации. Атаки могут эксплуатировать уязвимости в веб-приложениях, ошибки конфигурации систем, слабую защиту удаленного доступа, неудачные решения в архитектуре инфраструктуры или человеческий фактор. Часть рисков нейтрализуется специализированными средствами защиты, некоторые — настройками штатного ПО, а другие требуют изменения рабочих процессов.

На практике даже в организациях с выстроенной защитой возникают инциденты, поскольку атакующие используют разные классы техник: эксплуатацию уязвимостей, компрометацию цепочек поставок, ошибки конфигурации и социальную инженерию.

Далее события развиваются по-разному:

- некоторые, если позволяют резервные копии, просто восстанавливают системы и продолжают работу;
- другие пытаются разобраться — что произошло, как злоумышленник проник в инфраструктуру и какие лазейки использовал.

Для выяснения причин инцидента необходимо восстановить последовательность событий — шаг за шагом реконструировать действия злоумышленника по цифровым следам на компьютерах и серверах. Эта деятельность относится к области форензики и реагирования на инциденты (DFIR).

Есть мнение, что для решения подобных задач не обойтись без Endpoint Detection and Response (EDR)-систем. Выглядят они внушительно, но потребляют много ресурсов и требуют внимания специалистов. Распространенная картина: несколько месяцев компания тратит деньги и человекочасы для внедрения EDR. В результате, эксплуатация требует значительных ресурсов и зрелых процессов обработки событий, среди шума которых практически невозможно разглядеть реальные инциденты. А ведь далеко не каждая организация способна внедрить EDR-решение или использовать его постоянно. При этом задача расследовать инциденты и анализировать состояние инфраструктуры остается.

На помощь приходят инструменты, которые позволяют точечно исследовать конкретные системы, собрать артефакты и выстроить хронологию событий на уровне хоста. Для этих задач специалисты «Доктор Веб» используют сервис **Dr.Web FixIt!**

ЧТО ТАКОЕ DR.WEB FIXIT!

Инструмент предназначен для детального анализа состояния компьютеров и устранения выявленных угроз безопасности. Сервис управляется через веб-интерфейс и не требует установки ПО на компьютеры клиента.

Dr.Web FixIt! активно применяется специалистами «Доктор Веб» в расследованиях и выручает в случаях, когда невозможно применить тяжелое решение типа EDR. С помощью веб-интерфейса генерируется индивидуальная утилита FixIt!, параметры которой задаются в зависимости от задачи. Утилита запускается на проверяемой системе, собирает данные и, при необходимости, выполняет процедуры очистки.

Ключевые преимущества **Dr.Web FixIt!**:

- работает без установки,
- совместим с антивирусными продуктами других производителей,
- используется в инфраструктурах с решениями других вендоров.

Помимо обнаружения активного вредоносного ПО, сервис позволяет выявлять следы уже удаленных программ — остаточные элементы закрепления, измененные системные настройки, артефакты активности злоумышленников и другое.

Сервис решает разные задачи: например, анализ и лечение после заражения или исследование подозрительной активности на конкретной машине. Мы часто используем его для поиска следов компрометации, особенно после целевых атак. Иногда в процессе исследования выясняет-

ся, что целевая атака разворачивается именно сейчас! **Dr.Web FixIt!** даже способен выявлять уязвимости и небезопасную конфигурацию — но для таких задач его стоит комбинировать с другими специализированными инструментами.

Помимо расследования инцидентов, **Dr.Web FixIt!** подходит для регулярных проверок состояния компьютерных систем — это коррелирует с регуляторными требованиями. В частности, приказ ФСТЭК России № 117, вступивший в силу с 01.03.2026 года, закрепляет риск-ориентированный подход к обеспечению безопасности и требует периодической оценки защищенности информационных систем.

На практике такая оценка включает анализ конфигурации систем, поиск следов компрометации и выявление нарушений политик безопасности — именно те задачи, для решения которых используется **Dr.Web FixIt!**.

ПРИМЕР ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ DR.WEB FIXIT!

Чтобы продемонстрировать возможности Dr.Web FixIt!, поделимся деталями одного показательного инцидента на российском машиностроительном предприятии. В конце июня 2025 года представители одной компании обратились к нам с запросом, не являются ли периодические срабатывания антивируса на одном из компьютеров следствием сбоя.

Проверка показала, что антивирус реагировал корректно, а за срабатыванием скрывалась целевая атака. Краткая хронология:

1. Первое заражение — 12 мая 2025 года. Начальная точка компрометации — компьютер без антивируса, через который злоумышленники получили первоначальный доступ в сеть предприятия. На устройство попал троян Trojan.Updatar.1, его запустил пользователь при открытии вложения в письме. На момент заражения, эта модификация уже около недели находилась в вирусных базах Dr.Web.

Подчеркнем еще раз ключевой момент инцидента: заражение началось на корпоративном компьютере без антивируса. Комментарии излишни.

2. Через час троян загрузил дополнительные компоненты — Trojan.Updatar.2 и Trojan.Updatar.3, которые продолжили атаку.

3. 14 мая злоумышленники использовали один из модулей для создания задачи службы BITS, через которую был загружен файл shell.exe. Он содержал шеллкод для установки бэкдора Meterpreter. Затем был установлен компонент FileManager.exe для удаленного управления файлами и выгрузки данных.

4. Для получения учетных данных пользователя Windows использовалась утилита Tool.HandleKatz.

Классическая ситуация: при отсутствии антивируса защищать память процесса LSASS некому, поэтому пароли извлекаются стандартными инструментами (HandleKatz). Такие случаи в нашей практике встречаются с разочаровывающей регулярностью.

5. Атакующие установили RDP Wrapper, чтобы упростить доступ к системе через удаленный рабочий стол, а также инструменты туннелирования Chisel и FRP.

6. Компрометация второго компьютера началась 14 мая. Злоумышленники использовали учетные данные с первого устройства и удаленно выполняли команды в сети предприятия.

7. 23 мая — попытка установить Trojan.Updatar.1 на второй компьютер, однако антивирус Dr.Web на нем заблокировал запуск. Но 29 мая атакующие снова получили доступ к системе и вручную установили другое вредоносное ПО. 3 июня через службу BITS был загружен бэкдор Meterpreter.

8. Третья система была скомпрометирована через учетные данные RDP. Начиная с 23 июня, злоумышленники подключались через удаленный рабочий стол и пытались закрепиться в системе с помощью инструментов из набора Metasploit. Была попытка выполнить вредоносный PowerShell-скрипт, однако антивирус Dr.Web обнаружил и заблокировал его как DPC: BAT.Starter.613.

Расследование инцидента — это не поиск одного вредоносного файла, а восстановление полной картины. Важно понять, где первая точка входа, как злоумышленник закрепился в системе, какие инструменты использовал, как перемещался по сети и где именно дыры в защите

ИТОГИ РАССЛЕДОВАНИЯ

Случай хорошо иллюстрирует, что расследование инцидента — это не поиск одного вредоносного файла, а восстановление полной картины. Важно понять, где первая точка входа, как злоумышленник закрепился в системе, какие инструменты использовал, как перемещался по сети и где именно дыры в защите.

Расследование при помощи **Dr.Web FixIt!** позволило проанализировать атаку, выявить инструменты и определить слабые места в инфраструктуре. И обратите внимание — задача решена без сложных систем постоянного мониторинга.

Когда инцидент уже произошел и нужно быстро разобраться в причинах без развертывания сложной инфраструктуры мониторинга, подобные инструменты оказываются крайне полезны и практичны.

С помощью **Dr.Web FixIt!** инцидент полностью расследован, ущерб определен, работа над ошибками сделана — и все это без развертывания систем массового сбора телеметрии и штата аналитиков Security Operations Center (SOC).

Dr.WEB

Специальная акция

Переход на Dr.Web со скидкой 50%

Специальная акция для бизнеса и государственных учреждений — скидка 50% при переходе на решения Dr.Web с антивирусов других производителей.

Акция действует до 31 декабря 2026 года включительно.

Если вы

Планируете переход на ПО Dr.Web

Ранее не использовали продукты Dr.Web для бизнеса и госучреждений, но планируете переход с решений других вендоров

Планируете возвращение на ПО Dr.Web

Использовали решения Dr.Web в прошлом, но не приобретали лицензии со скидкой по программе миграции «Переходи на зеленый» на соответствующие продукты

Планируете расширение лицензии

Используете **Dr.Web Desktop Security Suite** для защиты от 1 до 5 рабочих станций и готовы в рамках акции увеличить лицензию от 50 до 250 рабочих станций или приобрести другие продукты Dr.Web в соответствии с условиями акции

То вы можете приобрести решения Dr.Web со скидкой 50%!

В акции участвуют следующие продукты Dr.Web для бизнеса и госучреждений:

Dr.Web Desktop Security Suite
защита рабочих станций

Dr.Web Server Security Suite
защита серверов

Dr.Web Mobile Security Suite
защита мобильных устройств и планшетов

Dr.Web Mail Security Suite
проверка почтового трафика

Dr.Web Gateway Security Suite
проверка интернет-трафика

Dr.Web ATM Shield
защита встроенных устройств

Комплект для малого бизнеса
оптимальное решение для малого бизнеса

Узнать подробности

ПРОСТЫЕ ШАГИ В ВЕРНОМ НАПРАВЛЕНИИ

КАК ПРАВИЛЬНО РЕАГИРОВАТЬ НА ИНЦИДЕНТ

Даниил БОРИСЛАВСКИЙ
Эксперт по ИБ
Контур.Эгиды

Атаки на информационные ресурсы Российской Федерации могут осуществляться не только извне периметра, но и в самой компании. В этой статье рассмотрим, как расследовать внутренние инциденты информационной безопасности (ИБ) и передавать результаты в ГосСОПКА.

Опишем на примере двух типов популярных инцидентов, абсолютно выдуманных, в которых все совпадения не случайны. Не стремимся соблюсти хронологию один-в-один, а показываем последовательность действий и результаты, которых хотим добиться.

Предполагаем, что инциденты происходили в среднестатистической организации — субъекте критической информационной инфраструктуры (КИИ), в которой есть ИБ- и ИТ-подразделения, юридическая служба, несколько сотен сотрудников. В организации уже используются инструменты ИТ и внутренней ИБ (например, IRM-систем Staffcop, сервис двухфакторной аутентификации ID от Контур.Эгиды, Security Information and Event Management (SIEM) система), но ещё нет Security Operations Center (SOC).

БАЗОВАЯ ПОДГОТОВКА К РАССЛЕДОВАНИЮ И РЕАГИРОВАНИЮ

Инциденты проще расследовать, если уже реализована система оповещений о нарушении политик ИТ и ИБ, и сами политики созданы и регулярно обновляются.

Поэтому важно на старте прописать самые главные блоки политик, например, «контроль над передачей критически важной и ДСП (для служебного пользования) информации по каналам передачи» и «аномальная файловая и сетевая активность приложений». В статье ниже мы рассмотрим два инцидента — для обнаружения каждого поможет своя политика.

Политики можно создавать в системах расследования инцидентов, например, Staffcop. Как пример, нужны политики, которые будут анализировать контент на наличие каких-то критически важных слов, терминов, номенклатур. Если на предприятии разрабатывают приборы БСЛ, то создадим поиск по словарю в содержимом перехваченных файлов. Для поиска используем простейшее регулярное выражение «БСЛ*ПЗК» (рисунок 1).

Для обнаружения аномальной активности можно использовать встроенные в SIEM политики или создать самостоятельно, если их нет. Чтобы политики работали верно, нужно в течение месяца изучить «нормальную» активность на 10% компьютеров, выбранных в случайном порядке и зафиксировать количество файловых и сетевых операций. Затем убрать выходные дни, усреднить значения и разделить пропорционально до одного дня, добавить 30% для потенциала роста. Исходя из полученных данных, создать политики реагирования в случае превышения этих значений.

Затем нужно провести проверку на количество срабатываний.

Если срабатываний нет, мы, скорее всего, завысили планку, если срабатываний больше 10, но среди них нет инцидентов, то мы занизили планку.

ИНЦИДЕНТ №1

Допустим, что офицер ИБ получает уведомление о том, что на одной из рабочих станций на подключённую флэшку был записан файл, содержащий упоминание о «БСЛ-110-ПЗК».

Шаг 1. Определение атрибутов инцидента. Для этого нужно зафиксировать время инцидента, на каком рабочем компьютере он произошёл, кто из сотрудников работал за ком-

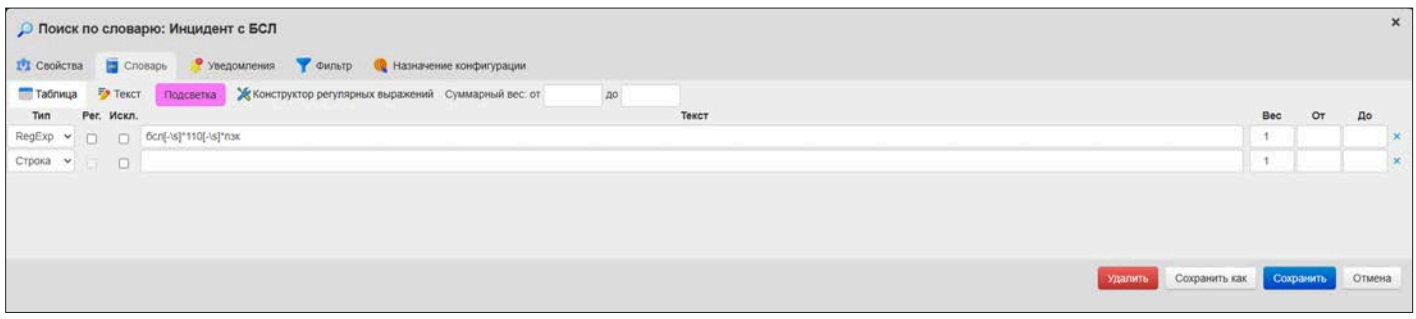


Рисунок 1. Скриншот из web-консоли Staffcop

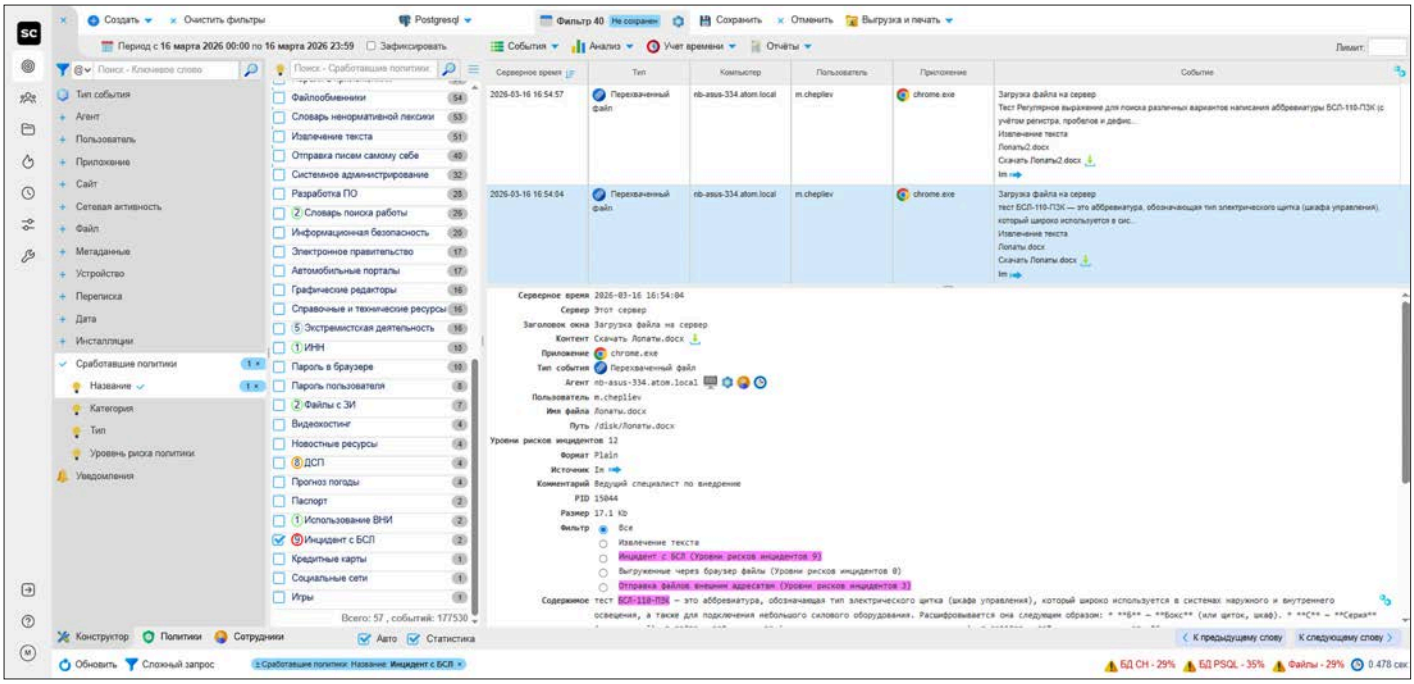


Рисунок 2. Скриншот из web-консоли Staffcop

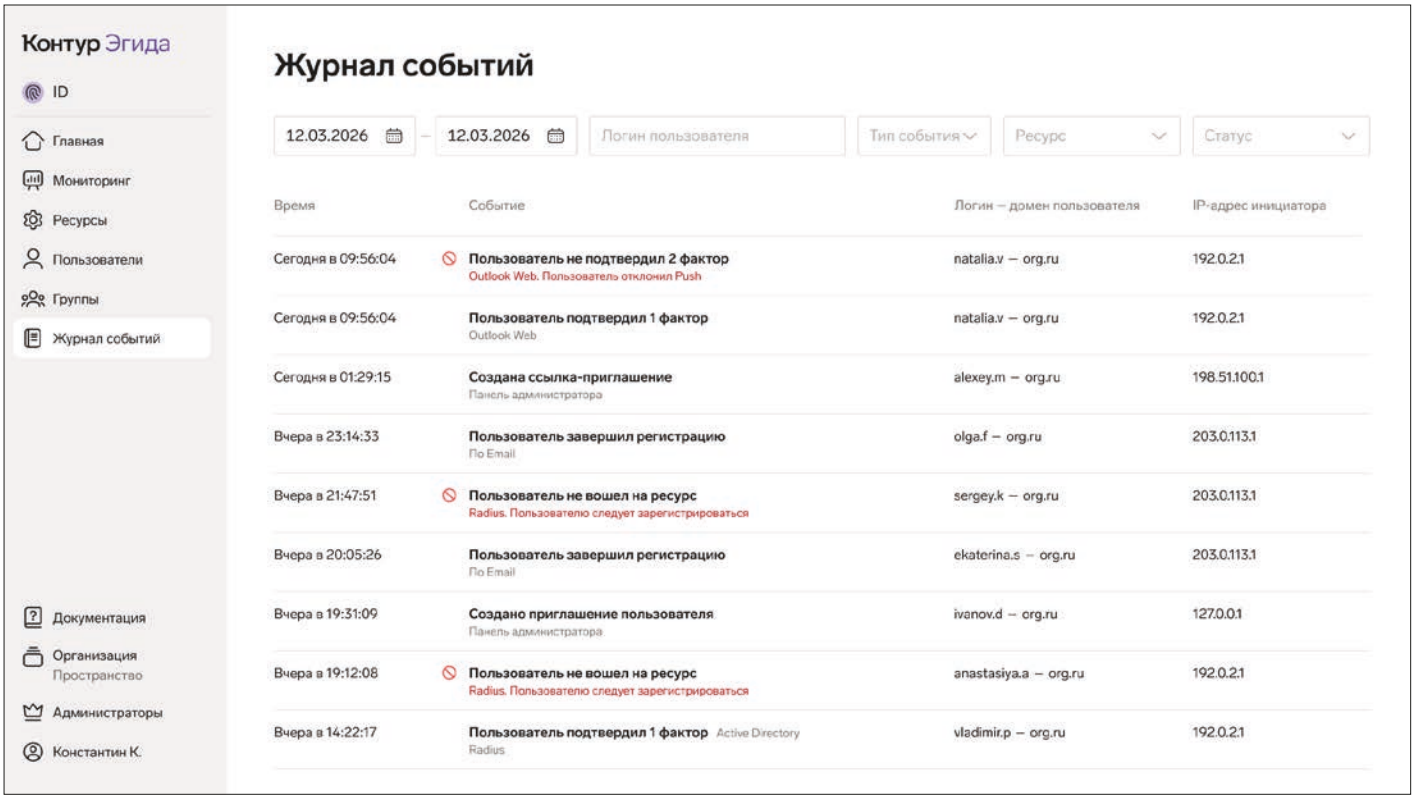


Рисунок 3. Журнал событий ID

пьютером, номер съёмного накопителя информации, название скопированного файла. Намного удобнее, когда вся подобная информация есть в одном событии, в одной системе, например, в линзе событий Staffcop (рисунок 2).

Шаг 2. Подтверждение личности субъекта. Дальше нам нужно подтвердить личность субъекта, осуществившего действия, ставшие причиной инцидента. Для этого можно воспользоваться журналом событий из системы двухфакторной аутентификации Контур.ID. Такая система даст точное подтверждение тому, что на компьютере работал определённый сотрудник. Без этого подтверждения доказать причастность сложнее — можно сослаться на то, что кто-то украл, подсмотрел, подобрал пароль (рисунок 3).

Шаг 3. Истребование объяснений. Для этого нужно зайти в кабинет, где находится персональный компьютер (ПК), с которого зафиксирована утечка информации, сообщить всем присутствующим, что произошел инцидент, запретить покидать помещение и потребовать предъявить все имеющиеся внешние накопители информации. В результате этого у субъекта инцидента изымают флеш-накопитель и просят написать объяснительную об инциденте с записью информации на неразрешенный внешний носитель.

Шаг 4. Сбор артефактов. Дальше нужно собрать вместе все накопленные артефакты инцидента:

- выгрузки и скрины из журнала ID об аутентификации при логине на рабочий ПК;
- выгрузки и скрины о подключении флэшки и записи файла на флэшку из Staffcop.

Также необходимо запросить артефакты у юридического или кадрового отдела:

- локальные нормативные акты (ЛНА), регламентирующие использование пароля и второго фактора аутентификации;
- документы о внедрении в организации системы автоматизированного сбора и обработки информации об активности на ПК.

Шаг 5. Уведомление об инциденте. После этого нужно заявить об инциденте на сайте Национального координационного центра по компьютерным инцидентам (НКЦКИ). Указываем в форме следующие данные:

- Категория. Выбираем «уведомление о компьютерном инциденте».
- Тип. Выбираем подходящий по смыслу. В данном случае это «несанкционированное разглашение информации».
- Затем указываем информацию об объекте КИИ, местоположении, категоризации.
- Если уже обнаружили инцидент и приняли меры, ставим статус реагирования «меры приняты».
- Если случай локальный, то указываем, что привлекать силы ГосСОПКА не нужно.
- В поле «краткое описание события ИБ» указываем «Сотрудник скопировал на внешний носитель информации документ ДСП».
- В поле «Сведения о средстве или способе выявления» описываем использованные в обнаружении и расследовании инструменты.
- В поле «Ограничительный маркер TLP» указываем нужный.
- Указываем влияние на конфиденциальность, целостность и доступность.
- Если инцидент имел какие-то дополнительные последствия вне компании или затронул другие информационные системы (ИС), нужно описать это.
- В поле «утечка ПДн» обязательно отмечаем были ли в содержимом «утекшей» информации персональные данные, даже если это единичная строка.

Таким образом, вы провели расследование инцидента и произвели уведомление НКЦКИ

ИНЦИДЕНТ №2

Предположим, что SIEM система или web-консоль Staffcop присылает уведомление об аномальной активности приложений на нескольких ПК. Из описания срабатывания видно, что всплеск файловой активности производит одно приложение. Через какое-то время в кабинет ИБ приходит сотрудник с жалобой «не могу работать за компьютером, потому что все файлы на рабочем столе изменились». И уже становится ясно, что ПК сотрудника зашифрован.

Важно:

приведенный порядок действий не является универсальным. Реальные сроки реагирования и восстановления зависят от зрелости процессов и подготовки команды. Стоит заранее разработать собственный план и провести учения.

Шаг 1. Изоляция устройства. Перезагрузка зашифрованного ПК может быть дорогой ошибкой. Так вы уничтожите следы в памяти и можете сломать картину произошедшего. Правильный ход — изолировать машины от сети, не отключая питание. Проще всего вытащить интернет-кабель, отключить Wi-Fi. Это останавливает распространение по сети и сохраняет артефакты, а файлы на локальном компьютере, если вы уже обнаружили шифрование, — уже не спасти.

Шаг 2. Организация штаба реагирования. Один даже очень квалифицированный офицер ИБ такой инцидент не закрывает. Минимальный состав штаба выглядит так:

- **Координатор** — ведет процесс, ставит приоритеты, держит связь с руководством.
- **Офицер ИБ** — отвечает за организацию управления рисками ИБ, и как следствие работает с инцидентами. Эксперт в области ИБ.
- **Владельцы ключевых систем** — отвечают за контекст и восстановление своих ИС.
- **Администраторы** — контролируют сети, серверы, домены, хранилища по зонам. Являются экспертами в ИТ.

ЧТО ТАКОЕ TLP

TLP: RED — крайне конфиденциальная информация, только для конечного получателя;
TLP: AMBER — ограниченное распространение внутри организации в рамках доступа получателям;
TLP: GREEN — широкое распространение в пределах сообщества партнёрских компаний или нескольких организаций без публикации в любых внешних источниках;
TLP: WHITE — неограниченное распространение, но передача информации не должна нарушать авторские права.

◆ **Юрист** — оценивает обязательства по уведомлениям и фиксирует юридически значимые факты.

◆ **PR или маркетинг** — готовят внутренние и, при необходимости, внешние информационные сообщения.

Работа строится короткими циклами. В конце каждого — промежуточный итог: что сделано, результаты, что делаем дальше, что мешает или требуется. Все действия заносятся в общий журнал. Важный принцип — **восстановление из резервных копий только после локализации и сбора следов,** а не вместо них. Иначе вредоносное программное обеспечение (ПО) может вернуться отложенной задачей или сохранённым доступом.

Шаг 3. Действия по плану.

Первый этап. Отмечаем границы поражения. Изолируем сегменты сети и отдельные узлы. Блокируем скомпрометированные учетные записи и ключи. Собираем артефакты: логи, снимки, хэши, копии подозрительных файлов. Организуем отдельный защищённый канал связи штаба. Юрист параллельно оценивает, попадают ли произошедшие события под обязательные уведомления каких-либо регуляторов.

Второй этап. Переходим к стабилизации. Поднимаем критичные процессы — из проверенных копий, с проверкой «чистоты» перед восстановлением. По плану меняем пароли и ключи, убираем лишние права, включаем дополнительный мониторинг на повторное проникновение. Внутреннее сообщение — коротко и по делу: что случилось, что уже сделано, что временно недоступно, куда обращаться, когда будет следующий апдейт.

Третий этап. Контрольная проверка сервисов и телеметрии. Закрываем «дыры», чтобы исключить повтор. Готовим отчет руководству: что произошло, какие меры приняты, что ещё предстоит сделать, каковы предварительные сроки. Назначаем ретроспективу с обязательным списком изменений: кто владелец каждого пункта и когда даст результат.

ЧТО ЕЩЁ ОБЯЗАТЕЛЬНО УЧЕСТЬ

Если инцидент затронул ПДн, оператор обязан оперативно уведомить уполномоченного регулятора (Роскомнадзор). По факту события — в течение 24 часов; в течение 72 часов — о результатах внутреннего расследования. Чтобы уложиться в сроки, заранее проверьте, что у ответственного в организации за обработку и защиту ПДн есть доступ к форме, что шаблоны уведомлений готовы, а маршрут согласования короткий. Нужны факты и четкие формулировки.

Для субъектов КИИ действует своё информирование через НКЦКИ. Пример заполнения формы уведомления разобрали в первом инциденте. В этом случае данных будет заметно больше, но и команда реагирования усилена специалистами.

В кризисной ситуации молчание может навредить больше, чем сам факт инцидента. Внешние и внутренние сообщения делаются при осознанной необходимости, по четкой схеме:

◆ **что произошло** — понятным языком, без технических деталей;

◆ **что уже сделано** — меры по локализации и защите клиентов;

◆ **что будет дальше** — расследование, дополнительные проверки, улучшения;

◆ **как себя могут защитить пользователи** — поменять пароль, включить многофакторную аутентификацию (MFA), проверить активность;

◆ **когда ждать обновлений** — четкие временные рамки.

Важно:

не обещать невозможных сроков, не сваливать всю вину на других и не давать противоречивых комментариев. Скорость, простота объяснений, ответственность, эмпатия и конкретные меры — именно эти элементы позволяют снизить панику и сохранить доверие.

ВАЖНОЕ ПРО ЗНАЧИМЫЕ ИНЦИДЕНТЫ

Чтобы реагирование на подобный инцидент не парализовало работу всей организации и не вызвало панику у сотрудников, нужно заранее готовить планы реагирования и проводить учения. Пройдите прямо сейчас небольшой чек-лист для своей организации:

◆ У вас есть актуальный список команды реагирования: координатор, владельцы систем, юрист.

◆ В организации понятны роли: кто восстанавливает, кто расследует, кто коммуницирует.

◆ Проводится прогон процедур уведомления регуляторов и НКЦКИ.

◆ Для системы бэкапов определены и исполняются: частота процесса, места хранения, тест восстановления.

◆ Еженедельно происходит проверка учётных записей: отсутствие учёток без паролей, защита через MFA, блокировка учёток уволенных сотрудников.

◆ Ведётся сбор и хранение логов на критичных узлах.

◆ Проводятся «настольные» учения с реальными сценариями и ретро по итогам.

* * *

Реагирование — это про дисциплину. Про то, что кто-то заранее проверил бэкапы, включил сбор логов, разложил роли, потренировал команду и удостоверился, что процедуры уведомления работают. Тогда в «час Ч» организация действует эффективно и не усиливает ущерб: быстро локализует, поднимает критичные сервисы, выполняет обязательства перед государством и клиентами, фиксирует уроки и встраивает их в процессы. Когда этого нет — обучение начинается в самый неподходящий момент и обходится дорого.

НЕ СТАТЬ ДОЛГОСТРОЕМ

О ЧЕМ ВАЖНО ПОМНИТЬ ДЛЯ БЫСТРОГО ВНЕДРЕНИЯ SIEM?

Павел ПУГАЧ
системный аналитик «СёрчИнформ»

Внедрение SIEM часто воспринимается как сложный и долгий проект. Нужно научиться расследовать инциденты и отслеживать аномалии, закрыть требования регуляторов (ФСТЭК, Роскомнадзор, ЦБ), настроить отправку данных в ГосСОПКА. Но что, если система сможет начать работать буквально в день установки?

Чтобы вложение в SIEM оказалось удачным, важно последовательно пройти несколько этапов: от планирования до выбора модели лицензирования и непосредственно внедрения. Разберем каждый из них.

КАК УЧЕСТЬ БУДУЩИЕ ЗАТРАТЫ И НЕ ПЕРЕПЛАТИТЬ

Прежде чем загружать дистрибутив, важно провести внутреннюю подготовку. Первый шаг — инвентаризация ИТ-среды. Какое оборудование, серверы, сетевые устройства и критичные приложения составляют вашу инфраструктуру? Это не просто список, а основа для определения масштаба проекта и, что немаловажно, формирования реалистичного бюджета.

Аппаратные требования напрямую зависят от того, какой объем и детализацию событий планируется собирать. Здесь важен взвешенный подход: «логировать все» может оказаться избыточным и дорогим, а слишком скудный сбор данных снизит эффективность SIEM. При этом в текущей ситуации стоимость аппаратного обеспечения становится все более значимой статьей расходов — за последние полгода цены на SSD выросли на 25–90%, а оперативная память DDR5 подорожала более чем в два раза. Прогнозируется, что совокупные расходы на DRAM и SSD к концу 2026 года вырастут. Это значит, что чем эффективнее SIEM использует имеющиеся ресурсы, тем ощутимее экономия на «железе» при развертывании и масштабировании системы.

Именно на этапе планирования важно смотреть не только на текущие потребности, но и на то, как выбранное решение повлияет на бюджет в перспективе. Коробочные системы, такие как «СёрчИнформ SIEM», позволяют избежать неожиданных расходов. Система не требует покупки дополнительных модулей для базовых сценариев — все уже работает «из коробки». Лицензирование в «СёрчИнформ SIEM» привязано не к объему событий, а к количеству источников — вы платите только за те узлы, которые реально контролируете, и не беспокоитесь, что рост числа логов неожиданно увеличит стоимость. А значит, вы сразу понимаете, во что обойдется проект, и можете заложить в план только то, что действительно нужно.

Результатом планирования должно стать описание проекта с техническими требованиями, архитектурой и сроками.

4 КОМПОНЕНТА, КОТОРЫЕ ВЛИЯЮТ НА ВАШ БЮДЖЕТ И СРОКИ

Чтобы внедрение прошло быстро и предсказуемо, полезно понимать, из каких частей состоит любая система мониторинга событий. От того, как реализован каждый компонент, напрямую зависит, столкнетесь ли вы с долгими доработками или получите работающий инструмент с первого дня.

Система сбора данных. Это набор контроллеров, которые подключаются к вашим источникам: серверам, сетевым устройствам, базам данных и приложениям. Именно здесь часто возникают первые сложности: под каждый нестандартный источник приходится писать собственные парсеры, а это время и деньги. В коробочных решениях, таких как «СёрчИнформ SIEM», этот этап уже не требует дополнительных вложений. Около 50 предустановленных контроллеров готовы к работе сразу после установки. Есть индивидуальные контроллеры для популярного оборудования и ПО и универсальные — для источников, которые передают данные по стандартным протоколам (NetFlow, SSH, Syslog).

Движок анализа и корреляции. Это «мозг» SIEM, который в реальном времени обрабатывает поток событий, сопоставляет их с правилами и выявляет инциденты. Если правила не настроены или их слишком мало, система превращается в дорогое хранилище логов, а не в инструмент обнаружения угроз. «СёрчИнформ SIEM» поставляется с готовым набором правил корреляции, покрывающих типовые угрозы — то есть система начинает детектировать аномалии в день установки, без месяцев настройки.

Система хранения. Она отвечает за то, чтобы данные надежно сохранялись и были доступны для расследований. В идеале модель хранения прозрачна и не требует сложных доработок — вы сразу понимаете, как долго будут доступны события и как оптимизировать затраты на дисковое пространство.

Консоль управления. Это рабочее место специалиста по ИБ. Здесь подключаются новые источники, настраиваются правила корреляции и, главное, происходит работа с инцидентами. От того, насколько консоль удобна и интуитивна, зависит, будет ли команда использовать ее в полном объеме. Консоль «СёрчИнформ SIEM» спроектирована так, чтобы быть понятной специалистам с разным уровнем подготовки: работа с инцидентами, подключение источников и настройка правил реализованы в графических интерфейсах, поэтому не требуют отдельных курсов и месяцев погружения.

ВАЖНОСТЬ МОДЕЛИ ЛИЦЕНЗИРОВАНИЯ

Когда вопросы архитектуры и совместимости решены, остается ключевой момент — модель лицензирования, которая напрямую влияет на объем затрат.

На рынке есть SIEM-системы, в которых стоимость привязана к объему обрабатываемых данных, который может неожиданно расти при аномалиях или вместе с инфраструктурой. «СёрчИнформ SIEM» использует прозрачную модель по количеству узлов. Вы платите за серверы и сетевое оборудование, которые реально контролируете, и всегда можете рассчитать бюджет на год вперед без сюрпризов.

Это и есть главное удобство «коробочной» модели: вы заранее знаете, за что платите, не переплачиваете за объемы данных и можете предсказуемо масштабироваться. В системах, требующих длительного внедрения и глубокой кастомизации, стоимость услуг по настройке нередко превышает стоимость самого ПО — и этот риск особенно важно учитывать при планировании бюджета. А то, что «СёрчИнформ SIEM» уже включает все необходимые компоненты «из коробки» — от контроллеров до правил корреляции — означает, что не придется докупать модули и расширения или переплачивать за внедрение.

В системах, требующих длительного внедрения и глубокой кастомизации, стоимость услуг по настройке нередко превышает стоимость самого ПО

БЕЗБОЛЕЗНЕННОЕ ВНЕДРЕНИЕ

Когда планирование завершено и выбрана модель лицензирования, наступает этап внедрения.

Установка «СёрчИнформ SIEM» в стандартной конфигурации занимает от нескольких часов до рабочего дня. Это возможно благодаря тому самому принципу «все включено»: система уже имеет предустановленные правила корреляции и готовые коннекторы. Более того, при правильной настройке сбора данных она способна ретроспективно выявить инциденты, произошедшие за несколько дней до официального запуска.

Процесс строится в сотрудничестве с вашей ИТ-командой:

- **Поэтапное подключение источников.** Рекомендуется начинать с сетевого периметра, затем переходить к ключевым службам и приложениям. Благодаря обширной библиотеке готовых коннекторов этот этап проходит максимально гладко: большинство источников подключаются по принципу «выбрал из списка — настроил — получил данные».
- **Настройка сбора данных.** Она выполняется силами ИТ-отдела заказчика при экспертной поддержке инженеров разработчика. Для сохранения конфиденциальности уже на этом этапе можно настроить, кому какая информация будет видна в системе — работает ролевая модель доступа, так что сторонним специалистам можно ограничить видимость логов.
- **Гибкость без лишних затрат.** Если в инфраструктуре есть нетиповые системы, подключение решается через стандартные протоколы или с помощью пользовательского контроллера на PowerShell по готовым шаблонам. И все это без необходимости покупки дополнительных модулей — еще одно преимущество коробочной модели.

SIEM ЗДЕСЬ И СЕЙЧАС

Итак, предварительный анализ инфраструктуры помогает оценить, с какими сложностями вы столкнетесь. Изучение архитектуры решения — оценить трудозатраты при внедрении и требования к компетенциям специалистов для работы с ним. А понимание лицензирования — выбрать модель, которая не преподнесет неприятных сюрпризов. В «СёрчИнформ SIEM» все три вопроса решены в пользу удобства, прозрачности и оптимизации ресурсов. В результате компания получает понятный инструмент мониторинга безопасности, который показывает эффективность с первого дня.

Убедиться в этом легко: попробуйте **полнофункциональную 30-дневную тестовую версию**. Это возможность оценить гибкость настройки и полноту покрытия на реальных данных вашей инфраструктуры — от этапа планирования до ежедневной работы с инцидентами.

SIEM ВМЕСТО IRP

КАК ALERTIX ЗАКРЫВАЕТ БАЗОВЫЙ ФУНКЦИОНАЛ IRP-РЕШЕНИЙ

Илья ОДИНЦОВ
менеджер
по продукту,
NGR Softlab

Современным системам Security Information and Event Management (SIEM) уже недостаточно быть просто системами сбора логов. В условиях усложнения ландшафта угроз и дефицита бюджетов на внедрение отдельных решений Incident Response Platform (IRP) всё более актуальными становятся SIEM, берущие на себя самую востребованную часть их функционала — автоматизированное реагирование на инциденты.

АВТОМАТИЗИРОВАННОЕ РЕАГИРОВАНИЕ

Начиная с версии 3.9, в SIEM Alertix реализован механизм плейбуков реагирования. Это могут быть как простые цепочки («инцидент — блокировка»), так и сложные сценарии с автоматическим сбором данных и выполнением типовых команд, но с обязательным одобрением человека на критических этапах (например, «блокировка — расследование — разблокировка»).

Плейбуки строятся на правилах корреляции, связанных со скриптами (реагирование, сбор данных, подключение источников). При этом система из всего многообразия сценариев предлагает только те, которые соответствуют конкретной угрозе: платформа автоматически подставляет параметры из событий в поля сценариев, поэтому аналитику L1/L2 не нужно думать, что делать с алертом. По итогам расследования можно одним кликом снять или расширить блокировку. Такой подход минимизирует ошибки и сокращает среднее время реагирования (MTTR).

ИНТЕГРАЦИЯ СО СМЕЖНЫМИ СИСТЕМАМИ

Реагирование часто требует данных из систем, не связанных напрямую с безопасностью (систем контроля и управления доступом (СКУД), Identity Management (IDM)). В Alertix для этого предусмотрены скрипты-коннекторы, позволяющие воркспейсам обращаться к API любых сервисов для получения контекста. Создаваемая автоматически карточка события обогащается информацией из смежных систем: техникой и тактикой MITRE, сведениями о связанных узлах, учётных записях, данными инвентаризации (включая список ПО на хостах и теги, используемые для изменения критичности и связи активов в логические группы, например, информационные системы (ИС)). При анализе аналитик может добавить события-оригинаторы и последствия, что, в свою очередь, подтянет информацию по ним из модуля инвентаризации. А интеграция с поставщиками фидов позволит сразу увидеть угрозы в рамках карточки. Всё это в комплексе позволяет качественно определить плейбук реагирования для конкретного события.

ГИБКАЯ РОЛЕВАЯ МОДЕЛЬ

Ролевая модель Alertix позволяет разграничивать доступ к редактированию и запуску скриптов. Например, аналитики L1/L2 могут только запускать готовые плейбуки через интерфейс, а инженеры ИТ — разрабатывать скрипты, не имея доступа к инцидентам и логам. Это даёт возможность безопасно привлекать смежные отделы к процессам реагирования.

SECOPS-ПОДХОД: GIT И DETECTION AS CODE

Для зрелых команд в Alertix реализована интеграция с Git-репозиториями (GitHub, GitLab, Bitbucket). Скрипты для плейбуков можно писать и отлаживать в привычной среде, хранить в репозиториях и загружать в платформу через CI/CD-пайплайн с сохранением полной истории изменений.

Это даёт возможность проводить код-ревью, тестировать скрипты в безопасной среде и только потом выпускать в прод, а при необходимости — быстро откатиться к стабильной версии. Управление правилами становится предсказуемым, снижается риск ошибок, ускоряется вывод новых детектов. Кроме того, снимается зависимость от вендора: при появлении zero-day угрозы команда может самостоятельно написать правило за несколько часов, не дожидаясь обновлений.

* * *

Alertix 3.9 способен заменить функционал базовых IRP и Security Orchestration, Automation and Response (SOAR)-решений. Встроенная автоматизация, умная подстановка данных, гибкая система безопасности и поддержка Git превращают его в единую платформу для детектирования, расследования и реагирования. Автоматизация сокращает среднее время реагирования (MTTR), снижает нагрузку на аналитика и минимизирует риск ошибок, делая процесс расследования быстрым, понятным и управляемым.

SECURITY VISION AM, КИИ И ГОССОПКА

КОМПЛАЕНС И ЗАЩИТА ГИБРИДНЫХ ИНФРАСТРУКТУР

Роман ДУШКОВ
эксперт, Security Vision

Когда специалистов не хватает, каждый час их работы на счету, успех защиты данных в сфере ИБ определяется рациональным распределением времени специалистов.

Security Vision выделяет три направления, в которых развиваются продукты, посвященные выполнению задач регуляторов и защите объектов критической информационной инфраструктуры (КИИ):

1) **практические** инструменты и средства защиты информации (СЗИ), связанные с автоматизацией и созданием экосистемы ИТ- и ИБ-продуктов;

2) инструменты **стратегической безопасности,** фокусирующиеся на управлении процессами, регламентами и задачами;

3) инструменты для **аналитических задач,** построения интерактивных дашбордов и быстрого создания отчётов под требования регуляторов.

Если специалист тратит время на рутину вместо борьбы с угрозами, защита слабеет, поэтому автоматизация всех трех направлений позволяет экспертам сосредоточиться на отражении реальных угроз, а не на однотипных задачах. В этой статье мы расскажем про применение no-code платформы с аналитическим движком и модулей, созданных на её базе: ГосСОПКА, КИИ.

ЦЕЛИ И ОСОБЕННОСТИ ПРОЦЕССОВ

Обеспечение устойчивого функционирования объектов КИИ, особенно в кредитно-финансовой, энергетической, транспортной и телекоммуникационной сферах, является стратегическим приоритетом государства, а невыполнение требований грозит субъектам КИИ серьезными юридическими последствиями, включая уголовное преследование.

Главная проблематика реализации 187-ФЗ заключается в том, что большинство организаций, попадающих под его действие, не специализируются на информационной безопасности, однако несут прямую ответственность за защиту своих активов. Поскольку процесс категорирования, оценки рисков и контроля защищенности требует колоссальных временных и финансовых затрат при ручном исполнении, автоматизация играет ключевую роль.

ОСОБЕННОСТИ АРХИТЕКТУРЫ

Программные комплексы нового поколения, такие как Security Vision, спроектированы для устранения человеческого фактора при реализации требований 187-ФЗ. В начале 2026 года продукт получил существенное обновление, в рамках которого были актуализированы формы сведений об объектах КИИ и внедрены типовые отраслевые перечни объектов. Архитектура решения базируется на нескольких фундаментальных механизмах автоматизации:

- инвентаризация и управление активами (AM / CMDB) использует как безагентские, так и агентские методы сбора данных с операционных систем (Windows, Linux, macOS), агрегируя телеметрию из гетерогенных источников, включая системы виртуализации (vCenter), службы каталогов (Active Directory) и различных СЗИ.
- механизмы дедупликации обрабатывают получаемые данные в единое, максимально актуальное представление объекта защиты и его состояний на протяжении всего жизненного цикла.
- автоматизация процесса категорирования включает генерацию опросных листов, сбор данных от смежных подразделений и проведение расчетов интегральных показателей значимости в строгом соответствии с актуальной редакцией ПП РФ № 127.

ОТ РУЧНОГО КАТЕГОРИРОВАНИЯ К АВТОМАТИЗИРОВАННОМУ УПРАВЛЕНИЮ АКТИВАМИ

Основополагающим регламентом для субъектов КИИ выступают Правила категорирования, утвержденные ПП РФ № 127. Осенью 2025 года в нормативную базу были внесены критические изменения, сделавшие процедуру категорирования обязательной для организаций в тринадцати ключевых отраслях экономики. Редакция Постановления от 07.11.2025 года радикально расширила и детализировала перечень показателей критериев значимости объектов КИИ, что потребовало от организаций полного пересмотра ранее созданных моделей угроз.

Управление активами с точки зрения аудита и комплаенса состоит из трёх этапов (рис. 1).

Система автоматически собирает данные об активах компании при помощи собственных «агентов», через сетевой поиск и интеграции с ИТ- и ИБ-сервисами: базы данных, EDR, SIEM, которые также представлены модулями или частью модулей единой Платформы (рис. 2).

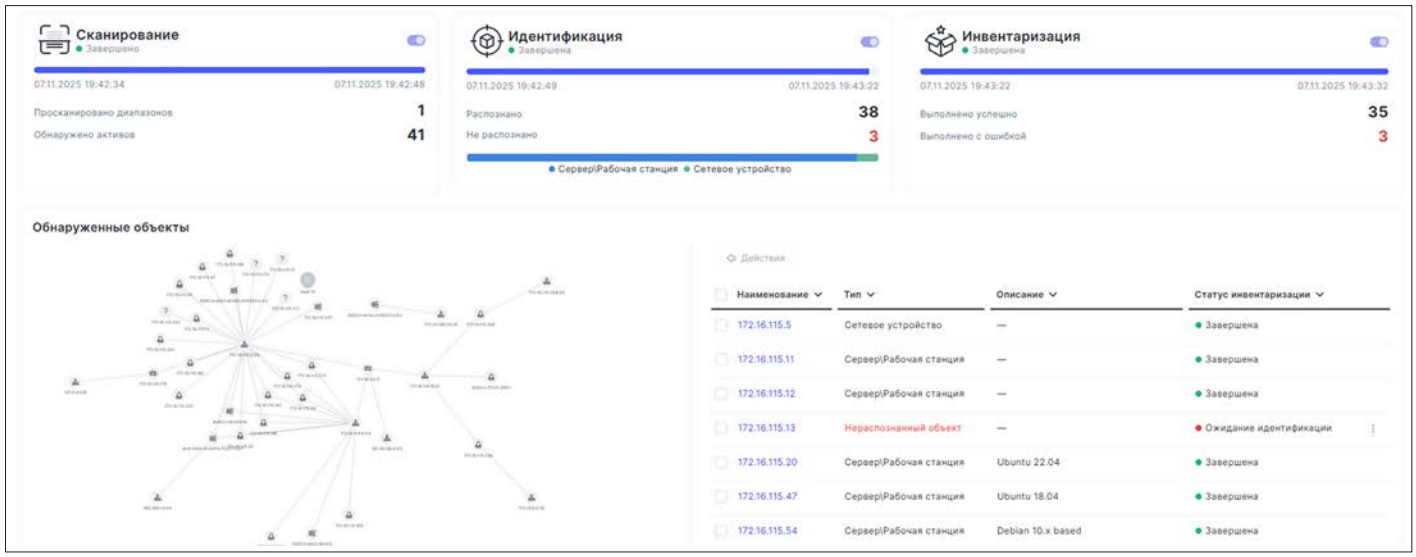


Рисунок 1. Управление активами и инвентаризацией

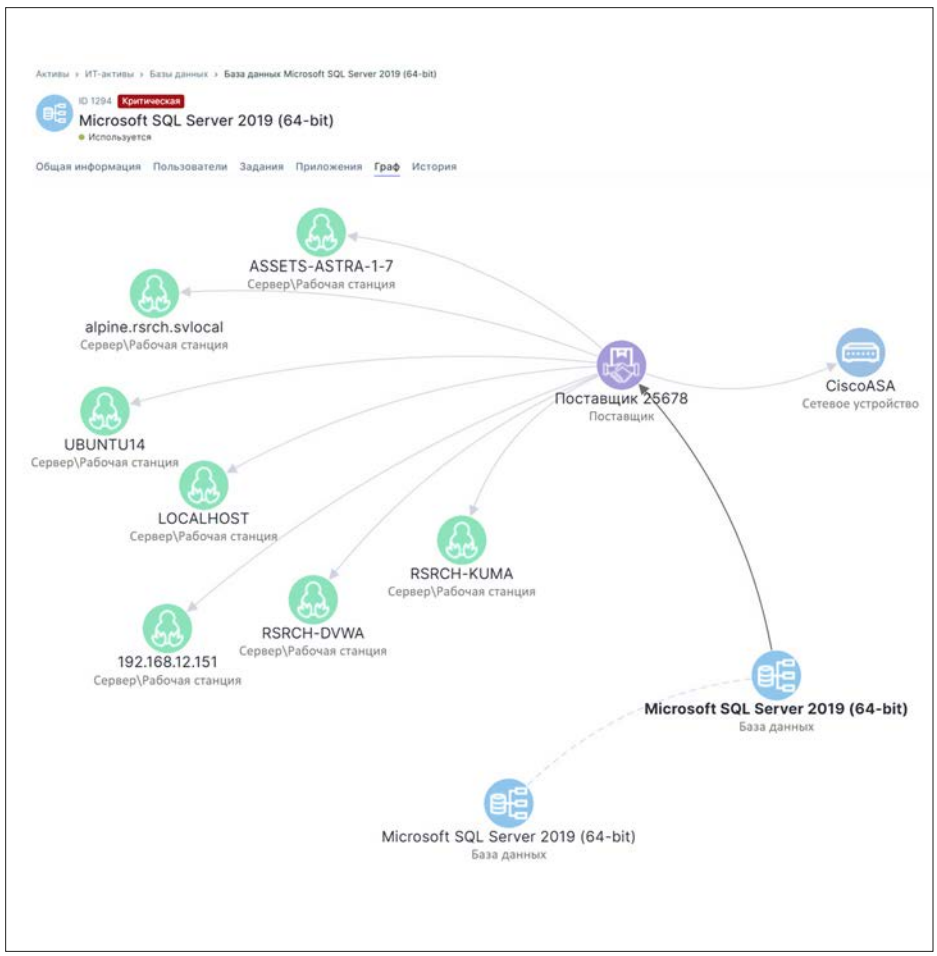


Рисунок 2. Построение ресурсно-сервисной модели

Все обнаруженные устройства, учетные записи, единицы программного обеспечения и др. технические активы собираются в ресурсно-сервисную модель автоматически. При помощи ИИ система строит карты маршрутизации (и маршруты нарушителей в случае обработки инцидентов при помощи SOAR), а аналитикам открываются возможности по связыванию объектов с бизнес-сущностями: поставщиками, подрядчиками, помещениями, процессами, приложениями и системами (рис. 3).

Затем, используя интегрированный Банк Данных Угроз (БДУ) ФСТЭК России, система анализирует возможные источники угроз, действия предполагаемых нарушителей и сценарии компьютерных атак. Алгоритмы расчетов непрерывно обновляются, полностью соответствуя методическим рекомендациям ФСТЭК.

АВТОМАТИЗИРОВАННЫЙ АУДИТ СООТВЕТСТВИЯ

Финальным этапом выступает анализ исполнения требований приказов ФСТЭК № 235, 236 и 239. Платформа осуществляет автоматическую оценку показателей состояния технической защиты, формирует единый перечень выявленных замечаний и создает интегрированный план мероприятий по их устранению с постановкой задач ответственным специалистам.

Концепция GRC (Governance, Risk Management and Compliance) представляет собой интегрированный подход к корпоративному управлению, оценке рисков и обеспечению соответствия нормативным требованиям. В 2025 году продукты направления SGRC прошли глубокую модернизацию, став более эффективными для территориально распределенных корпораций и получив расширение Governance для управления стратегическими целями и задачами кибербезопасности (рис. 4).

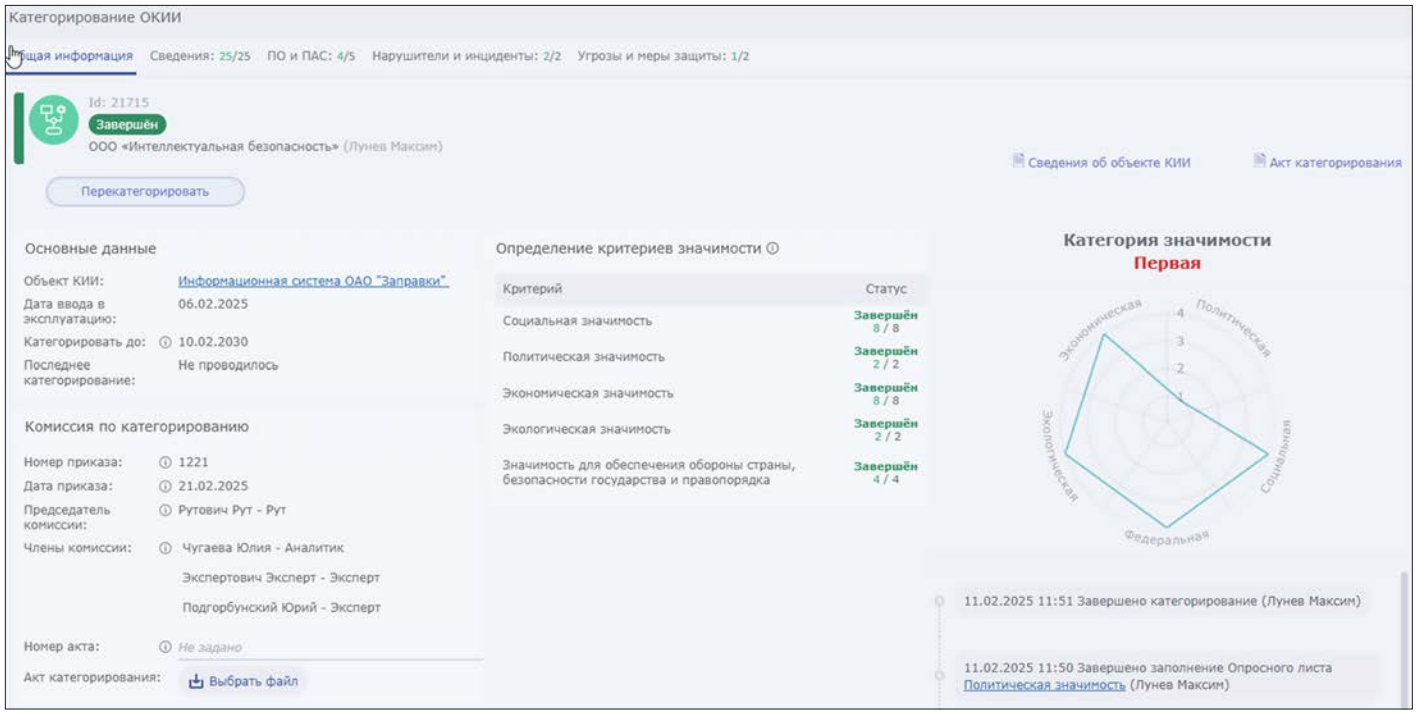


Рисунок 3. Категорирование и моделирование угроз

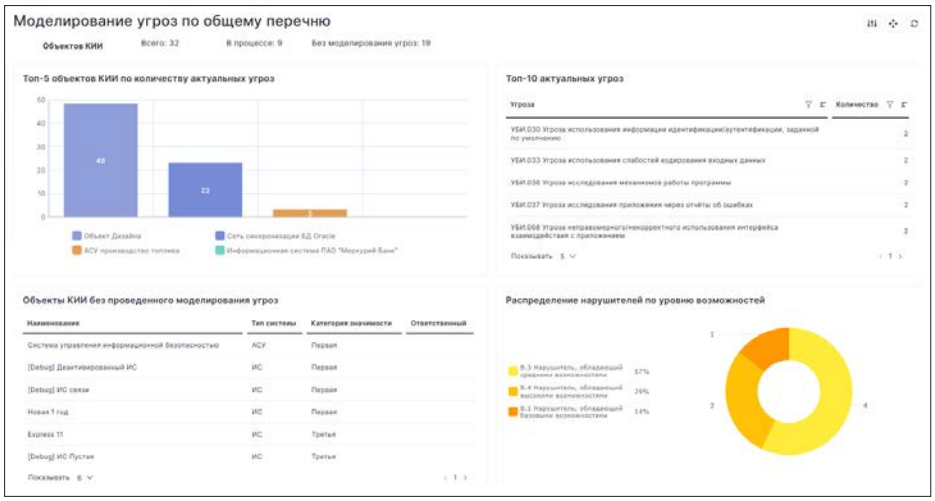


Рисунок 4. Моделирование угроз и управление соответствием для объектов КИИ

ДВУСТОРОННЕЕ ВЗАИМОДЕЙСТВИЕ С РЕГУЛЯТОРАМИ

Информационный обмен с государственными регуляторами перешел из категории опциональных задач в разряд строгих законодательных обязательств. Информирование Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) о киберинцидентах давно является обязательным для субъектов КИИ. Более того, вступление в силу Федерального закона от 14.07.2022 № 266-ФЗ сделало такое взаимодействие обязательным и для всех операторов Персональных данных (ПДн).

Законодательство предписывает передавать информацию о выявленных компьютерных атаках в ГосСОПКА в срок не позднее 24 часов с момента их обнаружения, но в условиях массированных кибератак ручной сбор артефактов и заполнение форм неминуемо ведет к нарушению данного SLA и ответственности. Для решения задачи бесперебойного информационного обмена существует специализированный модуль взаимодействия с Национальным координационным центром по компьютерным инцидентам (НКЦКИ), интегрируемый непосредственно в платформу оркестрации.

С одной стороны, модуль автоматизирует отправку уведомлений по форме регулятора (аналогичный процессу в модуле FinCERT), а с другой — собирает и обрабатывает поступающие задачи и бюллетени (в т.ч. с применением ИИ для неструктурированных данных).

ЗАКЛЮЧЕНИЕ

Модульность платформы Security Vision позволяет закрыть задачи как точечно (моделирование угроз, оценка соответствия и аудит, управление активами и инвентаризацией, управление уязвимостями и инцидентами, анализ угроз и т.д.), так и комплексно (за счет синергии трех направлений: технологии, процессы и аналитики).

Специалисты по информационной безопасности могут работать с коллегами в единой системе, но с разными представлениями (витринами данных), позволяющими закрывать задачи с максимальной автоматизацией и прозрачностью.

КАК НЕ СТАТЬ ПЛАЦДАРМОМ ДЛЯ АТАК НА ЦЕПОЧКУ ПОСТАВОК

Николай ОМЛАНД
руководитель направления SOC, SolidLab Group

Максим ИЛЬИН
руководитель по развитию продуктов безопасности инфраструктуры, SolidLab Group

Среди представителей различных отраслей, где нет четких нормативных требований, часто встречается позиция: «Мы никому не интересны, чтобы нас взламывать». К сожалению, данный подход делает небольшие компании уязвимыми для киберпреступлений и повышает риск их использования в качестве стартовой площадки для скоординированных атак на более крупные компании. Компрометация цепочки поставок уже является одним из ключевых путей проникновения в инфраструктуру целевой организации. Инцидент с CrowdStrike в 2024 году показал, что даже крупнейшие мировые корпорации в области кибербезопасности могут быть уязвимы к подобным атакам.

С ЧЕГО НАЧАТЬ НЕБОЛЬШИМ КОМПАНИЯМ?

1) Обеспечить процесс инвентаризации и непрерывный мониторинг поверхности атаки. При анализе защищенности инфраструктуры нередко обнаруживаются уязвимости, позволяющие осуществить несанкционированный доступ через неконтролируемые сегменты сети, которые требуют значительных ресурсов для устранения недостатков со стороны ИТ-инфраструктуры, что приводит к понижению их приоритета со стороны владельца.

2) Использовать более строгие политики безопасности. Крупные организации, в которых отсутствуют четко определенные нормативные требования, в отличие от малого и среднего предпринимательства (МСП), проявляют осторожность при внедрении строгих политик безопасности. Как правило, существуют исключения из общих правил: например, учетную запись генерального директора не допускается блокировать, сервер бухгалтерии не может быть изолирован, а также существует страх перед активацией расширенного логирования в бизнес-системах. Зачастую согласования и изменения могут затянуться на месяцы или годы либо быть отложены в долгий ящик.

3) Уделить больше внимания настройке расширенных параметров аудита. Отсутствие больших бюджетов заставляет небольшие компании быть более прагматичными и активнее использовать штатные средства и типовые решения. В данных условиях логирование систем и сбор событий с последующей аналитикой представляют собой доступную альтернативу корпоративным решениям. Однако без должного опыта это может занять очень много времени. В то время как мы, используя свою экспертизу, предоставляем готовые решения этих задач под ключ.

Например, мы помогаем компаниям усилить цепочку поставок, в которых участвуют МСП, выстроив оперативные каналы коммуникации, обмена знаниями и системные процессы контроля.

КАК ЗАЩИТИТЬСЯ КРУПНЫМ КОМПАНИЯМ

На основании накопленного опыта в области предотвращения атак на цепочки поставок нашей компанией были разработаны комплексные методы контроля подрядчиков и оперативного выявления инцидентов, связанных с данной категорией угроз.

В результате внедрения нашего Security Operations Center (SOC) разрабатываются методики, которые охватывают все ключевые аспекты взаимодействия между подрядчиками, включая:

1. Выявление «слабого звена». Нет необходимости контролировать всех подрядчиков одинаково. Первым делом необходимо провести инвентаризацию своих связей и выявить подрядчиков, у которых низкий уровень безопасности, но при этом существует доступ к вашим системам. Наши эксперты консультируют заказчиков по способам оценки в соответствии с собственными методиками.

2. Организация мониторинга недостатков. Недостатки могут вы-

являться в первую очередь через новые инциденты, в которых присутствуют системы или пользователи подрядчика. Помимо этого, необходимо уделить внимание проактивному поиску угроз (Threat Hunting) для выявления следов компрометации систем и пользователей подрядчика в границах вашей инфраструктуры.

3. Обеспечение контроля устранения недостатков подрядчиками. Процесс устранения недостатков требует системного подхода. Зачастую этого сложно добиться от подрядчика, однако здесь могут помочь четкие границы и сценарии взаимодействия:

- Включение в договор с подрядной организацией пунктов об обязательных требованиях ИБ и ответственности за их невыполнение.
- Установление четких сроков на исправление критических недостатков, которые могут повлиять на ваши системы или привести к утечке данных, а также описание критериев, по которым можно определить критичность и степень влияния.
- Регулярные контрольные проверки для подтверждения устранения недостатков.

КАК МСП ПОДГОТОВИТЬСЯ К РЕАГИРОВАНИЮ НА УГРОЗЫ

На сегодняшний день рынок систем ИБ позволяет выбрать продукт не только для больших компаний, но и для МСП. Внедрение Security information and event management (SIEM) является одним из первых шагов. При внедрении SIEM ключевым фактором является правильная подготовка логов и внимательная настройка аудита на конечных хостах.

В наших проектах мы стремимся оптимизировать поток событий для снижения затрат на лицензию SIEM путем точечной доработки состава событий. Избыточный поток данных может быстро исчерпать лимиты лицензии SIEM, а без контроля качества данных даже базовые правила корреляции могут работать некорректно.

При этом важно понимать, что стандартные правила корреляции «из коробки» — это лишь фундамент, требующий обязательной адаптации под специфику вашей инфраструктуры. Поэтому мы рекомендуем сначала детально изучить структуру событий конкретного источника и проверить, насколько поля в правилах корреляции совпадают с фактическими данными. На этом же этапе будет не лишним убедиться, что подключенный аудит работает корректно и события поступают, чтобы не ждать алертов, которые никогда не придут.

ОСОБЕННОСТИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ В МСП

Когда дело доходит до реагирования на инциденты, МСП часто совершают ошибку, пытаясь самостоятельно построить миниатюрную копию корпоративного SOC. Однако для решения задач реагирования на инциденты не нужно копировать подходы больших компаний с большими бюджетами. Важнее правильно распределить роли и отчетливо понимать, что возможно сделать самостоятельно, а для каких процессов лучше использовать аутсорсинг или гибридную модель.

Часто высказывается мнение, что создание собственного центра мониторинга и реагирования на инциденты информационной безопасности (SOC) сопряжено с повышенными затратами на этапе внедрения, но позволяет оптимизировать расходы в долгосрочной перспективе.

Однако необходимо учитывать, что методы и техники, используемые киберпреступниками, постоянно эволюционируют. В связи с этим поддержание высокого уровня квалификации подразделения SOC требует постоянной практики расследования сложных инцидентов, что недостижимо не только в реалиях МСП, но и в некоторых крупных компаниях.

Наши подходы адаптируются под конкретные потребности бизнеса, учитывая его особенности, и помогают развивать собственные компетенции заказчика в области кибербезопасности.

Однако если у вас уже есть своя SIEM, которая работает, не обязательно от нее отказываться. Наш опыт показывает, что адаптация и доработка существующей инфраструктуры силами внешнего эксперта часто дают лучший результат, чем попытка переделать всё с нуля. Тем самым сохраняется контроль над хранением данных, но используется опыт профессионального центра мониторинга.

Гибридная модель подразумевает передачу на провайдера услуг только некоторого функционала.

На основании нашего опыта гибридной схемы взаимодействия мы предлагаем различные подходы, которые учитывают все особенности заказчика, например передачу функций, требующих экспертизы. На стороне заказчика при этом остается функция гибкого управления процессами.

КАК МЫ МОЖЕМ ПОМОЧЬ ЗАКАЗЧИКУ

- Мониторинг 24×7.
- Глубокая экспертиза и расследование.
- Поиск недостатков в конфигурациях.
- Проактивный поиск угроз (Threat Hunting).
- Разработка индивидуальных правил корреляции.
- Подключение нетиповых источников.
- Помощь в выстраивании индивидуальных процессов реагирования.

* * *

В конечном итоге гибридная модель или полный аутсорсинг — это оптимальное решение для МСП, которое позволяет небольшим компаниям получить доступ к квалифицированной экспертизе за прогнозируемую стоимость.

Это не только снижает нагрузку на внутренних специалистов, но и дает четкий сигнал крупным заказчикам: их подрядчик — не слабое звено, а зрелый партнер, способный гарантировать безопасность.

КОГО И КАК АТАКОВАЛИ В 2025 ГОДУ

Вредоносное ПО и несанкционированный доступ к системам были основными угрозами для российских компаний в 2025 году, а промышленность и региональные органы власти — самыми атакуемыми секторами экономики. Такие выводы сделали эксперты ГК «Солар» на базе аналитики данных своего центра противодействия кибератакам Solar JSOC.

В фокусе внимания экспертов оказалось около 300 организаций из разных отраслей экономики: госсектор, финансы, нефтегазовая отрасль, энергетика, телекоммуникации, крупный ритейл, добывающая и пищевая промышленность, транспорт и логистика и др. Все компании представляют сегмент Large Enterprise и Enterprise с количеством сотрудников от 500–1000 человек и более, оказывают услуги в разных регионах страны.

МАСШТАБЫ АТАК

Всего за 2025 год мониторинг Solar JSOC выявил 1,16 млн событий ИБ — подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний (в 2024 г. — 1,81 млн событий). В целом же с точки зрения общего количества событий ИБ за прошедшие четыре года прослеживается тренд на снижение, однако до показателей 2022 года и ранее всё ещё далеко (рис. 1).

На фоне снижения количества зафиксированных подозрений на инциденты вырос процент подтвержденных заказчиками инцидентов: более 33 тыс.— в 2025 г. против 31,5 тыс.— в 2024 г.

На горизонте четырех лет по этому показателю видны отчетливые всплески, связанные с политической обстановкой. Например, значительный рост атак в 3 квартале 2022 г. был связан с вхождением новых территорий в состав РФ. При этом каждый год мы видим похожую «сезонность»: в начале года относительное затишье, затем рост числа инцидентов, причем в последние два года наиболее «ударным» во всех смыслах становится конец года (рис. 2).

КАТЕГОРИИ ПОДТВЕРЖДЕННЫХ ИНЦИДЕНТОВ

В этом году мы немного пересмотрели категории инцидентов для возможности погрузиться «вглубь» каждой из них и оценить статистику в других разрезах. Она представлена ниже (рис. 3).

ЗАРАЖЕНИЕ ВРЕДОНОСНЫМ ПО

В топе, как и в прошлые годы, вредоносное ПО. Мы каждый год отмечаем, что это достаточно логично: антивирусы, EDR-решения хорошо делают свою работу и при наличии вердиктов от них, как правило, ИБ-специалисту на стороне заказчика достаточно просто «подтвердить» факт инцидента.

Однако в этом году мы видим заметный рост инцидентов, связанных с ВПО (на 6 п.п.). При этом, если погрузиться чуть глубже в категории, мы все еще фиксируем большую часть детектов по известному и типовому ПО (29% из 36%). Явная классифика-

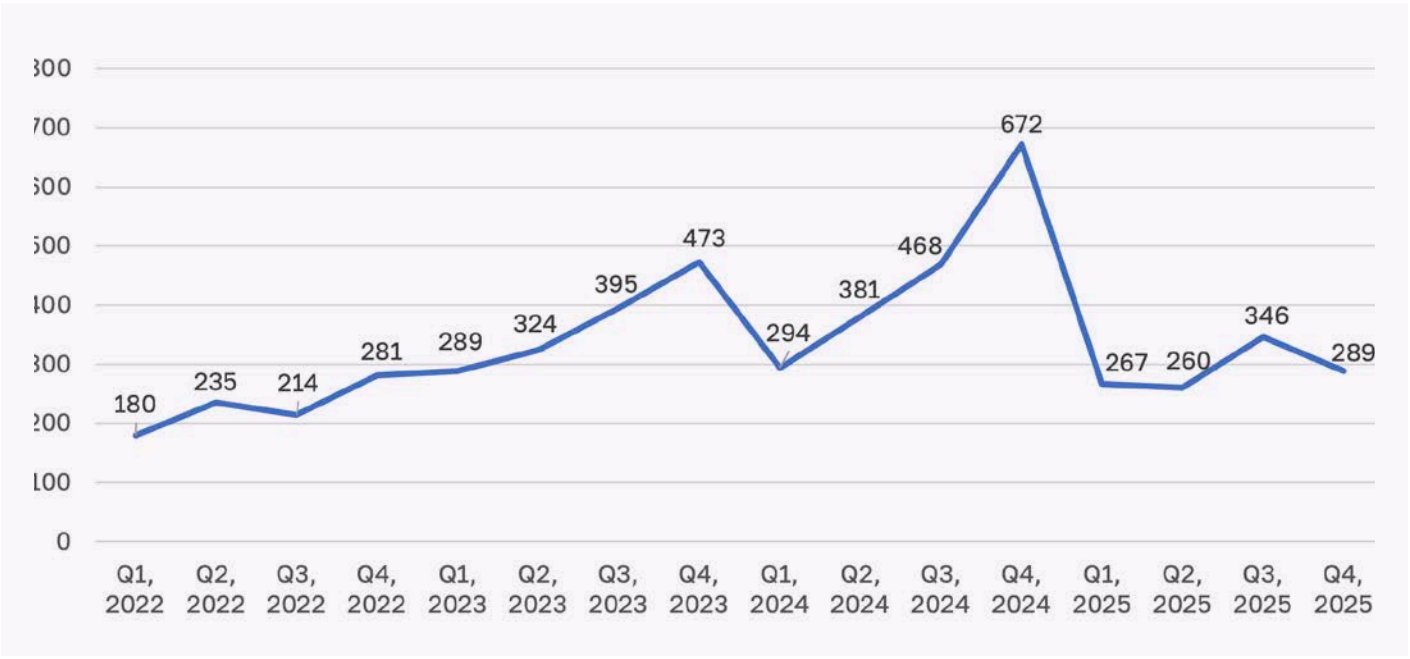


Рисунок 1. Динамика событий ИБ в 2022–25 гг., тыс.

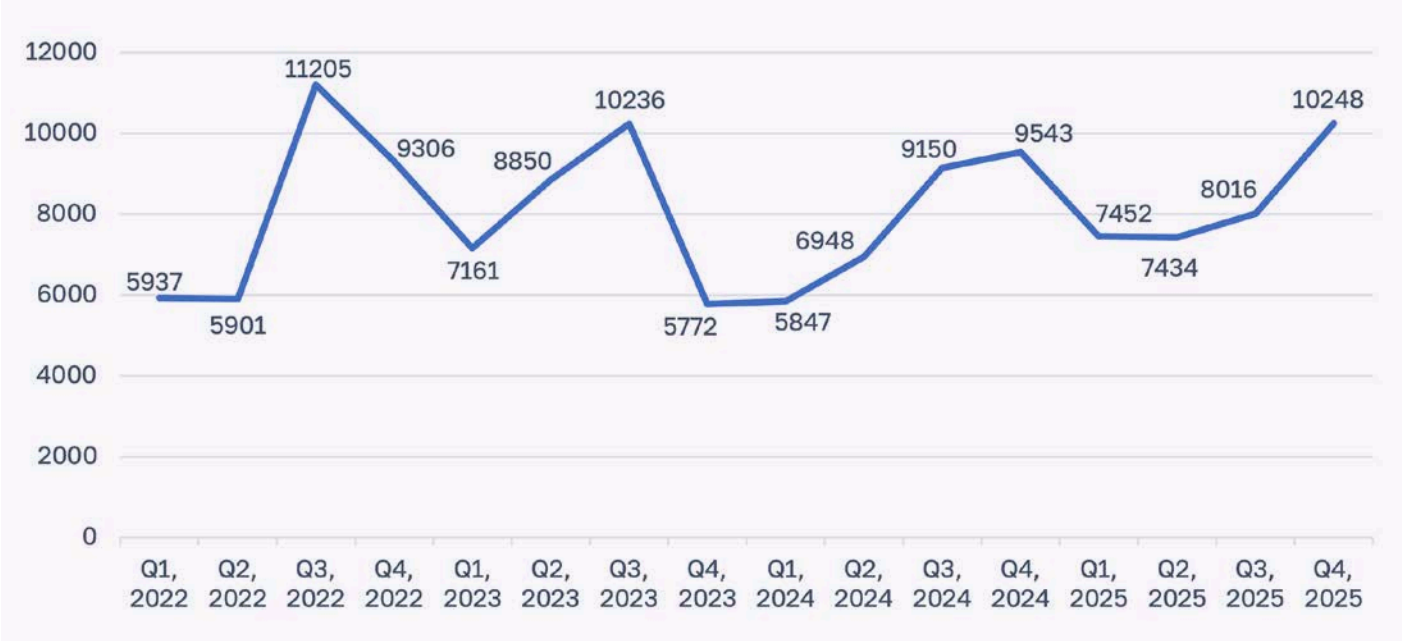


Рисунок 2. Подтвержденные инциденты ИБ в 2022–25 гг.

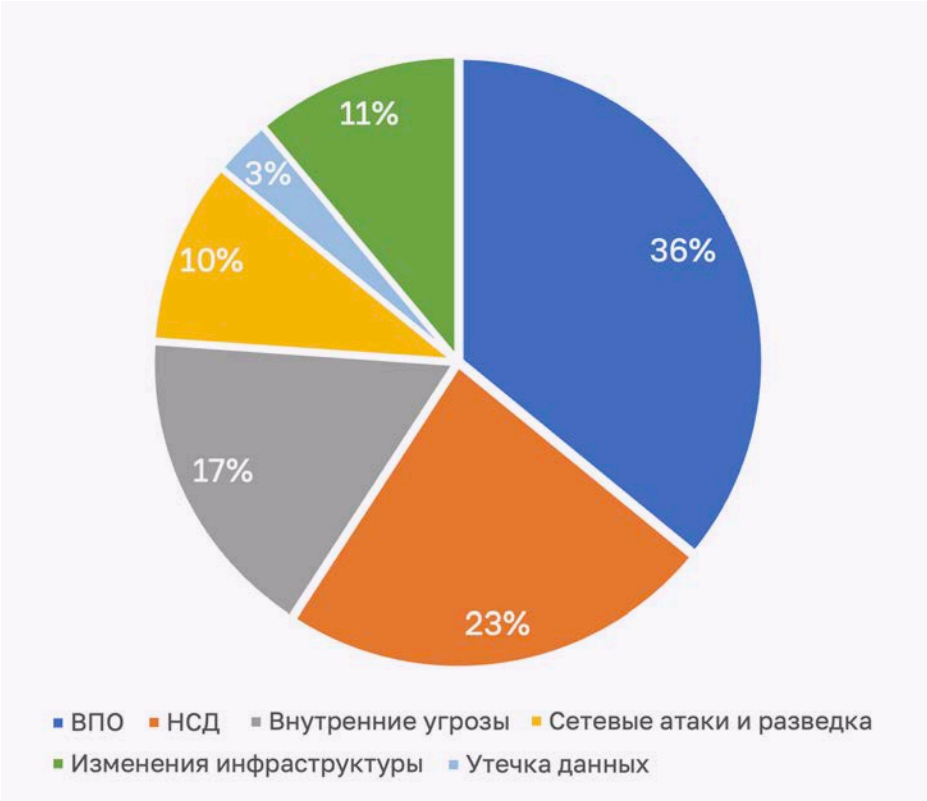


Рисунок 3. Категории подтвержденных инцидентов в 2025 г.

ция по эвристике, хакерским утилитам, майнерам и т.д. — занимает лишь малую долю. Эту тенденцию мы связываем в первую очередь с тем, что в большинстве случаев все же атакующие стараются использовать уже готовые инструменты и легитимные утилиты для атак на компании. Происходит все большая автоматизация атак: с развитием автоматизированных платформ (например, Malware-as-a-Service) злоумышленники могут массово распространять вредоносное ПО, что снижает барьер входа для атакующих и увеличивает общее количество таких инцидентов.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП

В эту категорию вошли различные техники, касающиеся попытки получить доступ в инфраструктуру клиента: атаки на веб-приложения, брутфорсы, атаки на системы аутентификации и т.д. Здесь очень хорошо прослеживается тренд, когда количество и качество таких атак растет под вполне конкретные события на уровне государства и/или компании. Например, в динамике веб-атак отчетливый всплеск пришелся на сентябрь, в период Единого дня голосования в России — очевидно, хакеры рассчитывали оказать деструктивное воздействие на избирательный процесс.

КЛЮЧЕВЫЕ ОТРАСЛИ И КИБЕРУГРОЗЫ

Доля атак на ту или иную отрасль рассчитывалась нами исходя из среднего числа атак на организацию в этой отрасли. В этом году фокус злоумышленников немного сместился. Если в 2024-м в топ-3 были госсектор (ФОИВ, РОИВ и другие госорганизации — 55%), финсектор (18%) и транспортная отрасль (16%), то в 2025 году особенно выделяются промышленность (добывающая и пищевая — совокупно 23%), а также госсектор (ФОИВ и РОИВ — совокупно 14%, из которых РОИВ — 11%). Также

Рисунок 4. Распределение инцидентов по отраслям в 2025 г.

в числе наиболее атакуемых секторов остаются торговля, финансовая и транспортно-логистическая отрасли, занимающие равные доли в 10% (рис. 4).

АТАКИ НА ПРОМЫШЛЕННОСТЬ

В 2025 году 12% всех инцидентов пришлось на добывающую промышленность. Она обеспечивает 40% экономики и ориентирована на экспорт. Остановка добычи ресурсов для нашей экономики может быть использована как инструмент давления в международных отношениях, что повышает интерес к таким объектам со стороны государственных и политически мотивированных хакеров с целью деструктивной деятельности или кибершпионажа. Также они являются привлекательной мишенью для вымогателей: остановка производства из-за атаки грозит большими финансовыми потерями, поэтому компании могут быть более склонны платить выкуп злоумышленникам.

Активная цифровизация в добывающей промышленности также создаёт определённые киберриски. Например, интеграция информационных (IT) и операционных (OT) сетей расширяет поверхность атаки, позволяя злоумышленникам проникать из корпоративных сетей в промышленные. В то же время важное промышленное оборудование часто управляется устаревшими, неподдерживаемыми операционными системами, что затрудняет их обновление и защиту.

Помимо прочего, добывающая промышленность активно взаимодействует с подрядчиками, поставщиками и логистическими компаниями. Если любой из партнёров становится жертвой атаки, это может привести к компрометации всей цепочки поставок.

В топ наиболее атакуемых отраслей попала и пищевая промышленность. Эта отрасль, как и вся промышленность, зависима от иностранного ПО и ОС устаревших версий, что является одним из важных факторов большого количества инцидентов. Также высокое число атак на сектор связано с его стратегической значимостью для населения и зависимостью от сложных цепочек поставок.

АТАКИ НА РОИВ

Рост числа кибератак на региональные органы власти (РОИВ) России — это наблюдаемый тренд, который связан с совокупностью факторов. Ключевые из них представлены ниже.

Мотивация атакующих. После начала спецоперации резко активизировались проукраинские хактивистские группировки. Их цель — нанести максимальный ущерб критической инфраструктуре и государственному аппарату России, включая региональный уровень. Не исключено также участие госструктур других стран в поддержке или проведении атак для дестабилизации обстановки внутри России и нанесения идеологического и репутационного ущерба.

При этом в последнее время наблюдается смещение фокуса злоумышленников с финансовых целей на дестабилизацию: если раньше многие атаки (особенно с шифровальщиками) преследовали финансовую выгоду, то сейчас часто главная цель — нарушить работу, украсть и обнародовать данные, посеять хаос. Для них РОИВ — это «близкая» и символически важная цель. Взлом сайта губернатора

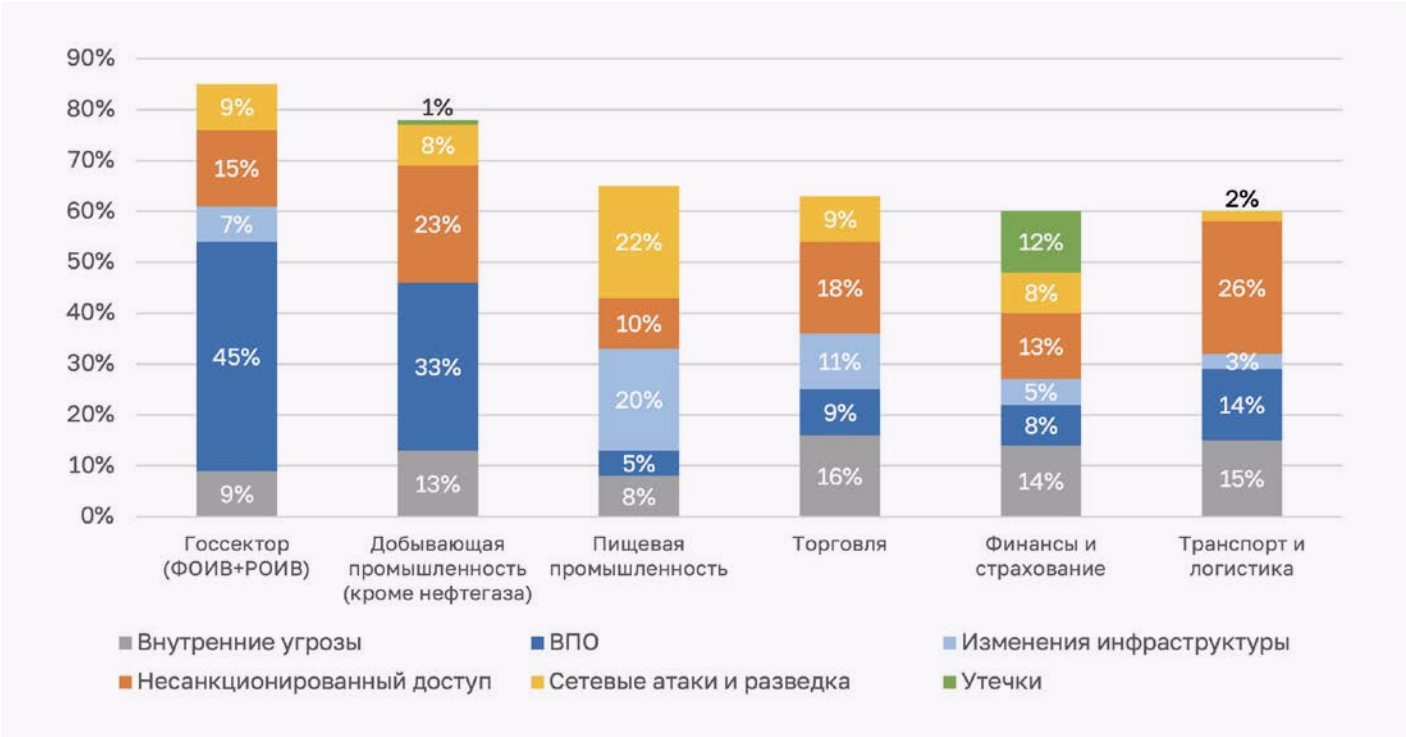


Рисунок 5. Типы инцидентов в наиболее атакуемых отраслях

или правительства региона — это не только технический инцидент, но и удар по имиджу власти, демонстрация уязвимости.

Кроме того, в системах РОИВ хранятся персональные данные граждан, информация по соцобеспечению, ЖКХ, управлению территориями и т.д. Их нарушение или шифрование может парализовать работу жизненно важных служб. Но и сами по себе эти данные представляют ценность для кибершпионов.

Инфраструктура РОИВ может стать для хакеров и точкой входа в более крупные госструктуры федерального значения, атаковать которые напрямую гораздо сложнее. По мнению экспертов, нынешний повышенный интерес группировок к РОИВ выглядит как «прощупывание» киберландшафта перед более крупными атаками.

Уровень киберзащиты РОИВ. Если федеральные органы и силовые структуры уделяют повышенное внимание ИБ и получают серьезное финансирование на кибербезопасность, то в регионах ситуация часто хуже. Бюджеты на безопасность меньше, квалификация ИТ-специалистов может уступать столичной. В регионах часто можно встретить устаревшие версии CMS (систем управления контентом сайтов), операционных систем и офисных пакетов, содержащих известные уязвимости.

Еще одна значимая уязвимость — человеческий фактор. Регулярные тренировки по кибербезопасности и повышение цифровой грамотности сотрудников не всегда являются приоритетом, что повышает киберриски.

Таким образом, в случае с РОИВ злоумышленники получают большую «поверхность атаки». У каждого региона — свой сайт, свои сервисы (часто разработанные сторонними подрядчиками с неизвестным уровнем безопасности), свои сотрудники. Таким образом, хакеры могут атаковать через уязвимости в сайтах, системы электронных услуг, почтовые рассылки (фишинг) и через самих подрядчиков, которые имеют доступ к системам заказчика (например, компания-разработчик регионального портала государственных услуг).

РИТЕЙЛ

Сфера торговли остаётся «золотой жилой» для киберпреступников по всему миру за счет очень высокой зависимости от непрерывности бизнеса и ценности обрабатываемых данных (включая персональные данные клиентов, данные платежных карт и транзакции). Интересно, что здесь как раз сильно ниже доля категории вредоносного ПО — акцент смещается на внутренние угрозы и попытки несанкционированного доступа (рис. 5).

ВЫВОДЫ

Геополитика всё ещё остаётся основным драйвером и «поставщиком» инцидентов в жизнь российских организаций. Общая напряженность в мире становится повседневной реальностью. Отчасти с этим мы связываем отсутствие «взрывного» роста количества кибератак. Поток инцидентов растет, но достаточно равномерно.

ВПО было и остаётся большой проблемой. Это связано в том числе со сложностью контроля распределенных и разнородных инфраструктур.

В числе наиболее атакуемых секторов — РОИВ, добывающая и пищевая промышленность. Также в топе остаются ритейл, финансово-страховой и транспортно-логистический сектора. Ключевая причина таких атак — в стратегическом значении этих отраслей (а значит, в возможности нанести максимальный ущерб государству и обществу).

APPSEC.AI GATE

КАК ЗАЩИТИТЬ ИИ-РЕШЕНИЯ В ФИНАНСОВОЙ ОРГАНИЗАЦИИ

Юрий ШАБАЛИН
директор по развитию технологий искусственного интеллекта, Swordfish Security

Банки и финтех-компании внедряют языковые модели быстрее всех. Большие языковые модели (LLM) уже обрабатывают клиентские обращения, помогают аналитикам, генерируют документы. Но у этого прогресса есть обратная сторона: каждый LLM-сервис — это новая поверхность атаки, которую традиционные ИБ-инструменты не покрывают.

Я общаюсь с Chief Information Security Officers (CISO) финансовых организаций и слышу один вопрос: «Мы понимаем, что LLM нужно контролировать, но чем?». WAF не понимает семантику промпта. Data Loss Prevention (DLP)-система не видит, что модель в ответе выдала системный промпт или внутренний IP. IDS не отличит легитимный запрос от jailbreak-атаки. Угроза — на уровне смысла текста, а не сетевого трафика.

Именно для этого мы создали AppSec.AIGate.

ЧТО ЭТО И КАК РАБОТАЕТ

AIGate — шлюз безопасности, который разворачивается перед языковой моделью как прозрачный прокси. Для приложений и пользователей ничего не меняется: они обращаются к модели как обычно, используют свои API-ключи. Но между ними и LLM теперь стоит слой, который анализирует каждый запрос и каждый ответ в реальном времени.

Gate работает с любыми провайдерами — облачными и локальными. Подключение нового провайдера не требует изменений в клиентском коде.

ЗАЩИТА МОДЕЛИ ОТ АТАК

На входе AppSec.AIGate перехватывает запрос и прогоняет его через несколько детекторов параллельно.

Jailbreak и prompt injection. Система определяет, пытается ли пользователь обойти системные инструкции модели — через ролевые сценарии, кодирование, многоходовые цепочки промптов. Порог срабатывания настраивается для каждого LLM-профиля отдельно.

Обнаружение PII. Gate распознаёт более 20 типов чувствительных данных: паспортные данные, ИНН, СНИЛС, номера карт, медицинские и иные данные. Обнаруженное можно замаскировать, удалить или заблокировать весь запрос — в зависимости от политики.

Контент-безопасность. Запрос классифицируется по 9 категориям: насилие, нелегитимные действия, раскрытие PII, попытки jailbreak и другие. Каждая категория — независимый порог, который настраивается под конкретный сценарий использования.

Защита от обхода. Gate нормализует Unicode перед анализом — гомоглиф-атаки (подмена кириллицы на латиницу для обхода фильтров) не сработают.

КОНТРОЛЬ ТОГО, ЧТО ОТДАЁТ МОДЕЛЬ

Ответ LLM тоже проходит через AppSec.AIGate. Система проверяет выходной поток на утечки: персональные данные клиентов, приватные ключи, внутренние адреса — и отдельно отслеживает утечку системного промпта. Если модель начинает отдавать то, чего отдавать не должна, Gate маскирует данные или блокирует ответ целиком. Всё это потоково, без заметной задержки.

ПОЛИТИКИ И КОМПЛАЕНС

Для CISO финансовой организации в обеспечении безопасности ИИ особенно критичны две вещи: гибкость политик и отчётность.

Политики применяются на лету — без перезапуска и без привлечения разработчиков. Можно определить кастомные правила: заблокировать упоминание конкурентов, запретить обсуждение определённых тем, ограничить использование LLM по ролям.

Gate ведёт полный аудит всех действий и генерирует отчёты по инцидентам с персональными данными — с классификацией по категориям 152-ФЗ — в PDF и CSV. Это не заменяет комплаенс-процессы, но даёт конкретный инструмент для контроля обработки персональных данных (ПДн) в контексте использования LLM. Для интеграции с Security Operations Center (SOC) есть экспорт событий в Security Information and Event Management (SIEM)-систему.

КАК НАЧАТЬ

Gate поддерживает режим мониторинга: система анализирует весь трафик к модели, логирует события, но не блокирует. Это позволяет за пару недель увидеть реальную картину — какие запросы приходят, что отвечает модель, где риски — и только потом включить политики на основе реальных данных.

Подробнее о продукте — на сайте: *https://appsec-aigate.ru*

«ЦИФРА – ОНА КАК КУКУШОНОК!»

НЕСТАНДАРТНАЯ СИТУАЦИЯ ТРЕБУЕТ АДЕКВАТНЫХ ПОДХОДОВ

Герман КЛИМЕНКО
председатель Совета Фонда развития цифровой экономики, сопредседатель Совета по развитию информационных технологий и цифровой экономики ТПП РФ, советник президента Российской Федерации В. В. Путина по вопросам развития Интернета в 2016–2018 гг.

Цифровая экономика – это, безусловно, один из символов нынешнего времени. Но создавать эту непростую конструкцию приходится в сложных условиях нарастающих геополитических противостояний, когда система глобального разделения труда разваливается. Для отрасли цифровых технологий это означает новые вызовы и риски. Как они выглядят сегодня? Каким образом на эти вызовы реагируют российские предприятия и государство? На вопросы BIS Journal отвечает Герман Клименко.

КУКУШОНОК

– Герман Сергеевич, создание цифровой экономики – практическая задача, а не только красивая идея. Какие аспекты, по Вашему мнению, являются критически важными для ее успешного решения?

– Критически важно понимание логики цифровизации большой страны. Нельзя занять рынок «цифрой» там, где невозможно обеспечить сервисы цифровыми данными. «Цифра» приходит только на подготовленную территорию, и тогда начинается экспоненциальный рост. Тут нет постепенного проникновения. По сути, речь идет о том, что нужно построить цифровой двойник – создать полноценное информационное покрытие и организовать зону стыковки с реальным сектором. Но как только вы это сделали, преодолели порог «критической массы», и все понеслось! Вы же видите, как развивается «цифра» в Москве, – по экспоненте. Это потому, что новые услуги появляются на основе тех, что уже были оцифрованы ранее.

Обратите внимание: когда приходили предыдущие волны промышленной революции, они накатывали в щадящем режиме. Образно говоря, трамваи сменяли лошадей, но некоторое время они существовали на улицах одновременно. А цифра – она как кукушонок! Современный МФЦ не может существовать вместе с ЖЭКом советского образца.

Поэтому одна из больших проблем нашей экономики в том, что разные отрасли по-разному заточены на цифровизацию, а также в том, что в Москве одна экономика, в областном центре Центральной России другая, в чернозёмной станице третья, а в дальней сибирской деревне четвёртая.

О ЦИФРОВОМ НЕРАВЕНСТВЕ РЕГИОНОВ

– Об этом недавно говорила вице-премьер Татьяна Голикова на итоговой коллегии Минтруда: «... сегодня автоматизация рутинных процессов недостаточная. 48% регионов сегодня находятся на начальном этапе использования ИТ-технологий».

– Да. Все дело – в наших огромных пространствах. Это в Европе с их небольшими странами столицы не сильно отличаются от регионов, а цифровизовать госуправление страны Эстонии (помните, как нам когда-то ставили это в пример?) можно с по-

мощью одного проекта внедрения типового технического решения и на кредит от корпорации Microsoft.

У нас уровень цифровизации разных регионов принципиально разный. И отдельных денег и усилий стоит организация смычки между старой инфраструктурой предоставления услуг и новой, цифровой. Ведь, например, появление цифрового паспорта не отменяет хождения бумажного документа, и нужно поддерживать функционирование обеих систем удостоверения личности.

Поэтому задача создания цифровой экономики в России на порядок сложнее, чем в той же Европе: нужно внедрить продукт, которым будут одинаково пользоваться люди, живущие на разных территориях в сильно разных условиях.

— Получается, что для создания полноценного масштабного фундамента «цифры» наличие очаговых цифровых экономик — это нормальный путь?

— Знаете, я присутствовал при начале всей этой истории, и тогда казалось, что ситуация безнадёжная... Потому что, когда у вас четыре типа цифровизации одновременно, как в примере выше, просто не хватает профессионального ресурса, чтобы справиться с этой задачей. Но за некоторое время удалось вырастить отдельные куски цифровых территорий, и параллельно наращивался опыт их стыковок. Теперь, по большому счёту, одни регионы помогают другим, делясь с ними технологиями и опытом в соответствии с их уровнем развития.

Соглашусь с теми людьми, которые говорят, что российский портал госуслуг — самый продвинутый и уникальный в мировом масштабе. Действительно, этими услугами одновременно пользуются люди и на Камчатке, и в Москве, и в Биробиджане. Это уникальный проект по степени сложности! Чтобы сделать это, пришлось решить массу сопутствующих задач. И наши банки — я это точно знаю, поскольку бываю в других странах по бизнес-делам,— лучшие в мире по уровню развитости цифровых услуг. Вы бы видели глаза одного западного банкира, когда я показывал ему на своем смартфоне, как я бесплатно и буквально в один клик завожу виртуальные банковские карты, настраиваю их на разные задачи!

Несомненно, все это серьезное конкурентное преимущество: несмотря на то, что цифровая инфраструктура разных территорий может сильно различаться, мы научились организовывать стыки между ними и предоставлять услугу на едином хорошем уровне. И это, между прочим, дает нам большие возможности тиражирования нашего опыта, например, в Африке.

О ЦЕНЕ ТОТАЛЬНОЙ «ЦИФРЫ»

— Почему же тогда почти половина регионов до сих пор находится на начальном уровне цифровизации?

— Помню, как в бытность мою советником Президента РФ один из губернаторов попросил: украдите для меня медицину Москвы. И очень удивился, когда услышал, что ему все с радостью передадут. Но сильно расстроился, когда узнал, что все необходимые мероприятия обойдутся в сумму, превышающую общий бюджет области... Но иначе никак. Для того чтобы больница стала цифровой, мало приобрести несколько десятков компьютеров и хирургического робота да Винчи, нужно проложить всю кабельную инфраструктуру, создать множество баз данных и автоматизированных рабочих мест сотрудников. То есть здесь тоже нужно накопить «критическую массу» информатизации, после которой начнется взлет «цифры».

КАКИЕ ПРОФЕССИИ УНИЧТОЖИТ «ЦИФРА»?

— Как «цифра» меняет госуправление на практическом уровне?

— Ключевой аспект управления в цифровой экономике — это то, что любое действие оставляет цифровой след. Нет лучшей системы контроля за деятельностью чиновников, чем «цифра»! Еще один важный аспект — возможность заменить «цифрой» немалую часть чиновников. Помните, что об этом говорил в прошлом году глава Минцифры Максут Шадаев? Как минимум, 50% чиновников способен заменить искусственный интеллект. При этом он подчеркнул, что занять место, например, учителей и врачей у технологии вряд ли получится, однако встать на место госслужащих она точно может. И если этого пока не происходит, то только по причине социальных последствий, включая учет баланса элит и прочие тонкие механизмы. Это весьма серьезная часть истории «цифры», и рудименты доцифрового госуправления должны сами уйти в небытие.

Очень хорошо, что в нашей стране два руководителя высокого уровня — глава Правительства РФ Михаил Мишустин и министр цифрового развития Максут Шадаев — прекрасно это понимают и не торопятся. Потому что сегодня технически это сделать можно, а вот политически — нельзя. Поэтому,

думаю, еще лет пять штаты будут сокращать, но очень плавно.

И это несмотря на то, что переход на новые принципы управления уже произошел. На смену, скажем так, «коммуникациям со смазкой», когда можно подойти и договориться, пришел чёткий протокол действий, который на уровне чиновника не поменять.

— Этот протокол может заменить человека?

— Я вам напомню, что некоторое время назад в Москве было около 300 таксопарков. А это 300 директоров, 300 главных бухгалтеров, 300 экономистов-плановиков, а еще девушки, которые принимали звонки на телефоне, диспетчеры. Сегодня вместо них в «Яндекс.Такси», например, несколько десятков программистов. Списан под ноль массовый средний класс — пара тысяч человек. Я называю общим словом «средний класс» всю прослойку бюрократии, менеджеров. Вот они больше не нужны!

Эта ситуация, конечно, сильно отличается от наших прошлых ожиданий, что «цифра» займет место уборщиц и санитарок, занятых тяжелой неквалифицированной работой. А по факту ненужными оказались менеджеры, бюрократы, так или иначе занятые перекладыванием бумаг.

О ДОВЕРЕННОЙ ЦИФРОВОЙ ЭКОНОМИКЕ

— Цифровая экономика по определению должна быть доверенной и защищённой. Но как сделать это наиболее эффективным способом? Можно ли здесь применить принцип Secure by design, подразумевающий проектирование информационной системы изначально на принципах защищённости?

— Вопрос большой. Давайте выделим самое главное. Оно заключается в том, что темпы развития «цифры» таковы, что мы попали в историю, где слабое звено — именно человек. Не техника. История с безопасностью на техническом уровне близка к идеальной. У нас прекрасные биометрические системы и отличный уровень распознавания лиц. Но найдётся человек, который нажмёт на кнопочку и пропустит человека в помещение, даже если все суперсистемы будут против. Найдется человек, который загрузит приложение из неизвестного источника, несмотря на то, что его десять раз предупредят: «Не делай этого!».

На примере нынешнего разгула мошенников мы видим, что никто не забирается в телефон человека. Он сам решает использовать самый популярный пароль (вы знаете, какой) и не менять его годами. Ввели дополнительную авторизацию по SMS, но человек называет код из этой SMS любому собеседнику, который представился курьером.

Это социальная инженерия, которая не имеет никакого отношения к «цифре». И финансирование Банком России мероприятий по продвижению среди населения финансовой грамотности кардинально изменить ситуацию не способно. Накапливать опыт, наблюдая, как мошенники «разводят» новых и новых бабушек, а также граждан среднего возраста и даже молодежь,— тоже нельзя считать выходом из ситуации.

— А где выход?

— Главное — понимание, что это именно задача государства. Почему? У врачей-психиатров есть статистика: в любом зале 50% присутствующих всегда подвержены гипнозу. Если им сказать со сцены: «Встать!», они встанут, не раздумывая. А среди этой половины зала есть 10%, которые точно поведутся на разговорный «цыганский» гипноз, вообще не видя собеседника. Для них все рациональные рассуждения о звонках с незнакомых номеров и прочем совершенно бесполезны.

Именно государство должно обеспечить безопасность для этих 10% граждан. А это означает абсолютный контроль с точки зрения доступа к массовым коммуникациям. Фактически это про устранение анонимности. Причем, для этого достаточно разрешить искусственному интеллекту слушать ваш разговор. Он это умеет, надо только ему разрешить. Тогда — я вас уверяю! — проблема с мошенниками вообще бы исчезла. И станет как в Китае — там это работает.

А у нас, если проанализировать статистику таких преступлений, получается на уровне тысяч в день! Представляете? Мы тысячу бабушек каждый день отдаём в жертву мошенникам! Дело в том, что государство физически не готово противостоять этой угрозе. Причем, технически-то оно готово, а вот физически... Я понимаю под этим «физическую силу» законотворчества депутатов. Они спокойно будут смотреть на происходящее до тех пор, пока сами либо их ближайшие родственники не станут жертвой мошенников.

— А чем заняты наши депутаты?

— Приведу яркий пример внедрения современной «цифры» — беспилотные автомобили. Какой вопрос вызывает тут споры? Как

разрешить дилемму: кого давить в критической ситуации на дороге — пожилого человека или молодого? Это подается как этический вопрос искусственного интеллекта. Я говорю этим людям: «В России ежегодно 15 тыс. человек гибнет под колесами автомобилей и еще 50 тыс. становятся инвалидами! Мы готовы прямо сегодня внедрить умные беспилотные решения, и погибать будет всего 500 человек». А мне на это: «Подождите, Герман Сергеевич, давайте сперва решим этический вопрос».

По моим оценкам, торможение внедрения нужной «цифры» обусловлено социальными моментами — чьими-то опасениями потери приватности и т.п. Возможно, должно смениться поколение людей, которые принимают решения о запретах/разрешениях. Все-таки современные молодые люди вырастают в другой зоне приватности, чем те, которым сейчас 40–50 лет. И когда нынешние двадцатилетние достигнут руководящих позиций, они не будут пугаться «цифры», и наступит цифровое счастье.

Но надо понимать, что уже сегодня каждый смартфон знает о человеке гораздо больше, чем любая спецслужба. И доступ к этим данным позволил бы быстро и решительно справиться со многими нынешними напастями. Меня лично эта доступность совсем не беспокоит, хотя я, наверное, отношусь к числу «профдеформированных».

Впрочем, все может быть гораздо быстрее. Я знаю бабушек, которые с удовольствием пользуются смартфонами и распознаванием лица вместо ключа при входе в подъезд. Внедрение «цифры» имеет нелинейный характер, и эффект нарастает очень быстро.

ПРО УМНЫЕ СЕРВИСЫ И ЗАПРЕТЫ

— У инфраструктуры цифровой экономики две главных составляющих: технические ИТ-системы и современные системы поддержки принятия решений на всех уровнях управления, включая пресловутый искусственный интеллект (ИИ). Что сегодня требует больше внимания?

— Давайте поговорим про умное ПО. Я начал изучать ИИ в 80-х годах прошлого века, еще в вузе. Тогда возможности аппаратной базы компьютеров не позволяли надеяться, что это устройство сможет выиграть шахматную партию у серьезного игрока. Что касается ПО, еще моя мама во времена ее молодости участвовала в исследованиях по оцифровке данных Госплана и модернизации принятия решений на этой базе. Тогда все упиралось тоже в ограничения аппаратной части. Сегодня этих ограничений нет. Но тут появляются запреты...

Приведу пример (гипотетический) из близкой мне сферы — медицинской информатизации. Представьте: бабушка живет на Камчатке в удаленном районе, у нее гипертония. Вопрос: с кем ей лучше поговорить о своем самочувствии? С местным врачом или ChatGPT? Мой ответ: сейчас — с ChatGPT. Предвижу: «Как так! Там же может быть ошибочная информация! И вообще галлюцинации! И буржуинский сервис персональные данные бабушки в своем облаке запоминает!» А я отвечу: можно представить ситуацию, когда ChatGPT в этом разговоре ошибётся, но это будет на тысячу бабушек — один раз. Но 999 бабушкам он поможет! И тут вновь возникает интересный выбор, похожий на «дилемму беспилотника»: беспокоиться нужно об этой одной бабушке, забыв о тех 999-ти, которым сервис помог? Либо оставить всю эту тысячу бабушек вообще без помощи, приговаривая: «Нет, пока мы не приведём все в порядок, пусть эти бабушки умирают православненько». Ну, в смысле — с соблюдением всех инструкций Минздрава...

— Но, по сути, Минздрав ставит вопрос ответственности за врачебную ошибку, который формально не решен в отношении ИИ?

— Я вам больше скажу: ChatGPT поможет повысить эффективность медицинской консультации (назовем это так), потому что пациент не будет врать доктору.

— Как так?!

— Это известный медицинский факт: больной приходит к врачу и стыдится честно рассказать доктору, что именно привело к серьезному ухудшению здоровья. Диабетик, у которого резко «стрельнул» уровень сахара в крови, расскажет про нервное состояние, ссору с коллегой, но не про то, что он про-

За ChatGPT стоят тысячи эндокринологов, которые подсказывают: «Спроси про сахар! И про вес!». А придя на прием к «живому» доктору, бабушка может попасть — давайте будем честными! — не к самому лучшему врачу в своей сфере

снулся ночью и сожрал в одно лицо целый торт с кремом. А «железке» человек врать не будет. Плюс к этому за ChatGPT стоят тысячи эндокринологов, которые подсказывают: «Спроси про сахар! И про вес!». А придя на прием к «живому» доктору, бабушка может попасть — давайте будем честными! — не к самому лучшему врачу в своей сфере. Вот почему порой происходят удивительные вещи — советы «железяки» оказываются лучше, чем доктора из местной поликлиники.

— Так что, «цифра» еще и конец профессии врача пророчит?

— Вовсе нет! Уйдут врачи, которые не соответствуют этому высокому званию. А их у нас, к сожалению, немало. Просто мы боимся это признать, и в этих страхах сегодня живём. А могли бы спасать здоровье людей в гораздо больших масштабах.

— Стоит вспомнить, что генеративный ИИ сегодня порой выступает как участник информационных войн. И это одна из причин призывов к запрету зарубежных ресурсов.

— Возьмем более понятный пример — Википедию, к которой тоже есть нарекания в этой части. Она четко делится на две части: факты и история с литературой. Что касается второй части, то там да, у разных стран есть свои особенности в трактовке исторических событий. Вопрос: как их совместить? Ответ: никак.

Но вот что важно: 90% контента Википедии и 90% использования ИИ находятся в пространстве, где нет теоретических споров. В распознавании снимков КТ/МРТ нет никакой политики и идеологии. Так почему же государство запрещает использовать там зарубежный ИИ? Оно, наверное, перепутало медицину с идеологией? Я вас уверяю, что на практике в ситуациях, когда требуется внедрить отечественный ИИ, он приобретается, однако, снизу подкладывается китайский, бесплатный, который присутствует там невидимо. Вот так это сейчас работает.

Нужно детализировать требования к ИИ. Те системы, где используются знания, скажем так, регионо-ориентированные, нам не надо применять. Не надо учиться по американским учебникам истории. А по американским учебникам химии или физики? Почему нет, если они хорошие?

— Понятно, что нужно отделить точные науки от гуманитарных знаний. Но как это сделать практически на уровне закона?

— Я не знаю. И наши депутаты тоже не знают... В прошлые годы, когда я по долгу службы общался с министерством образования, были предложения модернизировать школьные учебники. В том числе, с помощью «циф-

Выкинуть всё зарубежное и оставить только наше — это поверхностное решение. Уже тогда было понятно: где вы возьмёте людей, чтобы заменить весь этот объём технологий?

ры», например, сделать их интерактивными, адаптивными к особенностям восприятия конкретного ребенка. Ничего не вышло даже на уровень эксперимента. Ответ профессионального сообщества был такой: даже если начать с учебника математики, мы всё равно придём к учебнику истории. И прежде, чем выпускать джинна из бутылки, нужно 10 раз подумать, насколько этот джинн хорош. И все упирается в вопрос: кто ответит, если через 10 лет дети не станут патриотами? Или что будет с русским народом через 10 лет, если говорить про здравоохранение?

— С одной стороны, это принцип минимизации ущерба — «не навреди»...

— А с другой стороны, вспоминается: «Направо пойдёшь — коня потеряешь, себя спасёшь; налево пойдёшь — себя потеряешь, коня спасёшь; прямо пойдёшь — и себя и коня потеряешь». Самое плохое — это стоять на месте. А лица, принимающие решения, стоят на месте. И на это, к сожалению, не обращается должного внимания...

ПРО ЦИФРОВОЙ КОДЕКС

— И еще добавляется подмена терминов: понятие «ИИ» сузили до пресловутого GenAI, который, по сути, представляет собой развитие технологии интеллектуального архива, в первую очередь, текстовых документов.

— Смотрите. Мы все живём в религиозной парадигме, даже атеисты. То есть «В начале было Слово». Когда-то гремел термин «инновации», а до этого «криптовалюты». Было время, когда в начале всего было слово «цифровизация». Ну, а сегодня — «искусственный интеллект». Хотя, если посмотреть, ни в продвинутых МФЦ, ни на Госуслугах, ни в передовых банках настоящего искусственного интеллекта не много. А хайп — он всегда произрастает на стыке психотерапии и журфака (в смысле медийной активности).

Любой промышленной революции, мне кажется, свойственно постоянное изменение терминов. И наша настоящая беда сегодня — это отсутствие Цифрового кодекса. То есть единого понятийного аппарата. Как в таком состоянии принимать решения? Осуществлять судопроизводство? Мы ситуативно принимаем какие-то нормотворческие, извините, «нашлёпки». А надо начинать с самых простых вещей — четких определений, что такое поисковая система, что такое куки (те, которые cookie) и т.д.

Обратите внимание: Европа в течение пяти лет работала над Digital Act. В это время они ни за кем не гонялись, никого не блокировали. Они создали понятийный аппарат, потом приняли все законы, и только после этого взялись за Павла Дурова. А у нас наоборот: понятийного аппарата нет, но принимается огромная масса ситуативных законов. Потому что некогда. В результате — разносортица. Только по мошенникам в конце декабря приняли около 30 поправок, недавно еще несколько десятков. И где эта единая база номеров IMEI мобильных телефонов? Где охлаждение SIM-карт?

Мы живем в удивительную пору, когда у кого-то есть Digital Act — вариант очень жёсткого регулирования Интернета, но нет своих ресурсов. А у нас нет Цифрового Кодекса, но зато есть «Яндекс»», «ВКонтакте» и много других ресурсов, которые позволяют нам активно развиваться в «цифре». И только вскрытие покажет, кто оказался прав...

И ВНОВЬ ПРО ИМПОРТОЗАМЕЩЕНИЕ

— Запреты зарубежных сервисов помогают переключать спрос на отечественные услуги. Это же логично?

— Как патриот, я абсолютно согласен: «Надо нашим помогать развиваться». Но как реалист, я понимаю, что это физически невозможно при нашем размере населения. Ассортимент ПО, которое разрабатывается в разных странах, настолько широк, что своими силами не справиться. Помните: «Через год выпустим свои процессоры, появится наш AutoCAD, появится наш Photoshop и всё-всё-всё»? Уже тогда было понятно: «Коллеги, где вы людей на все это возьмёте?». Выкинуть всё зарубежное и оставить только наше — это поверхностное решение.

Мы должны выучить уроки и 2014 года, и 2022-го. Но надо быть здравомыслящими людьми и не впадать в очередную зависимость. Надо везде, где можно и как можно, брать лучшее и внедрять у себя лучшее. С учетом, разумеется, «странностей» ИИ и вопросов безопасности. А самим делать то, что отлично умеем — образно говоря, «атомные станции и балет» в «цифре».

— Какой наибольший риск вы видите при таком подходе к созданию цифровой экономики?

— Пожалуй, единственный риск или, скорее, проблема — это то, что из-за санкций мы отсечены от мирового рынка программных решений и, что еще более неприятно, от рынка «железа». Даже если мы производим собственную сборку вычислительной техники, всё равно используем зарубежные детали. То есть «кирпичи» для строительства наших прекрасных цифровых «зданий» мы всё-таки завозим из-за рубежа. Это факт, который надо принять как данность. Другой вопрос, что из-за усиления санкций это значительно затруднилось, что замедляет наше движение.

Китайцы — наши друзья — не очень горят желанием обеспечивать нам серьезные поставки. В отличие от западных «партнеров», которые прямо говорят «нет», эти обещают, но результат похож... Сопредельные страны — Киргизия, Армения, Казахстан — снижают свою активность в роли «хабов» поставок «железа».

Рассчитывать всерьез на отечественную радиоэлектронику? Чиновники ее видят и даже собираются ввести аналог утильсбора на смартфоны, чтобы собрать триллион рублей и передать их производителям «Байкалов» и «Эльбрусов», и таким образом восстанавливать российскую радиоэлектронику. Но я в это не верю, честно говоря.

— Почему?

— Точнее, я не верю в быстрое решение этой масштабной задачи. Я верю в долгую, нудную, методичную историю. Китай показал, что за 20 лет это все можно создать практически с нуля. Беда в том, что у нас никто не мыслит категориями в 20 лет. Надо срочно «освоить» средства и отчитаться российскими «шильдиками» на оборудовании! А надо начинать с самого основания — с простейших тройников — кабельных коннекторов, научиться их производить и двигаться дальше, усложняя продукцию. Это займёт, конечно, не 20 лет, но лет 10 потребуется. Но нужен ли будет нам через 10 лет процессор, который технически отстает на 10 лет от нынешнего мирового уровня? И это без учета сегодняшнего фактического отставания?

Кстати, отъезд за рубеж многих специалистов создает гораздо меньшие риски. Наши люди ведь натренированы в этом плане — уезжали и в 90-е, и в «нулевые». И очередное «кровопускание» только освежило кадры, включая полезную ротацию руководящих кадров.

Так что главный риск — это «железо», ресурсные мощности, облака.

ЧТО ДЕЛАТЬ?

— Что нужно сделать, чтобы улучшить состояние ресурсной базы цифровой экономики?

— Несмотря на усилия государства в этой части, нужно еще и дотирование этой сферы. Потому что коммерческие ценники, скажем, наших цифровых лидеров «Яндекса» и Сбера — это безнравственно. Причём, именно для серьезного бизнеса это выливается в критические суммы, и он пытается тихо найти другие варианты. И это, конечно, риски, которые надо решительно пресекать.

— Как может выглядеть эффективное частно-государственное партнерство?

— Давайте смоделируем разговор государства с коммерческими поставщиками:

— *Хочу покупать только отечественное ПО.*

— *Хорошо. Покажите требования, и мы вам скажем, когда это выдадим.*

— *Хочу завтра.*

— *Завтра не получается.*

— *Нет, завтра! Вот вам реестр.*

Что остается бизнесу? Выполнять поставленные условия. То есть найти способ «перелицевать» какое-либо доступное ПО и внести его в реестр.

— А как должно быть?

— Государству нужно очень чётко формулировать стратегию развития. Например, есть 5 млн рабочих мест, которые необходимо обеспечить ПО. Затем объявляются тендеры, скажем, два тендера на две операционные системы и к ним господдержка — 200 руб. в месяц за каждую лицензию. Вот за это, собственно, и пойдет настоящая борьба реальных отечественных, а не «перелицованных» программных продуктов.

Разговоры на эту тему идут давно. И я проводил такие совещания в Администрации Президента РФ, и Вячеслав Володин в бытность его первым заместителем Председателя Правительства. Но, возможно, дело сдвинется с места, когда цифра, наконец, заменит всех чиновников?.. А если всерьез, в целом мне нравится, как государство сейчас выстраивает ГЧП *(государственно-частное партнерство — ред.)* в сфере «цифры». Главное — оно учится это делать лучше: размещать заказы на рынке коммерческих разработчиков и получать хороший результат.

Беседовала
Елена Покатаева,
обозреватель
BIS Journal

ВСЁ НА ВИДУ

ПУБЛИЧНЫЕ ИИ-СЕРВИСЫ И УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ИЗ КОРПОРАТИВНЫХ СРЕД

Илья ТКАЧЕНКО
независимый эксперт

Настоящая статья посвящена складывающейся ситуации с растущей угрозой утечек конфиденциальной корпоративной информации, вызванной неконтролируемым использованием сотрудниками публичных сервисов искусственного интеллекта (ИИ-сервисов). Практика «быстро обратиться к генеративному ИИ» превращается в устойчивый канал вывода данных из корпоративной среды: в запросы уходят фрагменты кода, внутренние регламенты, коммерческие документы, персональные данные клиентов и техническая документация. По материалам открытых публикаций за 2023–2026 годы в настоящей статье собраны и структурированы ключевые риски, подтверждённые инциденты, доступные ресурсы для мониторинга проблемы, а также сформулированы практические рекомендации по снижению вероятности утечки данных и обеспечению контроля применения ИИ в корпоративных процессах.

1. ВВЕДЕНИЕ: МАСШТАБ И АКТУАЛЬНОСТЬ ПРОБЛЕМЫ

Массовое внедрение генеративного ИИ в бизнес-процессы создало парадоксальную ситуацию: технологии, призванные повысить эффективность, стали одним из главных каналов утечки информации. К 2025 году 83% корпоративных команд использовали генеративный ИИ, однако лишь 31% организаций имели формализованные политики обращения с данными при работе с этими инструментами [1]. Это привело к феномену «теневого ИИ» — использованию сотрудниками публичных ИИ-сервисов (ChatGPT, Claude, Gemini и др.) без одобрения и контроля со стороны ИТ-безопасности. Российская статистика демонстрирует катастрофическую динамику: в 2025 году объём данных, отправляемых сотрудниками российских компаний в публичные ИИ-сервисы, вырос в 30 раз [2]. Проблема вышла за рамки технической уязвимости, превратившись в комплексный организационно-управленческий вызов, требующий незамедлительного стратегического ответа.

2. КЛАССИФИКАЦИЯ КЛЮЧЕВЫХ РИСКОВ

Риски утечек информации через публичные ИИ-сервисы носят многоуровневый характер и могут быть структурированы по трём основным категориям.

2.1. Технические риски

◆ Уязвимости конфигурации и архитектуры: неправильная настройка ИИ-систем, включая облачные базы данных и API-шлюзы, является частой причиной масштабных утечек. Яркий пример — инцидент с платформой Moltbook в феврале 2026 года, где из-за ошибки конфигурации стали публично доступны 1,5 миллиона API-ключей, используемых для управления ИИ-агентами [3].

◆ Атаки на модель (Prompt Injection, Model Inversion): злоумышленники используют специально сконструированные промпты для обхода ограничений модели, извлечения конфиденциальных данных, на которых она обучалась, или манипуляции её выводом. Исследование компании Anthropic выявило случаи, когда злоумышленники использовали Claude Code для автоматизации рекогносцировки и проникновения в корпоративные сети [4].

◆ Компрометация цепочки поставок: уязвимости в сторонних библиотеках, фреймворках или моделях, интегрированных в корпоративные ИИ-решения, могут стать вектором для атаки на всю инфраструктуру. На этот тип атак приходилось около 30% инцидентов, связанных с ИИ [5].

◆ Недостаточная обработка вывода (Data Leakage через ответы): модель может непреднамеренно включить конфиденциальную информацию из своего обучающего набора данных или контекста предыдущих взаимодействий в генерируемый ответ.

2.2. Организационные и кадровые риски

◆ «Теневой ИИ» и отсутствие политик: сотрудники, стремясь решить рабочие задачи быстрее, загружают в публичные чат-боты код, финансовые отчёты, персональные данные клиентов, стратегические документы. Классический случай произошёл в Samsung в 2023 году, когда инженеры загрузили фрагменты секретного исходного кода в ChatGPT для проверки и оптимизации [6]. Аналогично в 2025 году исполняющий обязанности директора Агентства кибербезопасности и инфраструктурной безопасности США (CISA) загрузил в ChatGPT служебные документы с грифом «For Official Use Only» [7].

◆ Недостаточная осведомлённость и обучение: сотрудники часто не осознают, что вводимые в публичный ИИ-сервис данные могут сохраняться, использоваться для дообучения модели и становиться потенциаль-

но доступными другим пользователям или злоумышленникам.

◆ Отсутствие контроля доступа и мониторинга: во многих организациях нет технических средств для обнаружения и блокировки передачи конфиденциальной информации в публичные ИИ-сервисы.

2.3. Правовые и регуляторные риски

◆ Несоответствие требованиям защиты данных: передача персональных данных сотрудников и клиентов в сервисы, чьи серверы находятся за пределами Российской Федерации, создаёт прямые риски нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Особое внимание следует уделить порядку трансграничной передачи, установленному Роскомнадзором, несоблюдение которого может повлечь значительные штрафы и предписания для оператора.

◆ Нарушение коммерческой тайны и интеллектуальной собственности: утечка через публичный ИИ-сервис конфиденциальной информации, ноу-хау и стратегических планов подрывает конкурентные преимущества компании и может квалифицироваться как разглашение коммерческой тайны со всеми вытекающими правовыми последствиями.

◆ Неопределённость и динамичность регуляторного поля: законодательное регулирование использования ИИ, особенно в части ответственности за утечки, продолжает развиваться. В этой связи организациям рекомендуется ориентироваться не только на текущие законы, но и на перспективные стандарты, такие как ГОСТ Р ИСО/МЭК 42001–2024[1], задающие рамки ответственного управления ИИ.

Важно отметить, что регуляторное поле в РФ начинает обретать более прикладные контуры именно в части ИИ-рисков. Позитивный сигнал — работа ФСТЭК России: в Банке данных угроз безопасности информации (БДУ) выделен отдельный раздел, посвящённый угрозам безопасности информации систем искусственного интеллекта. Это означает, что ИИ-сценарии начали формально учитываться при моделировании угроз и обосновании мер защиты.

Параллельно появляется и нормативная рамка: приказ ФСТЭК России № 117 от 11.04.2025[2] актуализирует требования по защите информации для государственных и связанных систем и вступает в силу с 1 марта 2026 года.

При этом это только начало пути. БДУ и нормативные требования задают направление, но не заменяют практику: классификацию данных для ИИ-сценариев, контроль внешних интеграций и регулярную переоценку рисков по мере развития публичных ИИ-сервисов и агентных режимов.

3. РЕАЛЬНЫЕ ИНЦИДЕНТЫ И КЕЙСЫ

В таблице приведена подборка подтверждённых инцидентов из открытых источников, связанных с утечками информации.

[1] Национальный стандарт Российской Федерации «Искусственный интеллект. Система менеджмента». Утверждён и введён в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 октября 2024 г. № 1549-ст.

[2] Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (Зарегистрировано в Минюсте России 16.06.2025 № 82619).

Организация / контекст	Год	ИИ-сервис / причина	Характер и объём утечки	Источник
Moltbook	2026	Платформа ИИ-агентов	1,5 млн API-ключей для управления ИИ-агентами из-за неправильно сконфигурированной базы данных	aimojo.io
Samsung Electronics	2023	ChatGPT	Сотрудники загрузили конфиденциальный исходный код полупроводникового и программного обеспечения	forbes.com
Агентство кибербезопасности и инфраструктурной безопасности США (CISA)	2025	ChatGPT	Сотрудник загрузил служебные документы с пометкой «For Official Use Only» (FOUO)	rbc.ru
OpenAI / ChatGPT (массовый инцидент)	2025	ChatGPT (функция публичных ссылок)	Миллионы личных чатов, содержащих API-ключи, пароли, детали личной жизни, конфиденциальные обсуждения, стали доступны через поиск Google	cnews.ru
Различные организации (здравоохранение, госсектор)	2025	Claude (Anthropic)	Киберпреступник использовал Claude Code для автоматизации масштабной операции по вымогательству: взлом 17 организаций, анализ данных для определения размера выкупа, генерация ransom-нот	anthropic.com
Google Gemini	2025	Gemini AI	Обнаружены три уязвимости (Gemini Trifecta), позволяющие через внедрение вредоносных команд и манипуляцию историей поиска извлекать персональные данные пользователей, включая геолокацию	anti-malware.ru

4. СТАТИСТИКА И АНАЛИТИЧЕСКИЕ ДАННЫЕ

Актуальные отчёты ведущих компаний в сфере кибербезопасности подтверждают системный характер проблемы [8]:

- в 2025 году в мире произошло 12 195 подтверждённых случаев утечки информации;
- сейчас кибератаки происходят примерно каждые 39 секунд по всему миру;
- в 2025 году была обнаружена огромная коллекция 16 миллиардов утёкших учётных данных;
- здравоохранение остаётся отраслью с наибольшим количеством взломов по всему миру;
- средняя стоимость утечки медицинских данных достигла 7,42 миллиона долларов;
- на системное вторжение пришлось 53% всех случаев утечки информации;
- в результате пяти крупнейших утечек данных в США было раскрыто более 131 миллиона записей;
- нарушения в цепочках поставок в среднем приводили к утечке почти миллиона записей за один инцидент;
- на долю США пришлось 56% всех случаев утечки информации в мире;
- средняя стоимость утечки информации в мире составила 4,4 миллиона долларов.

4.1. Обнаружение и реагирование: на обнаружение утечки в среднем уходит 181 день, на её локализацию — ещё 60 дней [5]. При этом инциденты, связанные с «теневым ИИ», обнаруживаются быстрее (в среднем за 62 дня), но их устранение остаётся сложным (185 дней) [5].

4.2. Динамика инцидентов: база данных AI Incident Database зафиксировала более 300 зарегистрированных инцидентов с ИИ в 2025 году, причём наиболее частыми были случаи с deepfake и мошенничеством [9]. Графики Our World in Data показывают устойчивый рост числа регистрируемых инцидентов с ИИ с 2012 года [10].

5. РЕСУРСЫ ДЛЯ МОНИТОРИНГА И АНАЛИЗА ИНЦИДЕНТОВ

Для отслеживания трендов и изучения конкретных случаев целесообразно использовать специализированные ресурсы.

- AI Incident Database (incidentdatabase.ai) — крупнейшая международная открытая база данных, посвящённая сбору и документированию инцидентов, когда системы ИИ причинили вред или создали его риск [11].
- Our World in Data — предоставляет наглядную статистику и графики по количеству зарегистрированных инцидентов и споров, связанных с ИИ, в долгосрочной перспективе [10].
- IBM Cost of a Data Breach Report — ежегодное авторитетное исследование стоимости, причин и трендов утечек информации [12][13].
- Verizon Data Breach Investigations Report (DBIR) — ежегодный всеобъемлющий анализ реальных инцидентов информационной безопасности, включая связанные с ИИ [14].

При этом важно понимать, что основная масса таких источников формируется за рубежом — это полезно для сопоставления с глобальной картиной, но добавляет фактор зависимости по доступности и полноте. Поэтому, наряду с обращением к международным базам и отчётам, имеет смысл поддерживать развитие общедоступных российских и/или локализованных ресурсов для сбора и анализа ИИ-инцидентов (включая утечки через публичные ИИ-

сервисы) — с понятной методологией, единым словарём терминов и возможностью воспроизводимого сравнения кейсов. Такая инфраструктура снижает риски «внешней опоры» и помогает быстрее переводить наблюдения из инцидентов в практические меры защиты.

6. РЕКОМЕНДАЦИИ ПО ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ

На основе анализа рисков и инцидентов можно сформулировать комплекс мер для организаций.

6.1. Разработка и внедрение политики использования ИИ: чёткий регламент, определяющий, какие публичные ИИ-сервисы разрешены, для каких задач, какие категории данных категорически запрещено в них загружать. Политика должна быть доведена до всех сотрудников.

6.2. Технические меры контроля:

- внедрение DLP-систем (Data Loss Prevention), настроенных на обнаружение попыток передачи конфиденциальной информации в публичные ИИ-сервисы;
- использование корпоративных прокси и шлюзовых решений для контроля интернет-трафика;
- рассмотрение возможности развёртывания закрытых корпоративных ИИ-решений или использования защищённых API коммерческих моделей ИИ с гарантиями конфиденциальности информации.

6.3. Повышение осведомлённости и обучение: регулярные тренинги, на которых сотрудникам на реальных примерах (вроде инцидентов в Samsung или CISA) разъясняются риски «теневого ИИ» и правила безопасной работы.

6.4. Аудит и мониторинг: регулярная проверка логов на предмет использования публичных ИИ-сервисов. Внедрение решений класса CASB (Cloud Access Security Broker) для контроля за облачными приложениями.

6.5. Создание инцидент-ответа для ИИ-угроз: в план реагирования на инциденты информационной безопасности должны быть включены специфические сценарии, связанные с утечкой информации через публичные ИИ-сервисы.

В качестве методологического фундамента для всех перечисленных мер рекомендуется рассмотреть внедрение принципов, изложенных в национальном стандарте ГОСТ Р ИСО/МЭК 42001–2024 «Информационные технологии. Искусственный интеллект. Системы менеджмента искусственного интеллекта». Данный стандарт предоставляет организациям структурированную модель для:

- разработки и формализации политик в области ИИ, согласованных с общей бизнес-стратегией и требованиями регуляторов;- проведения регулярной оценки рисков, связанных с ИИ, включая риски конфиденциальности и безопасности информации;
- создания прозрачных процедур управления данными на протяжении всего жизненного цикла ИИ-системы;
- обеспечения необходимого уровня осведомлённости и компетентности персонала, работающего с ИИ.

Использование данного стандарта позволит перейти от разрозненных мер к целостной системе управления, минимизирующей вероятность инцидентов и демонстрирующей должную осмотрительность перед регуляторами и партнёрами.

7. ПРОГНОЗЫ И ЗАКЛЮЧЕНИЕ

Эксперты единодушны в том, что проблема будет обостряться. Специалисты Swordfish Security предупреждают, что в 2026 году следует ожидать громких инцидентов с участием ИИ-агентов, которым будет предоставлен доступ к конфиденциальной информации и корпоративным API [15]. «Лаборатория Касперского» прогнозирует, что главным кибервызовом 2026 года станет массовая автоматизация атак с использованием ИИ как целостной экосистемы [16].

Утечки информации из-за использования публичных ИИ-сервисов перестали быть гипотетическим риском и превратились в повседневную угрозу для организаций по всему миру. Борьба с ней требует не разовых мер, а комплексного подхода, объединяющего технологические решения, пересмотр внутренних процессов, постоянное обучение персонала и адаптацию правовой базы. Организации, которые уже сегодня начнут выстраивать систему управления рисками, связанными с использованием ИИ, смогут не только избежать финансовых и репутационных потерь, но и получить конкурентное преимущество в эпоху тотальной цифровизации.

ССЫЛКИ

[1] https://www.isaca.org/about-us/newsroom/press-releases/2025/ai-use-is-outpacing-policy-and-governance-isaca-finds

[2] https://www.anti-malware.ru/news/2026-02-03-121598/48907

[3] https://aimojo.io/moltbook-data-leak/

[4] https://www.anthropic.com/news/detecting-countering-misuse-aug-2025

[5] https://www.brightdefense.com/resources/data-breach-statistics/

[6] https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/

[7] https://www.rbc.ru/politics/28/01/2026/697a29eb9a7947a1bfffd8d8

[8] https://www.demandsage.com/data-breach-statistics/

[9] https://techround.co.uk/news/ai-incidents-2025-ai-incident-database/

[10] https://ourworldindata.org/grapher/annual-reported-ai-incidents-controversies

[11] https://incidentdatabase.ai/

[12] https://www.bakerdonelson.com/webfiles/Publications/20250822_Cost-of-a-Data-Breach-Report-2025.pdf

[13] https://www.ibm.com/reports/data-breach

[14] https://keepnetlabs.com/blog/2025-verizon-data-breach-investigations-report

[15] https://safe.cnews.ru/articles/2025-12-19_eksperty_swordfish_security_v_2026_godu_my_uvidim

[16] https://www.vedomosti.ru/technologies/special/2025/12/24/top-kibervizovov-20252026-glavnie-trendi-v-ib-ot-laboratorii-kasperskogo-erid-2Vfnxxvgiq1

ДЛЯ ЧЕГО НУЖНЫ И КАК РАБОТАЮТ ID-ПРОВАЙДЕРЫ

Иван ПИСАРЕНКО
заместитель руководителя службы УОИБ ДБ Банка ВТБ (ПАО), к. т. н., доцент

Сергей ПОПОВ
руководитель службы УОИБ ДБ Банка ВТБ (ПАО), к. т. н., CISSP

Сегодня среднестатистический пользователь может иметь по разным оценкам от нескольких десятков до нескольких сотен аккаунтов в различных приложениях и интернет-сервисах, начиная от социальных сетей и мессенджеров, заканчивая банковскими приложениями и государственными порталами. Для доступа к каждому из этих аккаунтов требуются логин и уникальный пароль. Создание, запоминание, хранение и использование такого количества учётных данных могут вызывать определённые сложности. Одним из способов облегчить жизнь рядового пользователя является использование так называемых ID-провайдеров.

ЧТО ТАКОЕ ID-ПРОВАЙДЕР

ID-провайдер (IdP, поставщик идентификационных данных) — это система, которая создаёт, хранит цифровые идентификаторы и управляет ими, а также выполняет для них аутентификацию.

ID-провайдер может обрабатывать данные таких субъектов (их ещё называют принципалами[1]), как пользователи, устройства или сервисы. Он хранит идентификаторы (например, электронную почту или имя пользователя), учётные данные и данные профиля, а также предоставляет услуги аутентификации, которые приложения или сервисы могут вызывать вместо непосредственной аутентификации на своей стороне. После успешного входа ID-провайдер возвращает доверенный результат (например, подписанный токен или утверждение), который приложение или сервис используют для создания сессии и обеспечения авторизации.

Другими словами, ID-провайдер осуществляет аутентификацию и авторизацию пользователей (говорить в статье будем в основном про них) в различных приложениях, системах или на сайтах без повторной регистрации, обеспечивая тем самым безопасность данных и упрощая доступ к разным сервисам. Пользователю необходимо всего один раз зарегистрироваться у ID-провайдера, а затем уже использовать эти данные для входа на другие сайты.

ДЛЯ ЧЕГО НУЖНЫ ID-ПРОВАЙДЕРЫ

Основными функциями ID-провайдеров являются:

- аутентификация — базовая и самая главная функция. ID-провайдер проверяет, действительно ли пользователь является тем, за кого себя выдаёт;
- авторизация. ID-провайдер определяет, к каким ресурсам, данным или системам имеет доступ проверенный пользователь;
- предоставление информации о пользователе сторонним приложениям — его роли, уровне доступа и т.д.;
- обеспечение единого входа (SSO) для доступа к другим сервисам. ID-провайдер позволяет использовать один аккаунт для аутентификации на множестве не связанных друг с другом ресурсов.

Использование ID-провайдеров повышает удобство пользователей при получении доступа к нужному сервису: не нужно запоминать, записывать или хранить связку логин — пароль для каждого ресурса, экономится время на введении аутентификационных данных, не нужно повторно вводить имя, домашний адрес, номер телефона — можно сразу пользоваться ресурсом.

Компании, которые подключают ID-провайдеров, также получают важное преимущество: клиентам не требуется каждый раз вводить логин и пароль. В результате продажи внутри всей экосистемы приложений растут. К тому же через ID-провайдера компания получает данные для аналитики. Они помогают улучшать сервис, делать процессы эффективнее и запускать персонализированную рекламу.

Как показывают исследования, почти половина россиян использует аутентификацию и авторизацию через ID-провайдеров для получения различных услуг. В среднем один человек имеет три-четыре идентификатора различных ID-провайдеров: например, портал Госуслуг, банки, VK. При этом некоторые компании до сих пор используют только пары «логин/пароль» и рискуют потерять клиентов. Так, часть пользователей уходят с сайтов при предъявлении сложных требований к паролю.

КАКИЕ БЫВАЮТ ID-ПРОВАЙДЕРЫ

По состоянию на конец 2025 года больше половины (53%) 100 самых популярных российских интернет-ресурсов используют внешние ID-провайдеры.

При этом необходимо отметить, что с 1 декабря 2023 года в соответствии

[1] Принципал — субъект (пользователь, устройство, сервис), чью подлинность необходимо подтвердить.

с поправками к закону № 149-ФЗ «Об информации, информационных технологиях и защите информации» запрещено использовать иностранные ID-провайдеры (Google, Apple и др.) для авторизации на российских ресурсах. К допустимым же методам авторизации закон относит:

- российский номер телефона (РФ);
- «Госуслуги» (ЕСИА);
- Единая биометрическая система (ЕБС);
- иная информсистема, контролируемая российским лицом.

Наиболее популярный ID-провайдер в России — это VK ID (62%). На втором месте по популярности — «Яндекс ID» (40%), а третье место разделили «Сбер ID», «Госуслуги» (ЕСИА, Единая система идентификации и аутентификации) и «Одноклассники» (ОК ID) — по 34%. Появляются и корпоративные системы федеративной аутентификации — CDEK ID, Ozon ID, MTS ID, которые объединяют проекты, принадлежащие одной холдинговой структуре, но их распространение не очень широкое — как правило, не больше десятка сайтов.

Таким образом, основные популярные ID-провайдеры в России:

- VK ID;
- «Яндекс ID»;
- «Сбер ID»/«Госуслуги» (ЕСИА)/ОК ID.

Из приведённого перечня ID-провайдеров особого внимания заслуживает ЕСИА.

ЕСИА, по сути, является «цифровым пропуском», который открывает гражданам доступ более чем к 2 тысячам различных государственных и коммерческих порталов. При этом ежедневно через ЕСИА проходят 14 млн пользователей, попадая на порталы госуслуг, сайты Росреестра и другие ведомственные ресурсы. Всего на конец 2025 года в ЕСИА были зарегистрированы 120 млн человек.

Ещё одним интересным с точки зрения концепции, но не слишком распространённым ID-провайдером является так называемый Мобильный ID (Mobile ID).

Мобильный ID — это сервис авторизации, который развивают мобильные операторы МТС, «Мегафон», «Билайн», t2. В его основе лежит непосредственно номер мобильного телефона.

Технология позволяет безопасно подтверждать личность пользователя без ввода логинов, паролей или кодов из СМС.

С помощью Мобильного ID приложение подтверждает данные клиента через мобильного оператора (у которого информация об этом клиенте почти наверняка есть). Для пользователя это один из самых простых и интуитивно понятных способов: чтобы авторизоваться, необходимо просто нажать «ОК» на push-уведомлении. При этом уведомления инициируются оператором связи через SIM-карту, а не установленным на устройстве приложением. Это позволяет доставлять уведомления даже при заблокированном экране.

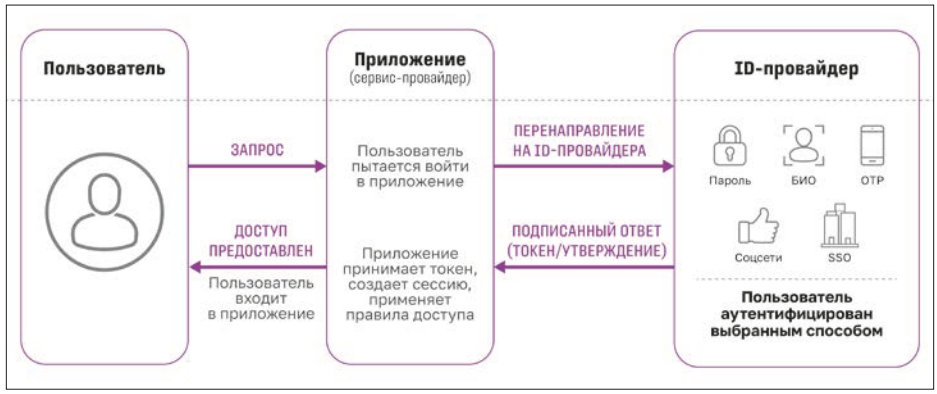


Рисунок 1. Типичная схема аутентификации и авторизации с помощью ID-провайдера

КАК РАБОТАЮТ ID-ПРОВАЙДЕРЫ

Общий порядок аутентификации и авторизации с использованием ID-провайдера обычно выглядит следующим образом: приложение, к которому хочет получить доступ пользователь, передаёт этап аутентификации на аутсорсинг ID-провайдеру и затем доверяет его решению.

Типичная схема аутентификации и авторизации с помощью ID-провайдера представлена на рисунке 1.

Запрос. Пользователь пытается получить доступ к приложению (сервис-провайдеру). Приложение видит, что пользователь не аутентифицирован, и перенаправляет его к ID-провайдеру.

Проверка. ID-провайдер запускает свой процесс аутентификации — для этого может применяться пароль, биометрия, одноразовый пароль (OTP), вход через социальные сети или корпоративное подключение SSO. При этом если пользователь ранее уже был аутентифицирован этим ID-провайдером, то он сразу получает доступ к приложению.

Доступ. Если аутентификация прошла успешно, ID-провайдер отправляет подписанный ответ (это может быть токен или так называемое утверждение) обратно приложению, которое затем проверяет его, создаёт сессию и применяет правила авторизации.

К основным протоколам и технологиям, с помощью которых чаще всего реализуется приведённая выше схема, относятся:

- OAuth2.0 (Open Authorization 2.0);
- OIDC (OpenID Connect);
- SAML (Security Assertion Markup Language);
- Mobile Connect.

От применяемого протокола зависит, как в ID-провайдере осуществляется аутентификация, авторизация (как формируются токены или утверждения), как устанавливается доверие между ID-провайдером и приложением и т.п.

OAUTH 2.0

OAuth (Open Authorization) — это открытый протокол авторизации, позволяющий предоставить стороннему приложению ограниченный доступ к данным пользователя без передачи логина и пароля. Чаще всего используется современная версия OAuth 2.0.

Этот протокол используется, когда:

- происходит авторизация на сторонних площадках через аккаунты

соцсетей или сервисов (например, СберID или ЕСИА);

◆ устанавливается на мобильное устройство приложение, взаимодействующее с данными в облачных сервисах, например Google или «Яндекс»;

◆ используются сторонние приложения (боты в мессенджерах) для уведомлений и пр.

Функционирование OAuth обеспечивается с помощью JWT-токенов (JSON Web Tokens).

Токен — это закодированная строка, используемая для аутентификации и авторизации пользователя без передачи его логина/пароля.

Например, пользователь может поделиться фотографиями из своего профиля в соцсети с приложением для редактирования фотографий. При этом приложению будет предоставлен доступ только к отдельным фотографиям и не будет предоставлен к сообщениям или списку друзей пользователя. Токен разрешает доступ только к данным, которые утверждает пользователь. Кроме того, с помощью токена может быть разрешён разовый или повторяющийся доступ, а также определён срок, на который этот доступ предоставлен.

Основные типы токенов:

◆ **токен доступа (Access Token):** ключевой токен, подтверждающий, что пользователь имеет право доступа к ресурсу;

◆ **токен обновления (Refresh Token):** используется для получения нового токена доступа после истечения старого, без повторной авторизации пользователя;

◆ **токен идентификации (ID Token):** используется при интеграции с OIDC для получения информации о пользователе.

Доступ с помощью OAuth всегда можно отозвать из раздела безопасности в настройках сервиса, с помощью которого была проведена авторизация.

OIDC. OIDC (OpenID Connect) — это открытый протокол аутентификации, который является надстройкой над протоколом OAuth 2.0, предназначенной для проверки личности пользователя и получения информации о его профиле.

Протоколы OAuth 2.0 и OIDC тесно связаны и обычно используются вместе.

SAML. SAML — открытый протокол обмена данными аутентификации и авторизации между ID-провайдером и сервис-провайдером.

Своим названием протокол SAML обязан применяемому для аутентификации пользователей и выдачи утверждений сервис-провайдерам языку разметки утверждений безопасности (Security Assertion Markup Language). Утверждения SAML представляют собой XML-документы, которые содержат информацию о субъекте (аутентифицированном пользователе) и различные соответствующие ему атрибуты. SAML широко используется в корпоративных системах SSO, и его поддержка является распространённым требованием при интеграции приложений B2B.

Mobile Connect. Работа ID-провайдера Мобильный ID основывается на технологии Mobile Connect.

Mobile Connect — это глобальный протокол безопасной аутентификации, разработанный Ассоциацией GSM (GSMA), который заменяет логины и пароли входом через номер мобильного телефона. Технология позволяет пользователям авторизовываться на сайтах и в приложениях, подтверждая личность через SIM-карту.

В основе работы протокола лежат OIDC и OAuth 2.0.

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ИСПОЛЬЗОВАНИЯ ID-ПРОВАЙДЕРОВ

К преимуществам использования ID-провайдеров для пользователей и бизнеса можно отнести следующие.

◆ **Снижение сложности работы с паролями.** Клиенты часто сталкиваются с трудностями при создании учётных записей, сбросе паролей и управлении множеством учётных данных в разных приложениях. При делегировании аутентификации ID-провайдеру появляется единая точка входа во все подключённые приложения.

◆ **Единые политики аутентификации.** Когда каждое приложение само отвечает за аутентификацию (проверку паролей, настройку двухфакторной аутентификации и т.д.), очень сложно добиться единых стандартов безопасности. ID-провайдер позволяет задать правила безопасности один раз, и они автоматически будут работать для всех приложений. Это делает аутентификацию предсказуемой и уменьшает поверхность атаки.

◆ **Повышение конверсии.** Сложная регистрация на сайте или в интернет-магазине часто становится причиной отказа от покупки. Клиент может «бросить» корзину и уйти на другой сервис. Чем короче путь пользователя от посещения сайта до покупки, тем выше маркетинговая эффективность. Использование ID-провайдера для аутентификации помогает бизнесу увеличивать продажи во всех приложениях экосистемы.

Вместе с тем использование ID-провайдеров имеет и свои недостатки.

◆ **Единая точка компрометации.** Если учётная запись пользователя в ID-провайдере будет скомпрометирована (например, через фишинг или вредоносное ПО), то станет возможным получение несанкционированного доступа не к одному, а сразу ко всем приложениям, которые доверяют этому провайдеру.

◆ **Единая точка отказа.** Выход из строя ID-провайдера (или интернет-канала до него) или DDoS-атака на него могут привести к тому, что пользователи потеряют доступ ко всем своим приложениям одновременно.

* * *

На практике бояться ID-провайдеров не стоит: если подойти к вопросу ответственно, выбрать проверенного провайдера и обязательно включить двухфакторную аутентификацию, то такой способ входа станет не только удобнее, но и надёжнее, чем использование множества разных паролей.

ИНФРАСТРУКТУРА ДОВЕРИЯ

ПЛАТФОРМА УПРАВЛЕНИЯ ДОСТУПОМ В ЭПОХУ ZERO TRUST

Андрей ТАРХОВ
директор по специальным проектам, Компания «Актив»

СОВРЕМЕННЫЕ УГРОЗЫ И ВЫЗОВЫ

Российские компании находятся сегодня в эпицентре кибервойны. Учащающиеся успешные целевые атаки приводят к параличу бизнес-процессов и катастрофическим убыткам. Анализ развития атак показал, что основная причина успеха современных кибератак — слабость парольной аутентификации, обусловленная фишингом, повторным использованием паролей, совместным использованием учетных записей сотрудниками и подрядчиками и слабыми механизмами хранения секретов в инфраструктуре.

Статистика выглядит однозначно: по данным группы компаний (ГК) «Солар», до 37% инцидентов связаны с компрометацией учетных записей; Лаборатория Касперского фиксирует, что 29% первичных проникновений начинаются именно с похищенных учетных данных, а BI.ZONE указывает, что 35% критичных инцидентов связаны с привилегированными аккаунтами. Международная картина еще показательнее: Microsoft и Google также отмечают высокую долю атак, стартующих с компрометации учетных данных. ФСТЭК прямо указывает на слабые пароли и однофакторную аутентификацию как ключевые причины успешных атак.

Параллельно с эскалацией угроз стремительно ужесточается регуляторное давление. Для госсектора введение Приказа ФСТЭК № 117 и Указа Президента № 250 стало жестким императивом к переходу на строгую аутентификацию в полностью импортозамещенный стек. Частный сектор также испытывает на себе давление растущих требований со стороны ЦБ РФ, международных стандартов и фреймворков (ISO27001, PCI DSS, CIS Controls, NIST CSF) и концепций типа Zero Trust, которые часто ложатся в основу корпоративных стратегий информационной безопасности.

НОРМАТИВНАЯ НЕИЗБЕЖНОСТЬ ZERO TRUST

Важно подчеркнуть, что концепция Zero Trust не противоречит российской нормативной базе и не требует ее пересмотра — напротив, она системно развивает уже закрепленные требования. Приказ ФСТЭК № 117 устанавливает необходимость строгой аутентификации и управляемого доступа, Указ Президента № 250 акцентирует импортонезависимость механизмов доверия, а отраслевые регуляторы требуют прослеживаемости и доказуемости контроля. Zero Trust переводит эти требования в целостную архитектурную логику: отказ от неявного доверия, обязательность подтверждения доступа и контроль привилегий на всех значимых этапах взаимодействия с ресурсами.

В условиях, когда компрометация учетных данных стала доминирующим сценарием атак, а регулятор требует доказуемой управляемости доступа, задача уже не ограничивается внедрением отдельных средств защиты. Речь идет о пересмотре самой модели доверия и формировании системного механизма контроля. В классическом определении Zero Trust исходит из предположения, что доверие не должно предоставляться по умолчанию ни субъекту, ни устройству, ни сегменту сети. Однако на практике многие внедрения ограничиваются лишь первоначальной аутентификацией, фактически воспроизводя модель «доверия после входа». Если доверие действительно не предполагается по умолчанию, оно должно подтверждаться в каждой значимой точке получения доступа — при первичном входе, повышении привилегий, смене контекста, обращении к критичным ресурсам.

Следовательно, доверие должно формироваться, проверяться и пересматриваться в рамках непрерывного процесса. В этой цепочке нужен элемент, доверие к которому не ставится под сомнение в силу высокой сложности компрометации, неподверженный фишингу, перехвату и воспроизведению,— элемент с аппаратной криптографией, обеспечивающей многофакторную аутентификацию.

НЕЗАВИСИМЫЙ ФАКТОР ДОВЕРИЯ: АППАРАТНАЯ АУТЕНТИФИКАЦИЯ КАК ФУНДАМЕНТ

В поиске аппаратной основы доверия нередко упоминается Trusted Platform Module (TPM). Его возможности важны: контроль целостности загрузки, защищенное хранение ключей, привязка криптографических операций к конечному устройству. Однако TPM не может рассматриваться как независимый аппаратный фактор аутентификации, поскольку является частью самой вычислительной платформы. Он подтверждает состояние устройства, но не личность пользователя. Поэтому TPM не решает задачу персонализированного подтверждения действия и не может выступать

вторым независимым аппаратным фактором в модели Zero Trust.

Если доверие должно быть персонализированным, переносимым между устройствами и устойчивым к компрометации, требуется аппаратный аутентификатор с неизвлекаемыми криптографическими ключами. Токен или смарт-карта генерируют и используют ключи внутри защищенного контейнера, исключая возможность их извлечения в программную среду. Дополнительное усиление обеспечивает контроль присутствия пользователя — подтверждение операции нажатием или биометрией.

НЕПРЕРЫВНОСТЬ ДОВЕРИЯ КАК АРХИТЕКТУРНЫЙ ПРИНЦИП

Однако сама по себе защищенность ключа еще не гарантирует целостности модели доверия. Аппаратный фактор должен работать не в одной точке входа, а во всей инфраструктуре. Современная крупная организация представляет собой гибридную среду с Linux и Windows, несколькими доменными службами и разнородными механизмами аутентификации. В таких гетерогенных средах существует множество точек контроля доступа: локальный и доменный вход, SSH, SUDO/UAC, VPN, VDI, прикладные системы, контейнерные платформы, мобильный доступ вне периметра. Если аппаратный фактор не интегрирован в сценарии контроля доступа во всех этих точках, реализация Zero Trust утрачивает архитектурную целостность и превращается в набор разрозненных механизмов аутентификации, не образующих единую модель доверия.

МАТЕРИАЛИЗАЦИЯ ZERO TRUST: ПЛАТФОРМА УПРАВЛЕНИЯ ДОСТУПОМ

Чтобы описанная модель работала не в презентации, а в инфраструктуре — чтобы токен действительно мог выполнять свою роль аппаратной основы доверия во всех точках доступа, ему требуется инфраструктурная обвязка, реализующая множество служебных процессов, скрытых от пользователя.

Требуется криптографическое ядро — корпоративный центр сертификации; компонент строгой аутентификации для Linux; единый слой управления доступом к разнородным ресурсам с централизованными политиками; а также централизованное управление жизненным циклом носителей и ключей (инициализация, выдача, перевыпуск, блокировка, отзыв, самообслуживание, аудит). Только совокупность этих компонентов создает платформу управления доступом корпоративного уровня.

Zero Trust в инженерной реальности — это не декларация, а совокупность технологических решений, обеспечивающих строгую аутентификацию, выпуск и проверку сертификатов, централизованное управление правами доступа и интеграцию с доменными службами и прикладными системами в гетерогенной среде. Такую систему необходимо рассматривать как целостную платформу, а не как совокупность разрозненных продуктов. На архитектурном уровне критична согласованность протоколов, криптографических механизмов и логики принятия решений о доступе (архитектура представлена на иллюстрации); на эксплуатационном — синхронизация релизных циклов, совместная проверка обновлений и единый контур технической поддержки, а также единая точка входа технической поддержки.

Если аппаратный токен формирует персональную точку доверия, то центр сертификации формирует инфраструктурный контур, внутри которого это доверие становится управляемым и проверяемым.

SafeTech CA представляет собой корпоративный центр сертификации для построения иерархии PKI в гетерогенной инфраструктуре: поддерживаются корневые, промежуточные и выпускающие центры, CRL/OCSP, хранение ключей центра в аппаратных модулях защиты, международные и отечественные алгоритмы, а также протоколы MS-WSTEP, SCEP, ACME и выпуск SSH-сертификатов. В платформе управления доступом SafeTech CA выполняет роль источника криптографического доверия, на базе которого реализуется строгая аутентификация пользователей в различных точках инфраструктуры.

В среде Windows аутентификация по смарт-карте является нативным элементом доменной архитектуры. В большинстве Linux-дистрибутивов такой механизм по умолчанию отсутствует. Решение Рутокен Логон для Linux устраняет этот инженерный разрыв, формируя системный механизм аппаратной аутентификации в среде Linux: интеграция в стек Privileged Access Management (PAM), доменная аутентификация по сертификату X.509 на токене, поддержка Active Directory, FreeIPA, SambaDC, ALD Pro и РЕД АДМ через Kerberos, централизованное развертывание и журналирование.

Indeed Access Manager формирует централизованный уровень управления доступом, связывающий доменную аутентификацию, прикладные системы и технологические сервисы. Поддерживаются RADIUS, SAML, OpenID Connect, ADFS, Kerberos. Это позволяет централизованно применять политики к веб-ресурсам и технологическому контуру (SSH, Git, CI/CD, Kubernetes), где критичны персонификация и контроль привилегий.

Рутокен KeyBox закрывает эксплуатационный слой: полный цикл работы с ключевыми носителями и сертификатами, автоматизацию операций, аудит, работу в гетерогенных средах с несколькими LDAP-каталогами и удостоверяющими центрами (УЦ), ролевое делегирование. Интерфейс самообслуживания (смена/разблокировка PIN, обновление сертификата, временная блокировка или отзыв токена) снижает нагрузку на техподдержку и уменьшает объем массовых обращений, связанных со сбросом и изменением паролей. Формализованный и автоматизированный жизненный цикл носителей завершает построение Платформы управления доступом как основы всей архитектуры доверия.

ПЛАТФОРМА УПРАВЛЕНИЯ ДОСТУПОМ КАК СТРАТЕГИЧЕСКИЙ АКТИВ ОРГАНИЗАЦИИ

На этом этапе проявляется практический симбиоз российской норма-

Иллюстрация 1. Архитектура Платформы управления доступом

тивной базы и реальной реализации Zero Trust: требования ФСТЭК к строгой аутентификации и управляемости доступа получают архитектурное воплощение в виде единой платформы, обеспечивающей непрерывное подтверждение доступа и прослеживаемость действий. Импортонезависимый стек становится не только условием соответствия, но и элементом архитектурной зрелости. В результате платформа управления доступом превращается в стратегический актив организации, снижающий операционные риски и повышающий устойчивость бизнеса.

Дополнительный эффект заключается в снижении совокупной стоимости владения (Total Cost of Ownership, TCO): централизованное управление аутентификаторами, автоматизация выпуска и перевыпуска сертификатов, самообслуживание пользователей и унификация протоколов устраняют избыточные интеграции, сокращают нагрузку на службу поддержки и уменьшают количество ручных операций. Одновременно улучшается пользовательский опыт: единый аппаратный фактор исключает использование сложных паролей, требующих постоянной смены, упрощает сценарии доступа в гибридной среде и снижает когнитивную нагрузку на сотрудников. При этом уровень защищенности возрастает системно – исключается фишинг, минимизируется риск компрометации привилегированных учетных записей и обеспечивается криптографически доказуемая персонификация действий.

СКВОЗНАЯ ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

ОТ УЧЕТНОЙ ЗАПИСИ К РЕАЛЬНОМУ ЧЕЛОВЕКУ

Евгений БРАЖНИКОВ
владелец продукта Platform V IDM

Когда сотрудник увольняется, в идеале должно произойти одно простое действие — блокировка его учётных записей во всех системах. На практике это работает не всегда так, потому что никто достоверно не знает, где этот человек существует в IT-инфраструктуре организации.

HR-система зафиксировала увольнение. Active Directory — нет. В 1С: ERP/SAP его учётная запись активна. В финансовой системе «живёт» привилегированная учётная запись `admin_fin_03`, созданная «временно» пару лет назад, и чья она, уже никто не помнит.

Это не редкость и не халатность. Это системный результат одной структурной проблемы: в инфраструктуре большинства организаций отсутствует единое понятие субъекта / физического лица.

ОДИН ЧЕЛОВЕК — ДЕСЯТКИ ИДЕНТИФИКАТОРОВ

Один субъект — сотрудник, подрядчик или администратор — в реальной корпоративной среде, как правило, имеет одновременно:

- запись в HR-системе с табельным номером;
- учётную запись в корпоративном Active Directory с идентификатором по sAMAccountName;
- технические учётные записи для работы с базами данных;

учётные записи с обезличенными именами: `admin_1c`, `postgres_fin_rw` и т.п.;

- аккаунты на внешних платформах, зарегистрированные на личную почту.

Каждый из этих идентификаторов корректен в контексте своей системы. Но как только возникает вопрос «кто это сделал» в масштабах всей организации, дать однозначный ответ не получается. Связать журналы аудита из разных систем без заранее выстроенных правил сопоставления крайне сложно.

ПОЧЕМУ СИСТЕМЫ НЕ ПОНИМАЮТ ДРУГ ДРУГА

В каждой системе своя логика идентификации, и она принципиально различается.

Active Directory использует SID (Security Identifier) как неизменяемый эталон и sAMAccountName как оперативный идентификатор. Второй может меняться при переводах и переименованиях.

ERP-системы (1С: ERP, SAP) используют собственные табельные номера, никак не связанные с корпоративной схемой идентификации.

Внешние платформы нередко идентифицируют пользователей по электронной почте — атрибуту, который в организации является изменяемым и может переходить от одного сотрудника к другому в связи со сменой фамилии или из-за структурных изменений.

Проблема возникает на стыках при попытке сопоставить событие из журнала одной системы с событием в другой.

К ЧЕМУ ЭТО ПРИВОДИТ

Неспособность обеспечить сквозную идентификацию — не теоретическая проблема. Это источник конкретных операционных и регуляторных рисков.

Слепые зоны для SOC. Инцидент, начавшийся в одной системе и продолжившийся в другой, невозможно расследовать как единую цепочку событий. Security Information and Event Management (SIEM) — система собирает события, но не может коррелировать их по субъекту, если нет связующего слоя над разрозненными идентификаторами. Аналитик видит два несвязанных события вместо одной атаки.

«Мёртвые души» и избыточный доступ. Без сквозного отслеживания жизненного цикла перевод или увольнение не влечёт автоматической блокировки учётных записей сотрудника. По данным отраслевых исследований, значительная часть активных учётных записей в организациях фактически не имеет владельца.

Атрибутный дрейф. Без единого источника правды ФИО, должность, подразделение, контактные данные расходятся в разных системах. Сотрудник, сменивший фамилию, через год присутствует в разных каталогах под разными именами, и автоматическая корреляция становится невозможной.

КАК ВЫСТРАИВАЕТСЯ РЕШЕНИЕ

Единая идентификация субъектов — это не готовое решение, которое покупается и включается. Это архитектурный слой, надстраиваемый над существующими системами без их замены. Он держится на нескольких принципах.

Мастер-идентификатор субъекта. Каждое физическое лицо получает единственный неизменяемый ключ, не зависящий ни от имени, ни от табельного номера, ни от email. Этот ключ не меняется при смене фамилии, переводе или реорганизации. Он становится осью, вокруг которой выстраиваются все локальные идентификаторы.

Корреляционная матрица. Identity Management (IDM)-система строит и поддерживает в актуальном состоянии карту соответствий: мастер-идентификатор ↔ множество локальных идентификаторов во всех подключённых системах. Новая учётная запись, обнаруженная при реконсиляции, либо автоматически привязывается к существующему субъекту, либо помечается как неопознанная и передаётся на ручной разбор.

Единый авторитетный источник. Вопрос «кому верить» решается один раз: HR-система является истиной для персональных данных, и только она инициирует изменения в остальных системах. Если данные расходятся, приоритетом становится HR-система, а не та система, в которой что-то поменяли вручную в последний раз.

Разделение IDM и IdP. IDM-система управляет тем, кем является субъект: ведёт жизненный цикл учётных записей, синхронизирует данные между системами, обнаруживает аномалии. IdP (Identity Provider) отвечает за то, что субъекту разрешено: политики доступа, Single Sign-On (SSO), выдача токенов. Это не дублирующие инструменты, а смежные слои одной архитектуры. Смешивать их задачи в одной из систем — лишиться преимуществ обоих.

Сквозной аудит. Любое событие в любой системе, попадающее в SIEM или Security Operations Center (SOC), несёт тег с мастер-идентификатором субъекта. Аналитик видит не набор несвязанных логинов, а единого человека, чьи действия прослеживаются сквозь всю экосистему.

КАК ЭТО ВЫГЛЯДИТ НА ПРАКТИКЕ

Опыт пилотных проектов и внедрений показывает три закономерности, с которыми сталкивается каждый проект.

Без единого источника правды ФИО, должность, подразделение, контактные данные расходятся в разных системах. Сотрудник, сменивший фамилию, через год присутствует в разных каталогах под разными именами

Инвентаризация всегда удивляет. Прежде чем строить корреляции, нужно ответить на вопрос, сколько субъектов вообще существует в организации. Пересечение данных HR-системы, Active Directory и нескольких бизнес-систем выявляет от сотен до тысяч аномалий — дублей, «мёртвых душ», учётных записей с неустановленной принадлежностью. Единственное, в чём сходятся все участники проекта на этом этапе,— результаты не совпадают с ожиданиями. Зрелые IDM-решения автоматизируют этот этап через механизм реконсиляции. Например, в Platform V IDM при первом сканировании подключённых систем формируется полная карта учётных записей, каждой из которых присваивается статус: привязана к субъекту, помечена как неизвестная или выделена в очередь на ручной разбор. Это не разовая процедура: реконсиляция запускается по расписанию или по событию и непрерывно фиксирует любые отклонения от ожидаемого состояния.

Закон сохранения легаси. В каждом реальном проекте найдётся система, чья единственная форма выгрузки — CSV-файл, по расписанию попадающий в сетевую папку на отдельном файловом сервере, а рядом — интеграционная шина, получающая кадровые события по схеме, зафиксированной при первом запуске и не менявшейся с этого момента. Это не исключение, а норма. IDM-системы как Platform V IDM дают возможность адаптировать коннектор под такие источники самостоятельно, без привлечения вендора. Схема атрибутов определяется при подключении, а изменения в источнике обрабатываются по мере поступления в очередь брокера, не дожидаясь следующего сеанса реконсиляции.

Серая зона корреляции. Алгоритмы сопоставления по ФИО, дате рождения, email и табельному номеру дают высокий процент совпадений, но всегда оставляют записи, которые нельзя привязать автоматически. Большинство систем на этом останавливаются. Выход — многоступенчатая корреляция: каждое правило сопоставления получает числовой коэффициент уверенности, правила комбинируются с настраиваемыми весами, итоговый балл определяет исход. Такой подход реализован, в частности, в механизме корреляции решения для централизованного управления учетными записями сотрудников, их правами и доступом к информационным ресурсам организации Platform V IDM. Пороговые значения настраиваются под требования организации, а каждое решение, автоматическое и принятое оператором, фиксируется в аудите.

ЗАКЛЮЧЕНИЕ

Сквозная идентификация субъекта — это не технологический тренд, а базовая необходимость управляемой ИТ-среды, позволяющая в любой момент и в любой системе ответить на вопрос «кто это».

Организации, которые выстраивают этот слой, получают не просто порядок в каталогах. Они получают фундамент для работающего SOC, прозрачного аудита и реального управления доступом. Те, кто игнорирует проблему, продолжают жить в среде, где `admin_fin_03` — это чья-то учётная запись, владельца которой знал только IT-специалист, уволившийся неделю назад.

СМОТРЕТЬ НА ДАННЫЕ ЧЕРЕЗ НАСТРОЙКИ И ПОЛИТИКИ — ЭТО ВСЕ РАВНО, ЧТО НАБЛЮДАТЬ МИР В ЗАМОЧНУЮ СКВАЖИНУ

Андрей АРЕФЬЕВ
директор по инновациям и продуктовому развитию ГК InfoWatch

Перед любой ИБ-службой рано или поздно возникает вполне типичная рабочая задача: нужно понять, что именно хранится на рабочей станции конкретного пользователя или в файловом хранилище. Поводы могут быть разными — проверка сотрудника, разбор инцидента, аудит старого файлообменника, где данные накапливались годами. Но суть всегда одна: перед ИБ-специалистом оказывается массив документов, содержание которого заранее неизвестно.

Все системы, которые сейчас есть на рынке для решения подобной задачи, включая Data Loss Prevention (DLP) и Data-Centric Audit and Protection (DCAP), имеют одну особенность — чтобы они могли работать с данными, их нужно предварительно обучить: задать словари, создать политики, настроить правила. Этот процесс занимает много времени: необходимо собрать образцы текстов, произвести донастройки, разобраться с ложноположительными и ложноотрицательными срабатываниями.

Мы в InfoWatch предложили принципиально иной подход, при котором человеку не нужно обучать систему: она сама «рассказывает» о данных, которые есть в компании. Эту логику мы реализовали в модуле «Кластеризация данных» в составе продукта для аудита данных InfoWatch Data Discovery.

КАК ВЫГЛЯДИТ ПРОЦЕСС

Представьте, что перед вами стоит задача разобраться, какие файлы хранятся на файловом сервере, нет ли там конфиденциальной информации, которая ещё не покрыта политиками, или документов, для которых требуется ужесточение прав доступа. Это выглядит так, как если бы на вашем письменном столе лежала кипа неопознанных документов, которые нужно вручную просмотреть и рассортировать, — коммерческие предложения в одну стопку, рамочные договоры — в другую, прайс-листы — в третью, и так далее.

Когда вы применяете Data Discovery вместе с модулем «Кластеризация данных», документы на вашем столе уже не свалены в одну кучу, а разобраны в тематические стопки (кластеры), которые не только скреплены между собой, но еще и размечены стикерами с ключевыми терминами для каждой стопки (рис. 1–2).

В ЧЕМ ОСОБЕННОСТЬ РЕШЕНИЯ

Модуль «Кластеризация данных» не требует обучения, не содержит словарей и предустановленных настроек и обучается именно на данных компании. Работа начинается, по сути, с чистого листа, когда ни решение, ни человек ничего не знают об информационных активах компании.

И вот, например, вам нужно разобраться, какие данные хранятся на файловом сервере. После его сканирования весь документооборот, даже самый экзотический, будет проанализирован, термины извлечены, а документы с одинаковой терминологией объединены в кластеры. Для каждого кластера определятся ключевые теги, из которых составится облако тегов — набор ключевых слов, которые лучше всего описывают каждую группу.

Кластеры можно отфильтровать, выбирая нужные теги. В результате будет построена карта кластеров, которая визуально отображает, какие кластеры схожи по терминологии между собой, а какие отличаются. Основной рабочий массив на карте формируют типовые документы, связанные с функциями сотрудника, подразделения, спецификой бизнеса. Рядом показываются группы и отдельные документы, которые статистически выбиваются из общей картины. Частотные термины показывают устойчивые темы, редкие — помогают быстро выйти на нетипичные или слабо представленные информационные активы. За счёт этого анализ файлового массива происходит не через просмотр файлов в ручном режиме, а через анализ смысловых признаков (рис. 3).

Рисунок 1–2. Документы без кластеризации и с кластеризацией

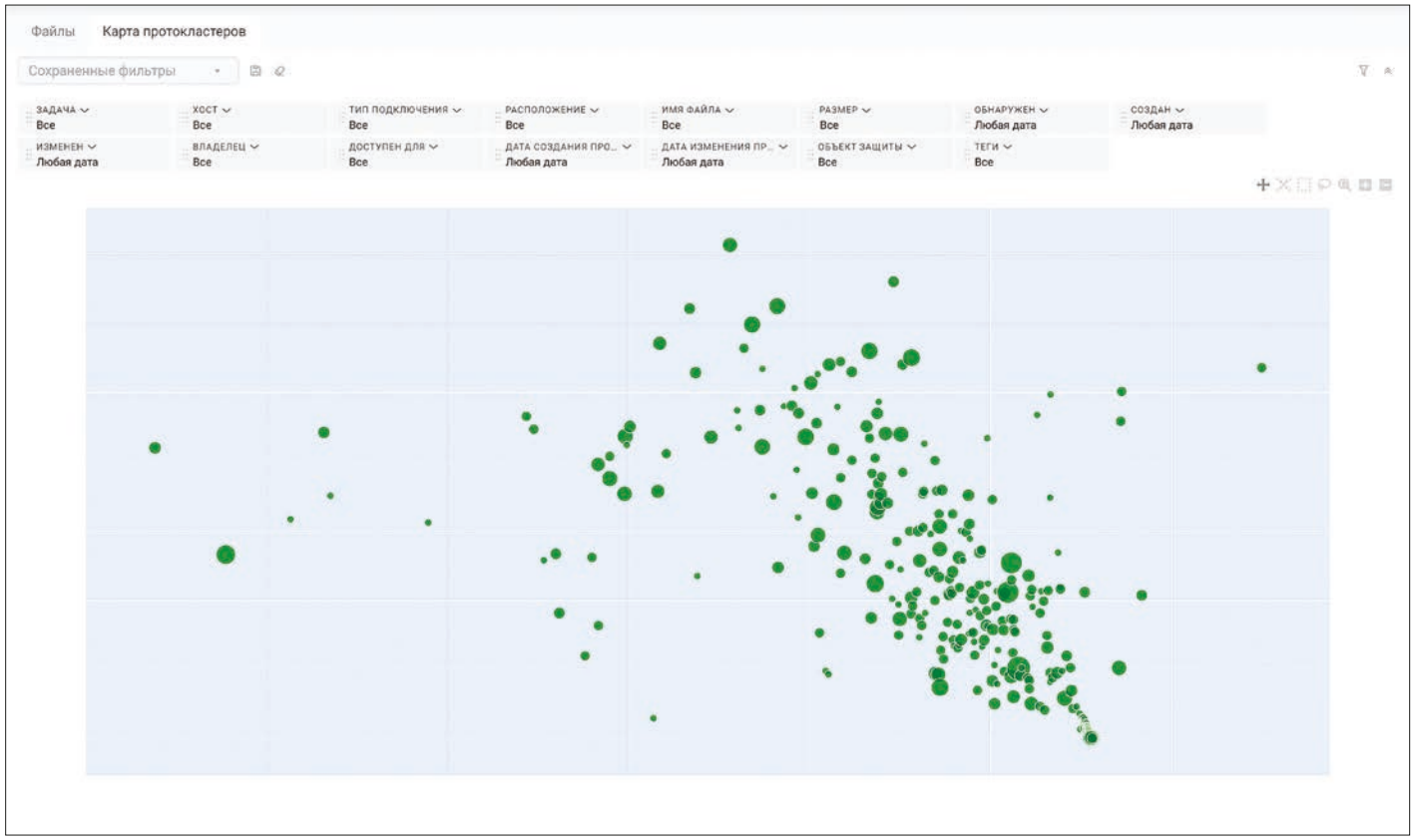


Рисунок 3. Карта документов показывает структуру проанализированного массива

Рассмотрим карту документов и облако тегов более подробно.

Карта документов показывает структуру проанализированного массива. На ней в кластеры собираются документы, которые похожи по терминологии и, как правило, относятся к одному и тому же виду деятельности. Если смотреть на это со стороны пользователя, то сразу видно, где находится основной рабочий профиль — плотные, крупные кластеры. Рядом с ними появляются более мелкие группы и отдельные документы, которые вообще не вписываются в общую картину.

Облако тегов дает возможность быстрого погружения в содержание файлового массива. Каждый тег — это ключевое слово из проанализированных документов. Более частотные слова описывают типовые процессы, характерные для пользователя или подразделения. В одном случае это может быть производственная терминология, в другом — логистика, закупки или внутренняя отчётность. Уже на этом уровне становится понятно, чем «живет» конкретный массив данных.

Но главная практическая ценность проявляется в отклонениях. Редкие слова в облаке тегов и небольшие группы на карте позволяют быстро выявить аномалии. Это может быть тема, не связанная с деятельностью сотрудника, документы из другой области или просто нетипичный набор материалов.

Дальше имеет смысл не просматривать все кластеры и теги подряд, а начинать с крайних точек: либо с редких тегов, либо с небольших кластеров, переходить к конкретным документам и принимать решение, требуют ли они внимания.

Важно, что модуль «Кластеризация данных» не навязывает свою интерпретацию. Он не сигнализирует, что документ является нарушением или инцидентом, а лишь показывает фактическую структуру массива и дает возможность быстро найти отклонения. Оценка остается за специалистом, но при этом объем ручной работы значительно сокращается за счет того, что система сама систематизирует данные и наглядно демонстрирует, что с ними происходит в реальности, не ограничиваясь субъективными факторами — словарями, политиками и правилами.

Подобных решений на рынке сейчас просто не существует, несмотря на то что кластеризация как технология не уникальна. Чаще всего объем кластеризуемых документов ограничивается лишь несколькими сотнями документов, так как известные алгоритмы кластеризации требуют большого объема оперативной памяти и мощного аппаратного обеспечения. При помощи модуля «Кластеризация данных» пользователь может систематизировать любой массив данных, не выдвигая высоких требований к аппаратному обеспечению, достаточно сервера средней стоимости.

КАК ЭТО СТАЛО ВОЗМОЖНЫМ И ЧТО ПОД КАПОТОМ?

Модуль «Кластеризация данных» позволяет «увидеть» все информационные активы компании в любом объеме благодаря нашей собственной технологии потоковой кластеризации, которая систематизирует дан-

ные постепенно, в потоковом режиме, по мере поступления и обработки документов без необходимости пересчитывать весь массив целиком. Это принципиальный момент: вместо глобального пересчета используется постепенное уточнение структуры через промежуточные кластеры. За счет этого вычисления распределяются во времени и не требуют большого потребления памяти в моменте. С помощью потоковой кластеризации документы индексируются и объединяются в группы с высокой скоростью и точностью при низком потреблении аппаратных ресурсов.

В одном из недавних кейсов процесс сканирования файлового хранилища занял пять часов, а процесс кластеризации всего массива данных завершился через 20 минут после загрузки последнего файла. Пока сканер собирал документы, модуль обрабатывал файлы в фоновом режиме, не требуя при этом большого объёма оперативной памяти.

Уникальность технологии подтверждена патентом «Способ потоковой кластеризации данных» (патент № 2844055). Кроме того, изобретение вошло в число победителей конкурса «Успешный патент», который проводит Федеральная служба по интеллектуальной собственности (Роспатент). Важно, что технология применима не только в информационной безопасности, но и в других сферах деятельности, где необходимо систематизировать большой объём текстовых документов, например для мониторинга соцмедиа, систематизации научных статей, исследования новостных трендов и так далее.

БОРЬБА С ЛОСАМИ — БОЛЬШЕ НЕ МИФ

Модуль содержит фильтры, которые позволяют отсортировать документы по дате создания и просмотреть недавно созданные и неразмеченные политиками файлы, хранящиеся на рабочих станциях, чтобы отследить нетипичный, аномальный кластер. Это практически нереально сделать вручную: пришлось бы просматривать все документы и проверять их на соответствие созданным политикам. Модуль помогает разобраться с «серой зоной» и увидеть подводную часть айсберга, не учтенную в политиках, которая может составлять до 70% информационных активов. Это особенно актуально для организаций, чей конфиденциальный документооборот создается внешними контрагентами за пределами компании, а значит необходимо отслеживать не только данные, которые хранятся внутри, но и входящие потоки.

Показателен опыт заказчиков, когда задача заключалась в разборе 4 000 документов, которые были скачаны на флешку, но не попали в поле зрения DLP-системы, так как не были покрыты политиками. Оценка ручного разбора составляла 30 дней, а с модулем «Кластеризация данных» на это ушло порядка полутора часов. В другом случае модуль использовался не для поиска нарушений, а для аудита файлового хранилища, чтобы собрать образцы документов и создать политики — задача, которую не могли решить долгое время из-за большого объема ручной работы.

ПРАКТИЧЕСКИЕ СЦЕНАРИИ ПРИМЕНЕНИЯ

1. Аудит рабочей станции или файлового хранилища, когда нет четкого понимания, что именно нужно найти. Система сразу выделяет группы документов и позволяет быстро выйти на отклонения.

2. Поиск заведомо нежелательного или нетипичного контента. Здесь пригодятся наиболее редкие слова в облаке тегов и небольшие группы на карте. Они позволяют быстро выйти на документы, которые не являются частью основной деятельности. Это могут быть документы из другой области или просто содержимое, которое требует отдельной проверки.

3. Подготовка к внедрению, обучению или настройке другой системы, например, DLP. На практике одна из самых трудоемких задач — собрать образцы документов, по которым можно будет в дальнейшем настроить политики и обучить систему. Когда исходный массив не структурирован, такая подготовка превращается в длительный ручной процесс. В этом случае модуль создаст готовые группы, из которых можно быстро выделить нужные типы документов и использовать их как основу для дальнейшей настройки DLP-системы.

Общий эффект во всех сценариях один и тот же — основное время уходит не на классификацию отдельных документов, а на их кластеризацию. Если эту часть работы делает система, дальнейшие действия становятся значительно быстрее и более осмысленными.

ОСОБЕННОСТИ РАБОТЫ РЕШЕНИЯ

- Продукт не требует существенного дискового пространства, потому что использует данные Data Discovery, не дублируя их.
- Продукт индексирует данные непрерывно в фоновом режиме по мере сканирования файлов. То есть к тому моменту, когда вы приступите к работе, данные уже будут проиндексированы.
- Может разбирать не только текстовые файлы, но и PDF, сканированные копии, распознает мультиязычные документы.

В ЗАКЛЮЧЕНИЕ

В текущих реалиях смотреть на данные через настройки и политики — это все равно, что наблюдать мир в замочную скважину. Как правило, политиками и правилами покрыто лишь около 30–40% информационных активов компании, так как это ресурсоемкий и дорогой процесс, все остальное — это та самая подводная часть айсберга, про которую ничего неизвестно, и о существовании которой зачастую никто даже не догадывается.

Переход от классификации к кластеризации данных, который мы предлагаем, позволяет увидеть абсолютно все данные, понять, что с ними происходит в реальности, разобрать «серую зону», систематизировать информационные потоки компаний, исчисляемые миллионами событий ежедневно, и таким образом снижать риски скрытых угроз и проводить расследование в десятки раз быстрее.

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

УПРАВЛЯЙТЕ ПРОЦЕССАМИ ИБ — ЭКОНОМЬТЕ ВРЕМЯ И ДЕНЬГИ БИЗНЕСА!

Николай КАЗАНЦЕВ
CEO SECURITM

Сегодня команды ИБ сталкиваются с ситуацией, где темпы роста и изменений инфраструктуры превышают возможности ручного контроля. Сервисы внедряются молниеносно, обгоняя инвентаризацию активов, а формирование отчётов часто скатывается в замкнутый круг повторных проверок и ручного выравнивания данных. В этих условиях SECURITM выходит на первый план как решение, помогающее бизнесу эволюционировать от интуитивного управления к структурированной, динамичной и автоматизированной системе кибербезопасности.

Основа работы SECURITM строится на актуальном реестре активов. На практике большинство ошибок и упущений рождается именно из «чёрных зон» — непромаркированных серверов, забытых систем, неучтённых интеграций. Динамичная CMDB в SECURITM фиксирует не только список устройств и сервисов, но и их функции в бизнес-цепочках, ответственных, взаимосвязи и степень важности. Благодаря этому компании отказываются от инвентаризаций «по памяти» или «на глазок» и переходят к автоматизированному мониторингу конфигураций, выявлению новых компонентов и учёту изменений в инфраструктуре в реальном времени.

Модуль соответствия требованиям (Compliance) переводит взаимодействие с регуляторами из плоскости бумажной волокиты в повседневные операции. Позволяет автоматизировать оценку соответствия требованиям ГОСТ Р 57580.1, 57580.2, 57580.3, 57580.4, Положений Банка России № 757-П, 821-П, 833-П, 802-П, 808-П, 822-П, 779-П, 716-П, а также стандартов PCI DSS и SWIFT. Помимо автоматизации соответствия банковским требованиям, система обеспечивает комплаенс по требованиям к защите персональных данных, критической инфраструктуре, лучшим мировым практикам ISO 27001, CIS CSC, NIST и требованиям по безопасной разработке ПО. Благодаря корреляции требований всех стандартов, система оптимизирует выполнение требований: соблюдение одного нормативного акта автоматически упрощает соответствие другим. Если к проверкам готовиться вручную, процесс занимает недели — нужно либо нанимать аудиторов, либо держать сотрудника, который постоянно отслеживает изменения. Но инфраструктура компании — крайне динамичная среда: системы появляются, меняются и исчезают быстро, маркетинг запускает кампании, интеграции происходят постоянно. В таких условиях без автоматизации поддерживать комплаенс невозможно. Использование модуля Compliance SECURITM существенно сокращает время подготовки к проверкам и переводит взаимодействие с аудиторами из режима «пожара» в режим регулярной операционной дисциплины.

Модуль управления рисками связывает технологическую часть с бизнес-контекстом. Это конкретные сценарии: как та или иная уязвимость или отсутствие меры повлияют на критичные процессы, сколько стоит простой, какие подразделения окажутся недоступны. SECURITM позволяет приоритизировать вложения в ИБ по экономическому эффекту и допустимому риск-аппетиту компании. В результате решения принимаются быстрее и более обоснованно, а ИБ становится полноценным управленческим инструментом.

Отдельное место занимает система метрик и KPI. Метрики в SECURITM — понятные рабочие индикаторы, связанные с автоматизацией процессов. Они показывают покрытие сканерами, долю устранённых проблем, время реакции, полноту инвентаризации, процент подрядчиков с актуальными соглашениями и многое другое. Важно, что метрики связаны с триггерами: при достижении критических порогов система автоматически создаёт задачи, уведомляет ответственных и при необходимости инициирует автоматизированные сценарии реагирования. Так IT-операции перестают «плавать» в нескольких консолях, а безопасность начинает работать в режиме живого управления.

Автоматизация операционной деятельности: задач много, фиксировать их в блокнотах бессмысленно, а при кросс-функциональном взаимодействии с ИТ или другими подразделениями компании это ещё и крайне неэффективно. Модуль задач SECURITM позволяет автоматически формировать задачи, назначать сроки и ответственных, приобщать

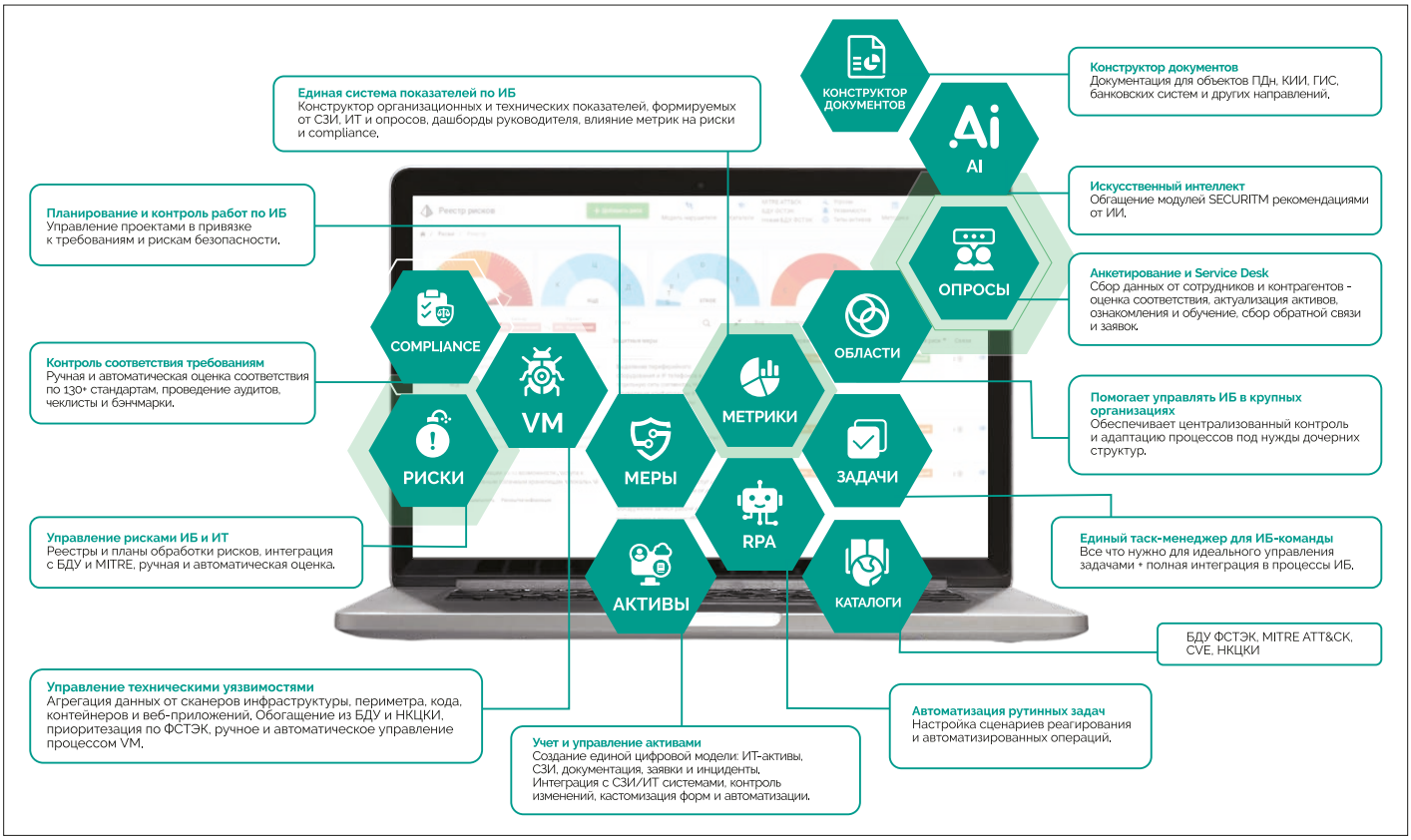


Рисунок 1. Модули системы SECURITM

файлы, отслеживать прогресс. И что важно — не дергать сотрудника по каждому пустяку. SECURITM помогает работать в единой цифровой среде.

Интеграционная способность SECURITM — ключевой фактор её практической ценности. Вместо разрозненных консолей средств защиты информации (СЗИ) SECURITM предлагает единую систему: интеграцию с 50+ типами СЗИ (антивирусы, межсетевые экраны, Security Information and Event Management (SIEM), Data Loss Prevention (DLP), системы обнаружения и предотвращения вторжений (IDS/IPS), сканеры уязвимостей) благодаря автоматическому сбору и нормализации данных из разных форматов в единую модель. В итоге вы получаете единую консоль мониторинга со всеми алертами, инцидентами и уязвимостями, кросс-корреляцию событий для выявления сложных атак, оценку эффективности СЗИ, через метрики покрытия, ROI и «слепые зоны» на одном экране, в одной системе. Благодаря API для интеграции с IT Service Management (ITSM), Configuration Management Database (CMDB) и системами мониторинга с автообновлением данных, вы получаете управление жизненным циклом СЗИ от закупки до списания, включая контроль лицензий и обновлений. Такое объединение даёт эффект синергии: информация становится общим источником правды.

Безопасники внедрившие систему компаний отмечают существенное сокращение времени на подготовку отчётности и аудитов, рост доли автоматизированных процессов и ускорение реакции на уязвимости. Экономический эффект складывается из снижения вероятности простоев, уменьшения операционных затрат на рутинную отчётность и повышения уверенности в работе с регуляторами и партнёрами.

Прямо сейчас данные и сервисы становятся ключевым активом компаний. Информационная безопасность стала интегрированной частью бизнес-управления, инструментом для принятия решений. Система управления информационной безопасностью SECURITM предлагает путь от бумажных отчётов к живой системе, где каждая метрика, каждая задача и каждый защитный механизм связаны с единой целью — снижением реальных бизнес-рисков. Такой подход превращает затраты в инвестиции в устойчивый рост.

Если ваша организация всё ещё ведёт ИБ на бумаге или в Excel, а не управляет реальными рисками, пришло время изменить подход. SECURITM предоставляет инструменты, методику и сопровождение, необходимые для перехода от формального соответствия к управляемой и прозрачной безопасности, которая работает в интересах бизнеса. И первое, с чего действительно стоит начать, — это с простого шага: получить инструмент, который сразу станет опорой для вашей службы ИБ. Для этого мы и сделали бесплатную Community-версию SECURITM (*https://service.securitm.ru/register*).

Она помогает выстроить базовый порядок, увидеть процессы целиком и начать управлять безопасностью системно — независимо от масштаба компании.

КВАРТАЛЬНЫЙ ОТЧЁТ

О НОРМАТИВНОМ РЕГУЛИРОВАНИИ В СФЕРЕ ИБ В I КВАРТАЛЕ 2026 ГОДА

Екатерина РАЧКОВА
обозреватель BIS Journal

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

26.02.2026 опубликовано распоряжение Правительства Российской Федерации от 26.02.2026 № 360-р.

Данным распоряжением утверждается перечень типовых отраслевых объектов критической информационной инфраструктуры (КИИ) Российской Федерации.

ПРЕЗИДЕНТ И ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

23.01.2026 в Государственную Думу Российской Федерации внесён законопроект № 1129912–8 «О внесении изменений в статью 44.1–1 Федерального закона «О связи» (в части установления требований к идентифицируемости голосов автоматизированных телефонных систем при осуществлении массовых и (или) автоматических телефонных вызовов)». Законопроект вносит новое требование к звонкам с использованием автоматизированных систем: их звуковое сопровождение должно быть явно отличимо от человеческого голоса и не должно быть способно создать впечатление общения с человеком.

27.01.2026 в Государственную Думу Российской Федерации внесён законопроект № 1133088–8 «О внесении изменения в статью 272.1 Уголовного кодекса Российской Федерации». Законопроект призван сделать уголовно наказуемым незаконное создание «дипфейков» путём автоматизированной обработки данных. Для этого предлагается дополнить часть 1 статьи 272.1 УК РФ понятием «автоматизированная обработка» как самостоятельным общественно опасным деянием. В случае принятия законопроекта преступлением будет считаться сам факт незаконной автоматизированной обработки персональных данных, полученных неправомерным путём, независимо от того, как они использовались в дальнейшем.

07.02.2026 опубликовано Постановление Правительства Российской Федерации от 06.02.2026 № 92 «Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры Российской Федерации в банковской сфере и иных сферах финансового рынка».

МИНЦИФРЫ РОССИИ

03.02.2026 опубликован приказ Минцифры России от 02.02.2026 № 49 «О внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 09.02.2021 № 69 «Об утверждении перечней нормативных правовых актов (их отдельных положений), содержащих обязательные требования, оценка соблюдения которых осуществляется в рамках государственного контроля (надзора), привлечения к административной ответственности в сферах электронной подписи и идентификации и (или) аутентификации».

Также 03.02.2026 опубликован приказ Минцифры России от 02.02.2026 № 45 «Об утверждении перечня нормативных правовых актов (их отдельных положений), содержащих обязательные требования, оценка соблюдения которых осуществляется в рамках федерального государственного контроля (надзора) в сфере электронной подписи и привлечения к административной ответственности за нарушение обязанностей, предусмотренных законодательством Российской Федерации в области электронной подписи».

ФСТЭК РОССИИ

15.01.2026 ФСТЭК России были опубликованы «Рекомендации по предотвращению реализации угроз безопасности информации при применении SAP-систем в условиях прекращения их технической поддержки и распространения обновлений на территории Российской Федерации». Данные рекомендации направлены на предотвращение реализации угроз информационной безопасности (ИБ) при применении систем планирования и учета ресурсов предприятия (SAP-системы) в условиях прекращения их технической поддержки и распространения обновлений на территории Российской Федерации. К таким системам относятся: платформы SAP NetWeaver ABAP, SAP NetWeaver Java, SAP S/4HANA, SAP Solution Manager (SAP-системы тестовой и производственной инфраструктуры, инфраструктуры разработки, системы управления базами данных SAP HANA, Oracle, Microsoft SQL Server и MaxDB) и их компоненты. Указанные рекомендации направлены на осуществление настройки параметров, ролей, сервисов и учетных записей, подлежащих контролю и приведению к безопасным значениям в SAP-системах.

30.01.2026 ФСТЭК России опубликованы «Рекомендации по безопасной настройке программного обеспечения Samba». Указанные рекомендации направлены на обеспечение информационной безопасности в информационной инфраструктуре органов государственной власти и субъектов критической информационной инфраструк-

туры Российской Федерации, использующих программное обеспечение «Samba».

09.02.2026 ФСТЭК России были опубликованы «Рекомендации по устранению типовых ошибок конфигурации (настройки) общесистемного и прикладного программного обеспечения». По результатам анализа инцидентов ИБ, проводимого в период 2024–2025 годов, ФСТЭК России были выявлены типовые ошибки конфигурации (настройки) общесистемного и прикладного программного обеспечения, которые способствуют реализации злоумышленниками угроз безопасности информации при осуществлении целевых компьютерных атак, а также разработаны рекомендации по их устранению. Указанные рекомендации направлены на нейтрализацию угроз безопасности информации, связанных с ошибками конфигурации (настройки) общесистемного и прикладного программного обеспечения.

11.03.2026 ФСТЭК России опубликованы «Рекомендации по защите сетевого периметра информационных (автоматизированных) систем». По результатам анализа успешных фактов реализации угроз безопасности информации, связанных с удаленной эксплуатацией уязвимостей, а также осуществлением несанкционированного доступа к внутренней инфраструктуре из внешней сети, разработаны рекомендации по защите сетевого периметра информационных (автоматизированных) систем, содержащие мероприятия по администрированию сетевых (пограничных) устройств, защите от атак, направленных на «отказ в обслуживании», сегментированию сети, резервному копированию, управлению уязвимостями, аутентификации и управлению доступом пользователей и администраторов, регистрации событий ИБ, проведению регулярных учений. Указанные мероприятия направлены на нейтрализацию угроз безопасности информации, связанных с уязвимостями сервисов и недостатками конфигурации сетевых (пограничных) устройств, находящихся на внешнем периметре информационной инфраструктуры органа (организации).

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

30.01.2026 Банком России опубликована выписка из «Требований к техническим средствам и программному обеспечению, реализующим криптографические механизмы информационной инфраструктуры значимой платежной системы, используемых при осуществлении переводов денежных средств по карточным счетам» для заказчиков указанных средств. Разработчикам и специализированным организациям необходимо запрашивать полную редакцию документа «Требования к техническим средствам и программному обеспечению, реализующим криптографические механизмы информационной инфраструктуры значимой платежной системы, используемых при осуществлении переводов денежных средств по карточным счетам» в Центре защиты информации и специальной связи (8 Центр) ФСБ России и в АО «НСПК».

13.02.2026 Банк России опубликовал сведения об основных типах компьютерных атак в кредитно-финансовой сфере в 2025 году.

ОТРАСЛЕВЫЕ ДОКУМЕНТЫ

29.01.2026 приняты следующие стандарты:

- ГОСТ Р 58624.5.2–2026 «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 5.2. Расширенная классификация инструментов атаки на биометрическое предъявление. Модальность “лицо”»;
- ГОСТ Р 72502.4–2026 «Информационные технологии. Биометрия. Качество биометрического образца. Часть 4. Данные изображения отпечатка пальца»;
- ГОСТ Р 72510–2026 «Информационные технологии. Биометрия. Применение биометрии в мобильных устройствах»;
- ГОСТ Р 72511.5–2026 «Информационные технологии. Биометрия. Требования к формату обмена данными для испытательных стендов. Часть 5. Биометрическая система — биометрическая идентификация».

30.01.2026 был принят стандарт ГОСТ Р 72511.3–2026 «Информационные технологии. Биометрия. Требования к формату обмена данными для испытательных стендов. Часть 3. Подсистема обнаружения атаки на биометрическое предъявление».

ПРОДУКТ ЭВОЛЮЦИИ

СТРАТЕГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ МЕНЯЕТСЯ ВМЕСТЕ С БЫСТРЫМ РАЗВИТИЕМ ТЕХНОЛОГИЙ

Усам ОЗДЕМИРОВ
обозреватель BIS Journal

В настоящее время в России активно ведётся работа над новой Доктриной информационной безопасности, которая призвана заменить действующий документ 2016 года. Необходимость этого обновления вызвана значительными изменениями информационного ландшафта за последние восемь лет. Появление технологий GenAI, развитие квантовых вычислений, распространение интернета вещей (IoT) и формирование цифровых экосистем создали принципиально новые вызовы и угрозы.

В ходе январских экспертных диалогов о будущем мира замглавы администрации Президента РФ Максим Орешкин, говоря о фундаментальных изменениях в мировой экономике и глобальной архитектуре, выделил важный тренд: переход к «платформенной экономике» создаёт предпосылки для новой формы колонизации. Если страна не суверенна, если она не обладает собственными платформенными решениями, то она будет вынуждена идти на поклон к другим. «Это означает сильную зависимость: необходимость платить комиссионные расходы за использование платформы вовне, риск отключения платформы в случае несогласия между странами, невозможность влиять на её развитие»,— резюмировал Орешкин.

Из-за стремительного нарастания геополитической напряжённости и новых экзистенциальных вызовов задачи, связанные с внедрением и использованием отечественных средств защиты информации, критически важны для обеспечения суверенитета страны. Выступая на «Инфофоруме 2026», помощник секретаря Совета безопасности Дмитрий Грибков указал, что наши недруги стремятся сохранить доминирование, целенаправленно сдерживая развитие национальных информационных инфраструктур и вводя санкционные ограничения на технологии. При этом иностранные ИТ-продукты, от мобильных устройств до облачных сервисов и систем спутниковой связи, могут быть использованы в качестве инструментов давления.

На том же мероприятии Александр Шойтов, заместитель министра цифрового развития, связи и массовых коммуникаций РФ, президент Академии криптографии России, рассказал об инициативе под названием «Информационная безопасность — 2030», в рамках которой идёт анализ перспективных проблем и направлений. Среди них — информационная безопасность цифровых платформ, спутниковых систем, центров обработки данных, робототехники и беспилотных комплексов, защита в сетях связи стандартов 5G и 6G, вопросы больших данных, нейросетей и так далее.

По мнению А. Шойтова, ИБ-проблематика стала особенно острой, так как «мы живём в эпоху быстро меняющейся технологии». Он провёл параллель с серединой XX века, периодом бурного развития ядерных и космических технологий, и охарактеризовал сегодняшний этап как гонку за скорейшее внедрение инноваций ради экономического эффекта. Это отразилось и в эволюции терминов: от импортозамещения и импортонезависимости к технологическому суверенитету и лидерству.

Технологии и продукты западных ИТ-компаний, включая широко распространённые мобильные устройства, системы спутниковой связи типа Starlink, почтовые и облачные сервисы, используются как инструмент деструктивного воздействия на объекты КИИ и для ведения компьютерной разведки, считает Дмитрий Грибков. Сюда следует добавить антироссийские пропагандистские кампании, разведывательную деятельность в киберпространстве и масштабные компьютерные атаки на инфраструктуру. Отсюда вывод: Доктрина 2016 года, хотя и была прогрессивной для своего времени, уже не отвечает в полной мере современным реалиям, в которых информационная сфера стала основой функционирования практически всех отраслей экономики и ключевым полем геополитического противостояния.

ЗАРУБЕЖНЫЙ ОПЫТ

Аппарат Совбеза координирует работу над проектом новой редакции доктрины с привлечением государственных органов, научных и общественных организаций. По информации, появившейся в СМИ осенью прошлого года, состоялось совещание рабочей группы, рекомендовавшей направить проект на рассмотрение членам Межведомственной комиссии.

В то время как идёт обсуждение в экспертном сообществе, было бы нелишне бросить взгляд на зарубежный опыт в данной сфере.

Китайский подход к ИБ-сфере, сформулированный в «Законе о кибербезопасности» 2016 года (вступил в силу в июне 2017 года) и последующих стратегических документах, основывается на концепции «киберсуверенитета». Эта модель предполагает полный государственный контроль над информационной инфраструктурой, строгую цензуру контента, обязательное хранение дан-

ных граждан на территории Китая и приоритетное использование отечественных технологий. В Поднебесной действует Great Firewall of China (или «Золотой щит») — это масштабная система фильтрации интернет-трафика и цензуры, подкреплённая соответствующими законодательными актами и техническими средствами. Она обеспечивает мониторинг, блокировку нежелательных иностранных сайтов (Google, Facebook и др.), соцсетей и сервисов, а также «просеивание» контента для обеспечения информационной безопасности, создавая изолированный, контролируемый «национальный интранет». Особенностью китайской стратегии является её интеграция с промышленной политикой (национальный стратегический план КНР по развитию производственного сектора «Сделано в Китае 2025»): ИБ в ней рассматривается как необходимое условие для технологического лидерства. Китай делает акцент на развитии собственных стандартов, создании альтернативных глобальным технологических экосистем (Huawei, ZTE, Baidu) и подготовке кадров в сфере кибербеза.

Принятая в Соединённых Штатах «Национальная киберстратегия» (National Cybersecurity Strategy) фокусируется на непрерывном противодействии противникам в цифровом пространстве «на передовых позициях» (persistent engagement), упреждении и «коллективной обороне». Штаты делают акцент на защите критической инфраструктуры, противодействии преступности и шпионажу в киберсфере, а также на сохранении технологического лидерства через поддержку частного сектора. Особенностью американского подхода является тесное партнёрство государства с ИТ-гигантами (Microsoft, Google, Amazon), развитая система bug bounty программ и акцент на международных союзах (например, AUKUS) в части кибербеза. США также открыто декларируют готовность к наступательным кибероперациям, если кто-то «посмеет» ущемить их интересы.

Идеи властей Евросоюза в информационной сфере, заложенные в «Стратегии кибербезопасности ЕС на цифровое десятилетие» (ключевой документ Европейской комиссии в ИБ-сфере, принятый в 2020 году) и подкреплённые нормативными актами (NIS2, Cyber Resilience Act), основываются на принципах защиты фундаментальных прав, устойчивости цифровых систем и трансграничного сотрудничества. Особенностью европейского подхода является создание единого правового пространства (с распространением действия регламентов на все государства-члены), акцент на сертификации продуктов и стандартизации, а также развитие совместных возможностей реагирования на инциденты через агентство ENISA. ЕС также продвигает концепцию security by design, требующую встраивания защитных механизмов на этапе разработки технологий.

После Brexit Великобритания разработала собственную «Национальную киберстратегию — 2022», основанную на принципах «активной обороны» и «кибермощи» (cyber power). Британский подход сочетает усиление собственных наступательных и оборонительных возможностей (через Национальный киберцентр NCSC) с развитием инновационного сектора кибербеза. Особенностью является упор на прогнозирование угроз с использованием искусственного интеллекта (ИИ), развитие государственно-частного партнёрства и подготовку кадров через специализированные образовательные программы.

КОНТЕКСТ ОБНОВЛЕНИЯ РОССИЙСКОЙ ДОКТРИНЫ ИБ

Как видно из приведённых выше наблюдений, обновление национальной ИБ-стратегии в России продиктовано самим временем. Среди важных факторов можно указать технологический прорыв, связанный с революцией в области ИИ и обработки больших данных; перспективы развития квантовых технологий, биометрии; усиление киберугроз, которые стали более изощрёнными, целевыми и масштабными; цифровизацию экономики и общества; информационно-психологическое противостояние и нарастающее санкционное давление.

Налицо геополитическая трансформация, ведущая к поляризации цифрового мира на основе конкурирующих технологических экосистем, что требует чёткого определения целей и места России в этом мире.

В контексте динамично развивающихся технологий новая Доктрина должна не только декларировать защиту конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, но и создать надёжные технологические, правовые и организационные основы для обеспечения суверенитета Российской Федерации в информационном пространстве, включая разработку отечественных стандартов и технологий, исключение критических зависимостей от зарубежных решений, особенно в области базового программного обеспечения и аппаратных платформ.

С распространением технологий deepfake, генеративного ИИ и таргетированной дезинформации следует предусмотреть механизмы обнаружения, нейтрализации таких угроз. Документ должен стимулировать создание полного цикла разработки и производства безопасных ИТ-решений — от процессоров и операционных систем до прикладного софта, с акцентом на открытые отечественные стандарты. Нельзя будет пройти мимо вопросов подготовки кадров и формирования международной повестки в области ИБ. Россия стремится активно участвовать в формировании международных норм и правил поведения в информационном пространстве, продвигать инициативы по «цифровому разоружению» и противодействию киберпреступности.

Ключевой задачей является создание условий для технологического развития, безопасного внедрения инноваций и цифровизации экономики. Доктрина должна заложить основы для правового регулирования технологий, которые будут определять будущее искусственного интеллекта, интернета вещей, квантовых коммуникаций, биометрических систем, обеспечивая их безопасное и этичное использование.

Новая российская Доктрина ИБ, вероятно, будет сочетать элементы различных международных моделей с учётом национальных особенностей. Приоритетом будет развитие инфраструктуры, позволяющей обеспечить функционирование российского сегмента интернета в условиях внешних угроз. Ожидается усиление сотрудничества государства с отечественными ИТ-компаниями в области разработки безопасных решений (то, что принято называть государственно-частным партнёрством). Безопасность будет рассматриваться не как отдельная функция, а как неотъемлемое свойство всех цифровых систем на этапе их проектирования.

ДВИЖЕНИЕ К НОВОЙ ПАРАДИГМЕ ИБ

Из заявлений представителей власти можно сделать вывод, что целью обновлённой доктрины является укрепление суверенитета Российской Федерации в информационном пространстве, определяемого как способность государства создавать, развивать и защищать соответствующую инфраструктуру и ресурсы. В качестве одного из определяющих принципов здесь выдвигается неразрывность безопасности на всех этапах создания и эксплуатации ИТ-продуктов, что особенно важно в эпоху вездесущих нейросетей. Как подчеркнул Дмитрий Грибков, «если обеспечение информационной безопасности не заложено на стадии разработки и создания продукта, то в дальнейшем это будет сделать очень трудно или вообще невозможно».

Разработка новой Доктрины происходит в переломный момент, когда цифровые технологии становятся основой не только экономики, но и национальной безопасности в целом.

Российская модель, вероятно, будет эволюционировать в сторону более гибкой и технологически продвинутой системы, сочетающей элементы предупредительного контроля (по аналогии с китайской моделью) с развитием инноваций и компетенций (как в западных моделях). Ключевым вызовом станет создание такой экосистемы ИБ, которая была бы одновременно эффективной, технологически независимой и не препятствующей цифровому развитию страны.

В глобальном контексте новая российская Доктрина ИБ может стать одним из элементов формирования многополярной архитектуры цифрового мира. Это потребует не только внутренних преобразований, но и активной работы по формированию международных норм и правил, учитывающих интересы всех сторон.

Таким образом, обновление Доктрины информационной безопасности — это не только техническое обновление ранее принятого документа, но и переход к активным действиям, направленным на защиту интересов граждан Российской Федерации, обеспечение технологического суверенитета и достойного места страны в глобальном цифровом ландшафте на десятилетия вперёд.

КЛЮЧЕВЫЕ СТРУКТУРЫ

НАЦИОНАЛЬНЫЕ ЦЕНТРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МИРЕ, ВКЛЮЧАЯ НАПРАВЛЕНИЕ «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ»

Александр ПЕРШИН
Ассоциация руководителей служб информационной безопасности

В настоящее время в мире в ряде стран существуют структуры, отвечающие за обеспечение информационной безопасности (ИБ). Их обязанности, функции и полномочия варьируются от страны к стране. В одних случаях, как правило, относящихся к малым государствам, их функции ограничиваются координацией реагирования на компьютерные инциденты – своего рода национальные CERT. В других случаях это центры или агентства с широким набором функций и полномочий. В их числе реагирование на компьютерные инциденты, сертификация средств защиты, а также роль координационного центра между участниками электронного взаимодействия в части обеспечения ИБ.

Для примера ниже приведены обязанности, функции и полномочия нескольких подобных зарубежных структур.

ГЛАВА 1. СТРУКТУРЫ, ОТВЕЧАЮЩИЕ ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Франция. Национальное агентство безопасности информационных систем (Agence nationale de la sécurité des systèmes d'information, ANSSI) создано 7.07.2009. Оно является наследником длинной череды агентств, отвечающих за обеспечение безопасности конфиденциальной информации, в частности государственной[1], и находится в ведении Генерального секретаря по обороне и национальной безопасности, является национальным органом власти в области кибербезопасности и киберзащиты во Франции.

Роль ANSSI заключается в создании и организации на межведомственном уровне защиты нации от кибератак, а также в содействии стабильности киберпространства.

Деятельность ANSSI вписывается в рамки государственных задач, направленных на достижение общей цели государственной политики безопасности и устойчивости администраций, экономики и общества в целом.

Его действия сводятся к пяти основным миссиям: защищать, знать, делиться, сопровождать, регулировать:

1. **Защищать** критически важные информационные системы страны за счёт разработки и эксплуатации средств обнаружения кибератак, а также обеспечения доступности надёжных продуктов безопасности, способных защитить самые конфиденциальные данные и реагировать на самые высокие угрозы.
2. **Знать** современное состояние в области безопасности информационных технологий и систем; угрозы и риски в киберпространстве; тенденции в мире кибербезопасности во Франции, Европе и за рубежом.
3. **Делиться** рекомендациями, методами и инструментами для специалистов в области кибербезопасности и цифровых технологий; знаниями и ноу-хау об угрозе и возможных ответных мерах совместно с техническими, оперативными и стратегическими партнёрами, будь то французы, европейцы или страны за пределами Европы.
4. **Сопровождать** развёртывание государственной политики в области кибербезопасности и её территориальное подчинение, власти в своём понимании киберфакта, а также регулируемые организации в применении мер защиты своих информационных систем и их реагировании на инциденты. Сопровождать развитие экосистемы доверенных частных поставщиков продуктов и услуг.
5. **Регулировать** качество продуктов и услуг в области кибербезопасности посредством процедур ква-

[1] https://cyber.gouv.fr/en.

лификации и сертификации; качество продукции, содержащей цифровые элементы, путём обеспечения безопасности по дизайну и по умолчанию путём разработки нормативных механизмов на национальном, европейском и международном уровнях, а также контролировать их правильное выполнение.

Организационная структура и поддиректории:

1. Подразделение экспертизы выполняет общую миссию агентства по экспертизе и технической поддержке.

2. Операционное подразделение обеспечивает на оперативном и тактическом уровнях выполнение возложенной на ANSSI функции органа по защите цифровых систем, представляющих интерес для нации.

3. Поддиректория ресурсов отвечает за программирование и выполнение мероприятий по управлению финансовыми, человеческими, движимыми и недвижимыми ресурсами, а также за экспертизу и юридическое сопровождение. Она поддерживает деятельность агентства.

4. Подразделение по стратегии способствует разработке и реализации государственной политики в области цифровой безопасности, взаимодействует со всеми аудиториями ANSSI и развивает взаимодействие с сетью ключевых партнёров. Оно опирается на свои знания проблем кибербезопасности, а также на технический и операционный опыт других подотраслей.

5. Подразделение контроля и надзора объединяет надзорные функции, которые возложены на ANSSI в его роли компетентного органа в соответствии с европейскими и национальными правилами (в частности, стратегией жизненно важной деятельности).

Как национальный орган по киберзащите, сетевой и информационной безопасности (NIS), ANSSI является хранилищем навыков, которое делится своим опытом и оказывает жизненно важную помощь правительственным ведомствам и операторам.

Великобритания. **Национальный центр кибербезопасности Великобритании (National Cybersecurity Center, NCSC)** – организация правительства Великобритании, которая оказывает консультативную помощь и поддержку государственному и частному секторам в вопросах предотвращения угроз компьютерной безопасности. Организация была основана в Лондоне и начала функционировать в октябре 2016 г.[2]

«Национальный центр кибербезопасности служит связующим звеном между промышленностью и правительством, предоставляя консультации, рекомендации и поддержку в вопросах кибербезопасности, включая реагирование на инциденты в сфере кибербезопасности.

NCSC входит в состав Главного управления правительственной связи»[3].

В документе «Проспект Национального центра кибербезопасности»[4] объясняется концепция NCSC и то, как он намерен преобразовать сферу кибербезопасности в Великобритании:

«Перед Национальным центром кибербезопасности будут стоять четыре ключевые задачи:

1. Понять кибербезопасность окружающей среды, обмениваться знаниями и использовать этот опыт для выявления системных уязвимостей и устранения их. NCSC станет центром правительственной экспертизы того, что происходит в киберпространстве, объединяя знания, полученные в результате инцидентов и разведданных, с информацией, которой делятся благодаря тесным отношениям с промышленностью, научными кругами и международными партнёрами.

2. Снизить риски для Великобритании, работая с организациями государственного и частного секторов, необходимо улучшить свою кибербезопасность. NCSC окажет поддержку наиболее важным организациям в Великобритании из государственного и частного секторов в обеспечении безопасности их сетей.

3. Реагировать на инциденты кибербезопасности, чтобы уменьшить вред, который они наносят Соединённому Королевству. Мы признаём, что, несмотря на все наши усилия по снижению рисков и повышению безопасности, инциденты всё равно будут происходить. Когда происходит серьёзный киберинцидент, мы будем работать с жертвами, чтобы минимизировать ущерб, помочь с восстановлением и извлечь уроки для уменьшения вероятности повторения и минимизации будущих последствий.

4. Развивать наш национальный потенциал кибербезопасности и обеспечивать лидерство в важнейших вопросах национальной кибербезопасности. Кибербезопасность и информационные технологии продолжают развиваться быстрыми темпами. Как правительственный центр кибернетических знаний, NCSC будет иметь наилучшее понимание того, что происходит сегодня – с точки зрения угроз, уязвимостей и технологических тенденций...»

Национальный центр кибербезопасности обслуживает широкий круг организаций Великобритании по всему спектру вопросов кибербезопасности.

Следовательно, предоставляемые услуги будут многоуровневыми, отражающими различные угрозы, с которыми сталкиваются организации, а также навыки и ресурсы, которыми они располагают для их устранения. Владельцы сетей, систем и данных останутся ответственными за управление рисками для своих организаций; NCSC не будет представлять собой изменение этого принципа ответственности за риски.

[2] https://ru.wikipedia.org/wiki/Центр_национальной_компьютерной_безопасности_Великобритании.

[3] https://www.gov.uk/government/organisations/national-cyber-security-centre.

[4] https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus.

Мы определили четыре категории взаимодействия для описания объёма нашего предложения:

1. NCSC предоставит общие рекомендации и руководство.
2. NCSC будет управлять партнёрством по обмену информацией в области кибербезопасности.
3. Мы предлагаем, чтобы NCSC подготовил индивидуальные рекомендации для определённых секторов и активно работал с компаниями над этим.
4. NCSC также предоставит индивидуальную поддержку небольшому числу наиболее важных организаций Великобритании».

Вот пример «работы» NCSC[5]:

***«Профиль: ГРУ, операции по борьбе с киберугрозами и гибридными угрозами»**. Информационный бюллетень, в котором рассказывается о кибероперациях и информационных кампаниях Вооружённых сил Российской Федерации (ГРУ) против Великобритании и её союзников. В частности:*

«Траектории угроз и сценарии будущего.

Великобритания обеспокоена тем, что с 2014 г. ГРУ использует Украину в качестве испытательного полигона для разработки ряда кибервозможностей, интегрированных в его военную доктрину.

Дестабилизирующая деятельность России не соответствует её роли постоянного члена Совета Безопасности ООН (СБ ООН). Она также противоречит нормам ООН об ответственном поведении государств в киберпространстве, которые, как утверждает Россия, она соблюдает.

Геополитическая неопределённость, намерения и возможности России по нанесению ударов по союзникам по НАТО, а также опыт ведения боевых действий в Украине создают условия для перенаправления этих угроз. Крайне важно, чтобы Великобритания и наши союзники продолжали поддерживать Украину и готовились к возможному перенаправлению киберугроз и гибридных угроз со стороны ГРУ на европейских партнёров, союзников по НАТО и Соединённое Королевство сейчас и в будущем.

Совместно с союзниками по НАТО и Европейскому союзу Великобритания продолжит повышать осведомлённость о потенциальных сценариях угроз, которые ГРУ представляет для нас и наших союзников».

Германия. **Nationales Cyber-Abwehrzentrum.** Национальный центр киберзащиты (NCDC или Cyber-DC)[6] – это платформа сотрудничества, взаимодействия и координации федеральных агентств и других учреждений из различных министерств, занимающихся, в частности, вопросами, связанными с кибербезопасностью, имеющими общенациональное значение.

Центр киберзащиты был создан в 2011 г. как совместная межведомственная и институциональная платформа для улучшения и ускорения обмена информацией между участвующими ведомствами и учреждениями, а также для усиления координации защитных мер и контрмер в отношении инцидентов, связанных с информационной безопасностью в Германии. 1.09.2019 Центр киберзащиты претерпел значительные изменения.

Центр киберзащиты не является самостоятельным органом. Федеральное управление информационной безопасности является вышестоящей организацией Центра киберзащиты.

«Федеральное управление информационной безопасности (Bundesamt für Sicherheit in der Informationstechnik, BSI)[7] – это немецкое федеральное ведомство высшего уровня, основанное в 1991 г. и отвечающее за обеспечение компьютерной и коммуникационной безопасности для правительства Германии. В сферу его компетенции и ответственности входят безопасность компьютерных приложений, защита критически важной инфраструктуры, безопасность в интернете, криптография, противодействие прослушиванию, сертификация продуктов для обеспечения безопасности и аккредитация испытательных лабораторий по обеспечению безопасности...

Федеральное ведомство информационной безопасности Германии было основано в 1991 г. Его предшественником был криптографический отдел немецкой службы внешней разведки (BND)».

«Целью BSI[8] является превентивное содействие информационной и кибербезопасности для обеспечения безопасного использования информационно-коммуникационных технологий в обществе. BSI оказывает поддержку в обеспечении серьёзного отношения к проблеме ИТ-безопасности в правительстве, бизнесе и обществе и реализует её независимо.

Например, BSI разрабатывает ориентированные на практику минимальные стандарты и рекомендации для целевых групп по обеспечению безопасности в сфере информационных технологий и интернета, чтобы помочь пользователям избежать рисков.

Федеральное ведомство по информационной безопасности также отвечает за защиту федеральных ИТ-систем. Это касается защиты федеральных компьютеров и сетей от вирусов, троянских атак и других технических угроз.

Функции BSI также включают в себя:

- защиту сетей федерального правительства, включая обнаружение атак на правительственные сети и защиту от них;
- тестирование, сертификацию и аккредитацию ИТ-продуктов и услуг;
- предупреждение о вредоносном ПО или уязвимостях в ИТ-продуктах и услугах;

[5] https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations.

[6] https://en.wikipedia.org/wiki/Nationales_Cyber-Abwehrzentrum.

[7] https://en.wikipedia.org/wiki/Federal_Office_for_Information_Security.

[8] https://www.bsi.bund.de/EN/Home/home_node.html.

◆ консультации по ИТ-безопасности для федерального правительства и других целевых групп;

◆ предоставление информации и повышение осведомлённости граждан в вопросах ИТ-безопасности и интернет-безопасности;

◆ разработку единых и обязательных стандартов ИТ-безопасности;

◆ разработку криптографических систем для федеральных ИТ-систем».

США.

Агентство по кибербезопасности и защите инфраструктуры (Cybersecurity and Infrastructure Security Agency, CISA) – это автономное федеральное агентство США, подчиняющееся Министерству внутренней безопасности. Создано в соответствии с Законом о кибербезопасности и агентстве безопасности инфраструктуры в 2018 г. Роль агентства заключается в улучшении кибербезопасности государства на всех уровнях управления, координации программ кибербезопасности со штатами США и улучшении государственной защиты от частных и национальных хакеров[9].

Роль агентства – защита критической инфраструктуры США от киберугроз. Некоторые задачи:

◆ мониторинг и анализ угроз;

◆ разработка рекомендаций по защите;

◆ обеспечение технической и информационной поддержки для организаций в этой отрасли;

◆ координация программ кибербезопасности со штатами США;

◆ улучшение государственной защиты от частных и национальных хакеров.

CISA предоставляет поддержку бизнесу и организациям, пострадавшим от кибератак.

В октябре 2024 г. агентство представило свой первый Международный стратегический план на 2025–2026 гг., который определяет приоритетные направления в области международного сотрудничества для повышения безопасности и устойчивости критически важной инфраструктуры. Согласно этому плану среди основных задач агентства – укрепление устойчивости зарубежной инфраструктуры, усиление интегрированной киберзащиты и унификация международной деятельности CISA.

«В CISA стратегическое партнёрство имеет важное значение для повышения национальной безопасности и устойчивости. Мы используем информацию, полученную от промышленности, правительства всех уровней, некоммерческих организаций, академических кругов и исследовательских сообществ, чтобы опережать появляющиеся возможности и тенденции рынка»[10].

Агентство оборонных информационных систем США (Defense Information Systems Agency, DISA) – агентство боевой поддержки (combat support agency) Министерства обороны США (DoD). Отвечает за планирование, разработку и реализацию информационной инфраструктуры, систем и услуг для поддержки DoD и его компонентов. DISA состоит из военных, федеральных гражданских и подрядчиков.

«DISA – это агентство боевой поддержки, которое обеспечивает безопасность и эксплуатацию глобальной ИТ-инфраструктуры, поддерживающей связь между всеми вооружёнными силами США и Министерством обороны США. DISA работает по всему миру в режиме 24/7, предоставляя сетевые решения, которые поддерживают весь спектр деятельности Министерства обороны. В его задачи входит планирование, проектирование, приобретение, внедрение и поддержка информационных и коммуникационных систем, необходимых для национальной обороны.

Основная оперативная функция DISA – управление информационной сетью Министерства обороны (DODIN), глобальной магистралью для всех коммуникаций Министерства обороны. DODIN – это глобальная взаимосвязанная система электронных информационных ресурсов, включающая в себя вычислительные подсистемы, принадлежащие Министерству обороны и взятые в аренду. DISA отвечает за планирование, проектирование, эксплуатацию и техническое обслуживание этой обширной инфраструктуры, обеспечивающей военные операции и потребности министерства.

DISA играет ключевую роль в обеспечении кибербезопасности и защите информации, защищая DODIN во всех подразделениях Министерства обороны. Агентство проводит оборонительные операции в киберпространстве, защищая DISN и его сервисы от вторжений и неправомерного использования. Эта защита включает в себя непрерывный мониторинг, обнаружение угроз и реагирование на киберинциденты, затрагивающие военные системы и данные. DISA управляет программой Security Technical Implementation Guide (STIG), которая устанавливает стандарты конфигурации для защиты ИТ-систем, программного обеспечения и сетевых компонентов. Соблюдение требований STIGs является обязательным для любой системы, работающей в рамках DODIN, и обеспечивает стандартизированный уровень безопасности»[11].

Некоторые другие задачи DISA:

◆ **обеспечение безопасной и надёжной передачи данных** по глобальной сети военных: Агентство использует спутниковую связь, оптоволоконные кабели и другую инфраструктуру для передачи голоса, данных и видео;

[9] https://ru.wikipedia.org/wiki/Агентство_по_кибербезопасности_и_защите_инфраструктуры?ysclid=ml4yzsfq89689940640.

[10] https://www.cisa.gov/doing-business-cisa.

[11] https://legalclarity.org/defense-information-systems-agency-mission-and-operations/.

◆ **разработка и управление информационными технологиями:** например, DISA разрабатывает сеть Defense Information Systems Network (DISN) — основную сеть коммуникации Министерства обороны, систему Global Command and Control System (GCCS) — систему совместного командования и управления, которая обеспечивает ситуационную осведомлённость военным командирам. А также Joint Information Environment (JIE) — безопасную и совместимую среду обмена информацией для Министерства обороны — и управляет ими;

◆ **обеспечение кибербезопасности:** DISA предоставляет услуги по мониторингу сетей и обнаружению угроз, чтобы защитить сети и системы Министерства обороны от кибератак;

◆ **поддержка совместных и коалиционных операций:** Агентство обеспечивает бесперебойную коммуникацию и координацию между военными подразделениями;

◆ **консультирование высшего руководства Министерства обороны** в вопросах информационной политики и реализация утверждённой им стратегии;

◆ **надзорная деятельность** за проведением любых сетевых операций всех подразделений Министерства обороны, включая Объединённый комитет начальников штабов.

ГЛАВА 2. БЕЗОПАСНОСТЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Во время саммита по безопасности искусственного интеллекта (ИИ) в ноябре 2023 г. Великобритания и Соединённые Штаты Америки приняли решение о создании собственных институтов безопасности ИИ. В рамках саммита по ИИ в мае 2024 г. в Сеуле лидеры ряда стран договорились о создании сети институтов безопасности ИИ, в которую вошли учреждения из Великобритании, США, Японии, Франции, Германии, Италии, Сингапура, Южной Кореи, Австралии, Канады и Европейского союза12.

В КНР структура, регулирующая и контролирующая ИБ, создана в 2014 г. Впоследствии на неё были возложены функции по обеспечению ИБ в ИИ.

Китай. Администрация киберпространства Китая (Cyberspace Administration of China, CAC) — центральный орган регулирования интернета в Китае, который занимается регулированием кибербезопасности, в том числе в отношении ИИ.

CAC — основной регулятор, который публикует подзаконные нормативные акты, разрабатывает стандарты и контролирует соблюдение требований в сфере кибербезопасности.

CAC несёт полную ответственность за планирование и координацию регулирования в сфере кибербезопасности. Это самый активный регулятор с точки зрения выпуска нормативных документов в сфере кибербезопасности, а его правоприменительная деятельность сосредоточена на управлении «экологией интернета» и сетевым информационным наполнением.

Сфера регулирования CAC имеет экстерриториальный охват, то есть компании за пределами Китая, которые обрабатывают персональные данные китайских пользователей, могут подпадать под его юрисдикцию.

CAC находится под прямой юрисдикцией Центральной комиссии по делам киберпространства, партийного учреждения, подчинённого Центральному комитету Коммунистической партии Китая (КПК).

CAC — главный регулятор трёх основных законов Китая в сфере кибербезопасности:

1. **Закон о кибербезопасности (CSL)** — действует с 2017 г., регулирует безопасность сетей, локализацию данных для операторов критических информационных инфраструктур и базовые стандарты кибербезопасности.
2. **Закон о безопасности данных (DSL)** — принят в 2021 г., вводит классификации данных на основе рисков (например, «важные данные») и определяет, как такие данные должны храниться, передаваться и защищаться, особенно в трансграничных сценариях.
3. **Закон о защите персональных данных (PIPL)** — рамочный закон, который устанавливает основные принципы, цели, полномочия и ответственность в области защиты персональных данных.

В 2024 г. принят «Закон об искусственном интеллекте», который вступил в силу 1.07.2025. Некоторые положения закона:

◆ **классификация рисков систем ИИ** — все приложения делятся на четыре категории: «минимального», «ограниченного», «высокого» и «неприемлемого» риска. К высокой категории отнесены системы, используемые в критической инфраструктуре, правоприменении, судопроизводстве и для сканирования эмоций в реальном времени. Для них введены обязательные аудиты, стресс-тесты и сертификация;

◆ **суверенитет алгоритмов** — компании, работающие с данными китайских граждан в стратегических отраслях (финтех, логистика, здравоохранение), обязаны использовать алгоритмы, разработанные и зарегистрированные на территории КНР;

◆ **ответственность разработчика** — закон чётко устанавливает цепочку ответственности: от сборщика данных и тренера модели до конечного интегратора и оператора.

Стандарты. CAC и Национальный технический комитет по стандартизации информационной безопасности (TC260) разрабатывают стандарты в сфере кибербезопасности ИИ. Например:

◆ Руководство по реагированию на инциденты с генеративным ИИ — документ, который предлагает прозрачную матрицу для оценки угроз и описывает фазы реагирования: подготовку, мониторинг, устранение, анализ.

◆ Национальный стандарт Cybersecurity Technology — Safety Specifications for Generative Artificial Intelligence

[12] https://ru.ruwiki.ru/wiki/Институт_безопасности_ИИ?ysclid=mkzau1wyyb448067276.

Pre-Training and Fine-Tuning Data — документ, который определяет требования к безопасности данных для обучения и настройки генеративных моделей ИИ, а также описывает методы оценки. Окончательная версия стандарта выпущена в апреле 2025 г.

Контроль. CAC имеет полномочия по контролю за соблюдением требований в сфере кибербезопасности ИИ. Некоторые из них:

- проводит обзоры кибербезопасности и передачи данных;
- требует оценки безопасности для трансграничных потоков данных;
- заказывает исправление или приостановку цифровых сервисов;
- выпускает административные штрафы за нарушения законов.

В августе 2023 г. CAC запустил реестр генеративных моделей ИИ, подлежащих обязательной проверке. По данным на сентябрь 2025 г., CAC одобрил к публичному использованию более 140 моделей.

Исследования. Под эгидой CAC совместно с научными институтами и компаниями разработана рамочная программа по регулированию безопасности ИИ. Цель документа — создание общей основы для управления рисками, связанными с ИИ, а также содействие международному сотрудничеству в этой сфере. Некоторые особенности программы:

- **классификация рисков ИИ** — вводятся пять уровней: минимальный, ограниченный, значительный, серьёзный и критический, что позволяет более точно определить необходимость регулирования в каждом конкретном случае;
- **базовые принципы управления безопасностью ИИ** — интеграция и осмотрительность, гибкое управление на основе рисков, интеграция технологий и управления, открытость и сотрудничество, надёжное применение и предотвращение потери контроля;
- **обязательный непрерывный мониторинг новых рисков** — подчёркивается необходимость многостороннего и трансграничного сотрудничества в сфере безопасности ИИ.

В августе 2023 г. Китай ввёл обязательную регистрацию провайдеров генеративного ИИ и потребовал от публичных моделей получить официальную лицензию от CAC. Некоторые меры, которые CAC использует для контроля соблюдения законов об ИИ:

- **запуск реестра генеративных моделей:** провайдеры обязаны отчитываться о составе наборов данных и результатах «красных команд» — этических хакеров, которые тестируют безопасность алгоритмов;
- **требования к провайдерам сервисов ИИ:** они должны брать на себя ответственность за вопросы безопасности на протяжении всего жизненного цикла продукта и создавать системы для проверки алгоритмов, защиты данных и личной информации;
- **запрет на распространение определённого информационного наполнения:** в частности, запрещается создавать и распространять информационное наполнение (content), который угрожает национальной безопасности, наносит ущерб национальной чести или интересам, подрывает этническое единство и т.д.;
- **требования к информированию пользователей:** провайдеры должны сообщать пользователям, что они взаимодействуют с ИИ, а не с человеком, и предупреждать их о вреде чрезмерного использования;
- **оценка эмоций и уровня зависимости пользователей.** Если у пользователей обнаруживаются сильные эмоции или деструктивное поведение, провайдеры сервисов должны будут принять необходимые меры.

Национальная стратегия Китая в области ИИ[13]. Китайские усилия в области ИИ сместились с догоняющего развития внутри страны на установление правил за рубежом, объединив в единый стратегический механизм независимость в производстве чипов, государственный капитал и дипломатию «Цифрового шёлкового пути». Основные положения стратегии:

1. Китай создаёт суверенную, управляемую государством экосистему ИИ, чтобы к 2030 г. стать мировым лидером, сочетая долгосрочное планирование политики с целенаправленными инвестициями в базовые технологии, такие как чипы, вычислительные системы и языковые модели.
2. Стратегия объединяет централизованное управление с локальными экспериментами, вовлекая министерства, отраслевые альянсы и опытные участки на уровне городов для быстрого внедрения ИИ в различных отраслях и масштабного формирования нормативных требований.
3. При разработке ИИ в Китае особое внимание уделяется устойчивости, этическому контролю и национальному единству, внедрению ИИ в государственные службы, защите цепочек поставок от иностранной зависимости и обеспечению инклюзивного доступа при сохранении идеологической согласованности и общественного доверия.

В части ИБ Китай создал одну из самых всеобъемлющих в мире систем регулирования ИИ под руководством CAC, которая определяет допустимые способы использования ИИ до широкомасштабного внедрения. С 2022 г. правила CAC требуют регистрации алгоритмов, оценки безопасности и внедрения механизмов подотчётности для рекомендательных систем и генеративных моделей.

США. В мае 2024 г. под эгидой Национального института стандартов и технологий США (NIST)[14] был создан **Институт безопасности ИИ (Artificial Intelligence Safety Institute, AISI)**. Его основными задачами были развитие науки, практик и внедрение безопасности ИИ по всему спектру рисков, в том числе связанных с национальной и общественной безопасностью, а также правами личности.

[13] https://www.ginc.org/chinas-national-ai-strategy/.

[14] https://www.nist.gov/.

В июне 2025 г. название Института было изменено на Центр стандартов и инноваций в области искусственного интеллекта (Center for AI Standards and Innovation, CAISI)[15], а его миссия была преобразована.

Этот Центр станет основным контактным лицом для представителей отрасли в правительстве США. Он будет способствовать проведению испытаний и совместных исследований, связанных с использованием и защитой потенциала коммерческих систем искусственного интеллекта.

С этой целью CAISI будет:

- сотрудничать с организациями NIST в разработке руководящих принципов и передовых практик для измерения и повышения безопасности систем ИИ, а также сотрудничать с представителями NIST в оказании помощи отрасли в разработке добровольных стандартов;
- заключать добровольные соглашения с разработчиками ИИ и оценщиками из частного сектора и проводить несекретные оценки возможностей ИИ, которые могут представлять угрозу национальной безопасности; при проведении этих оценок CAISI сосредоточит внимание на очевидных рисках, таких как кибербезопасность, биозащита и химическое оружие;
- делать основные выводы и оценки возможностей систем ИИ США и их противников, внедрения иностранных систем ИИ и состояния международной конкуренции в сфере ИИ;
- делать основные выводы и оценки потенциальных уязвимостей в системе безопасности и вредоносного иностранного влияния, возникающего в результате использования систем ИИ противника, включая возможность создания «чёрных ходов» (backdoors) и других скрытых вредоносных действий;
- координировать действия с другими федеральными агентствами и организациями, включая Министерство обороны, Министерство энергетики, Министерство внутренней безопасности, Управление научно-технической политики и Разведывательное сообщество, для разработки методов оценки, а также для проведения оценок и экспертиз;
- представлять интересы США на международном уровне для защиты от обременительного и ненужного регулирования американских технологий иностранными правительствами и сотрудничать с сотрудниками NIST для обеспечения доминирования США в международных стандартах ИИ.

«Администрация Трампа меняет подход США к управлению ИИ, превращая институт, занимающийся вопросами безопасности, в центр стандартов и инноваций. Этот сдвиг представляет собой существенное изменение политики, в которой приоритет отдаётся коммерческому развитию и конкурентоспособности, а не регулированию, при этом учитываются соображения национальной безопасности. Этот шаг показывает, как разные администрации могут кардинально менять приоритеты технологической политики и отношения правительства с индустрией ИИ»[16].

«В новом названии отсутствует слово „безопасность“, чтобы подчеркнуть важность быстрого развития и более тесного сотрудничества с промышленными и международными партнёрами.

Центр стандартов и инноваций в области ИИ сохранит основные функции своего предшественника, включая оценку возможностей и уязвимостей систем ИИ и разработку добровольных стандартов безопасности[17]».

Федерального закона об ИИ в США нет. Регулирование ИИ строится на добровольных стандартах и инициативе штатов. При этом большое значение уделяется вопросам безопасности и прозрачности.

«Мозговым центром» развития и обеспечения безопасности ИИ является NIST. Он выпустил более 10 методичек и рекомендаций по данному направлению, глоссарий и ряд других документов. Кроме того, в этой работе принимают участие:

- некоммерческая организация MITRE, «мозговой центр», занимающийся исследованиями, разработкой рекомендаций и руководств в области высоких технологий, включая информационные технологии, ИИ и ИБ;
- Массачусетский институт технологий США, который в том числе ведёт базу данных таксономий рисков ИИ[18], содержащую более 1600 рисков, классифицированных по 65 категориям;
- а также ряд других организаций и институтов.

23.07.2025 Белый дом опубликовал официальный документ «Победа в гонке: план действий США в области ИИ»[19] (Winning the Race: America's AI Action Plan). План направлен на достижение глобального доминирования в сфере ИИ, установление мировых стандартов в области ИИ и получение экономических и военных преимуществ от наличия крупной экосистемы ИИ. Некоторые ключевые положения плана:

- **экспорт американского ИИ.** Министерство торговли и Госдеп США будут сотрудничать с частным сектором в организации поставок защищённых экспортных пакетов ИИ, включающих аппаратное обеспечение, модели, программное обеспечение, приложения и стандарты, друзьям и союзникам Америки по всему миру;
- **содействие быстрому строительству центров обработки данных:** ускорение и модернизация процесса выдачи разрешений для строительства центров обработки данных и заводов по производству полупроводниковых микросхем, а также создание национальных инициатив по увеличению числа лиц, владеющих востребованными профессиями;

[15] https://www.nist.gov/caisi.

[16] https://getcoai.com/news/u-s-ai-safety-institute-transforms-into-center-for-ai-standards-and-innovation-caisi/.

[17] https://particle.news/story/trump-administration-rebrands-ai-safety-institute-to-center-for-ai-standards-and-innovation.

[18] https://airisk.mit.edu/.

[19] https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

◆ **стимулирование инноваций и их внедрения:** отмена обременительных федеральных актов, препятствующих разработке и внедрению ИИ, а также привлечение частного сектора к выявлению правил, которые следует отменить;

◆ **поддержка свободы слова в передовых моделях:** обновление федеральных руководящих принципов в области закупок с целью обеспечения того, чтобы правительство заключало контракты только с разработчиками крупных передовых языковых моделей, гарантирующих, что их системы являются объективными и свободными от идеологической предвзятости на основе директив.

Европейский союз. Европейская служба по ИИ (European Artificial Intelligence Office) – это экспертный центр ЕС, который способствует разработке и внедрению решений на основе ИИ, приносящих пользу обществу и экономике.

Эта служба создана в рамках Европейской комиссии (ЕК) и является центром экспертизы по ИИ. Цель службы – содействовать разработке и внедрению решений на основе искусственного интеллекта, которые приносят пользу обществу и экономике.

Некоторые функции службы:

◆ мониторинг, надзор и обеспечение соблюдения требований Закона об искусственном интеллекте к моделям и системам в 27 государствах-членах ЕС;

◆ анализ возникающих непредвиденных системных рисков, связанных с разработкой и внедрением ИИ;

◆ разработка оценок возможностей, проведение оценок моделей и расследование случаев потенциального нарушения и несоблюдения требований.

В апреле 2025 г. ЕК представила план действий AI Continent по превращению сильных сторон ЕС, таких как уникальные кадры и развитые традиционные отрасли, в ускорители развития ИИ. В плане действий AI Continent объясняется, как использовать нераскрытый потенциал наших исследователей и отраслей. Он направлен на формирование следующего этапа развития ИИ, стимулирование экономического роста и повышение нашей конкурентоспособности в таких областях, как здравоохранение, автомобилестроение, наука и другие.

В дополнение к плану действий в октябре 2025 г. Европейская комиссия запустила стратегию применения ИИ, призванную повысить конкурентоспособность стратегических отраслей и укрепить технологический суверенитет ЕС. Стратегия направлена на стимулирование внедрения ИИ и инноваций по всей Европе, особенно среди малых и средних предприятий.

ЕС стремится к тому, чтобы ИИ был безопасным и заслуживающим доверия. С этой целью был принят Закон об ИИ – первая в мире всеобъемлющая нормативно-правовая база в области ИИ, гарантирующая здоровье, безопасность и основные права людей, а также обеспечивающая правовую определённость для бизнеса во всех 27 государствах – членах ЕС.

Закон об искусственном интеллекте (Регламент об искусственном интеллекте) – нормативный акт Европейского союза, принятый Европейским парламентом 13.03.2024 и одобренный Советом ЕС 21.05.2024.

Цель закона – создание общей нормативно-правовой базы для использования искусственного интеллекта, защита здоровья, безопасности и основных прав людей.

Некоторые положения закона:

◆ классификация систем ИИ. Продукты ИИ делятся на три категории: запрещённые системы (с недопустимой степенью риска), системы с высокой степенью риска и остальные системы ИИ;

◆ запрет на использование некоторых систем ИИ. Например, на применение манипулятивных или обманных методов, на использование уязвимостей людей, связанных с инвалидностью, возрастом или социально-экономической ситуацией;

◆ контроль за работой высокорисковых систем. Их должен постоянно контролировать человек, а информация о работе должна быть доступна пользователям; в ряде случаев владельцам таких систем необходимо пройти техническую сертификацию;

◆ требование прозрачности. Искусственно созданное или отредактированное информационное наполнение (аудио, изображения, видео) должно быть чётко обозначено как таковое;

◆ механизм юридической ответственности. Государства-члены обязаны установить конкретные санкции за нарушения норм закона, в том числе административные штрафы.

Закон охватывает все отрасли (кроме военной) и все виды ИИ.

Аналогичные службы также созданы в Японии, Южной Корее, Сингапуре, Канаде, Индии и ряде других стран. Однако в некоторых случаях они существуют чисто номинально.

ГЛАВА 3. О СИТУАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

В Российской Федерации орган (структура), выполняющий функции такого координационного центра, отсутствует. Есть регуляторы (ФСБ России, ФСТЭК России, Банк России для кредитно-финансовой сферы), есть надзорный орган (Роскомнадзор), а также идеолог и регулятор в сфере ИТ (Минцифры). А вот координационный центр, выполняющий функции интерфейса или переводчика между перечисленными государственными структурами, компаниями-разработчиками и компаниями-заказчиками решений и продуктов в области ИБ, включая направление ИИ, отсутствует. Между тем его создание более чем актуально. Безусловно, прямо копировать зарубежный опыт и подходы не стоит. Но проанализировать их, выделить подходящее к нашим условиям и специфике – можно и должно, особенно с учётом того факта, что в последние 2–3 года технологии

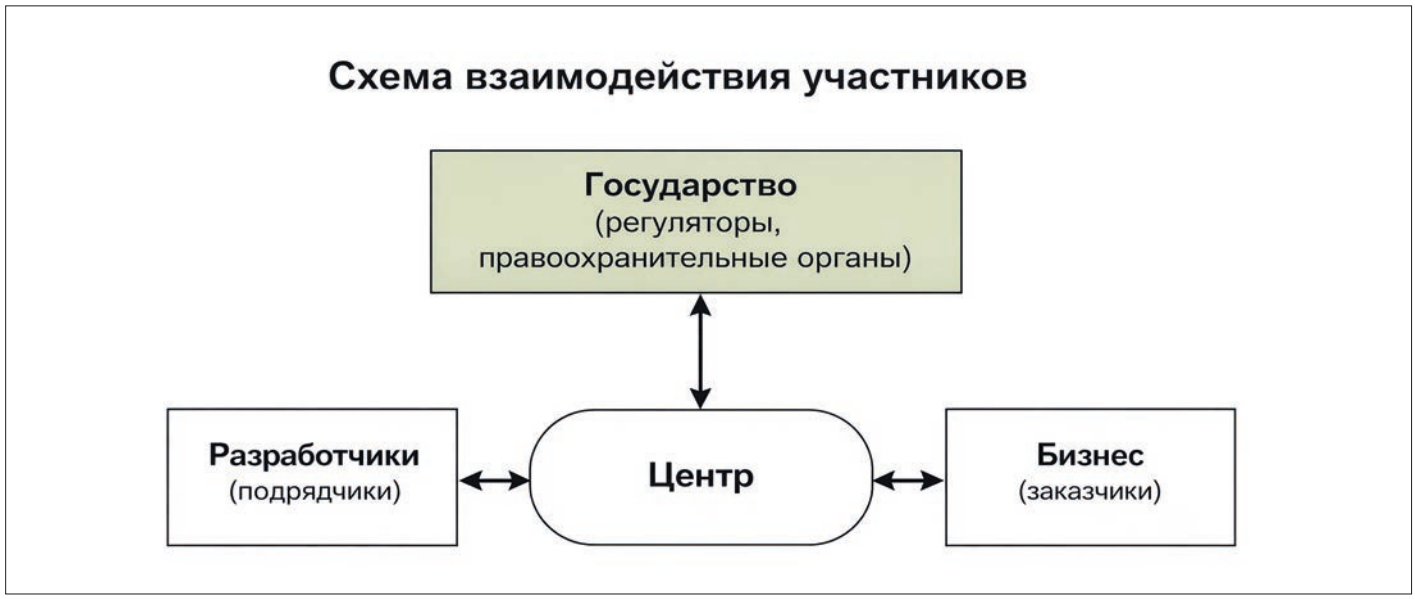


Рисунок 1. Упрощенная схема взаимодействия

ИИ развиваются настолько быстрыми темпами, что их поспешная или некорректная разработка, а также недостаточное тестирование могут привести к тому, что результаты их работы могут быть ошибочными или неожиданными.

Таким образом, представляется необходимым создание в России отдельного государственного органа (организации) с возложением на него следующих основных функций:

- разработка стандартов и правил объяснимого и интерпретируемого ИИ;
- обеспечение надёжности и безопасности ИИ (разработка требований и рекомендаций к ИИ и проведение соответствующих экспертиз);
- разработка методик и процедур практического применения ИИ;
- организация (консолидация) теоретических и прикладных исследований в области перспективного развития ИИ.

Упрощённая схема такого органа (организации или Центра) может выглядеть следующим образом (см. рис. 1).

Цели, задачи и функции Центра могут быть сформулированы детально.

КОГДА ВЕРСТАЛСЯ НОМЕР

Владимир Путин 26 февраля 2026 года подписал указ о создании Комиссии по развитию искусственного интеллекта (ИИ) при президенте России.

Комиссия займётся вопросами интеграции технологии в различные сферы: от социальной до экономической. Её возглавят вице-премьер Дмитрий Григоренко и замруководителя администрации президента Максим Орешкин. Также в комиссию среди прочих вошли министр обороны Андрей Белоусов, директор ФСБ Александр Бортников, губернатор Подмосковья Андрей Воробьёв, глава Сбербанка Герман Греф, помощник президента Алексей Дюмин, мэр Москвы Сергей Собянин, экс-руководитель «Яндекса» Тигран Худавердян, глава Минцифры Максут Шадаев.

Задачи Комиссии по развитию технологий ИИ. Комиссия образована в целях координации деятельности федеральных органов исполнительной власти, Центробанка, органов государственной власти субъектов Федерации, иных государственных органов и заинтересованных организаций по вопросам разработки согласованных подходов к формированию и реализации государственной политики в области создания, развития и внедрения технологий ИИ.

Комиссия займётся разработкой стратегических подходов к созданию, развитию и внедрению технологий ИИ с учётом необходимости повышения эффективности работы отраслей экономики, социальной сферы, сферы государственного управления и обеспечения национальной обороны и национальной безопасности; разработкой подходов, обеспечивающих адаптацию отраслей экономики, социальной сферы и сферы государственного управления к активному использованию технологий ИИ; разработкой мер, направленных на обеспечение технологического лидерства России в области создания, развития и внедрения технологий ИИ, включая создание и развитие российских больших фундаментальных моделей и передовых сервисов, использующих технологии ИИ, вычислительных мощностей и необходимой электронной компонентной базы, а также обеспечение этих мощностей электроэнергией.

КАК ОРГАНИЗОВАТЬ ЭФФЕКТИВНЫЙ ПРОЦЕСС БЕЗОПАСНОЙ РАЗРАБОТКИ С ПОДРЯДЧИКОМ

Александр ГАДАЙ
руководитель службы консалтинга Swordfish Security

IT-отрасль стремительно развивается, и, чтобы успеть за её темпами, частные компании и госсектор часто прибегают к услугам внешних подрядчиков для разработки программного обеспечения. Однако эта практика приводит к росту числа атак на инфраструктуру организаций через доступ, предоставляемый исполнителям, и к появлению уязвимостей в ПО. Вы можете заключить с контрагентом строгий NDA (соглашение о неразглашении информации) и понадеяться на его благонадёжность, но это не спасёт вас от рисков компрометации его системы или рабочих станций. С таким доступом злоумышленники способны проникнуть внутрь сетевого периметра вашей компании или подменить объект поставки: добавить закладку в исходный код или зависимый компонент ПО.

В этой статье мы рассмотрим вариант архитектуры процессов безопасной разработки ПО, который позволяет сохранять высокую скорость создания приложений без доступа подрядчика к инфраструктуре.

В первую очередь необходимо выделить несколько сетевых контуров в порядке повышения их значимости:

1. **Контур подрядчика** – внешний сегмент разработки в инфраструктуре компании-исполнителя.
2. **Контур вноса** – демилитаризованная зона (DMZ), в которую загружаются результаты работы подрядчика.
3. **Контур конвейера безопасной разработки** – изолированный контур, в котором находятся средства проверки защищённости цифрового продукта.
4. **Продуктивный контур** – изолированная зона, в которой размещаются релизные версии ПО.

Чтобы свести к минимуму риски компрометации, необходимо ограничить сетевой доступ между контурами на уровне правил межсетевого экранирования. Должна быть запрещена инициация сетевых соединений из менее безопасных контуров к более безопасным, то есть доставка ПО должна осуществляться в итерационной последовательности, не «перескакивая» через уровни (рис. 1):

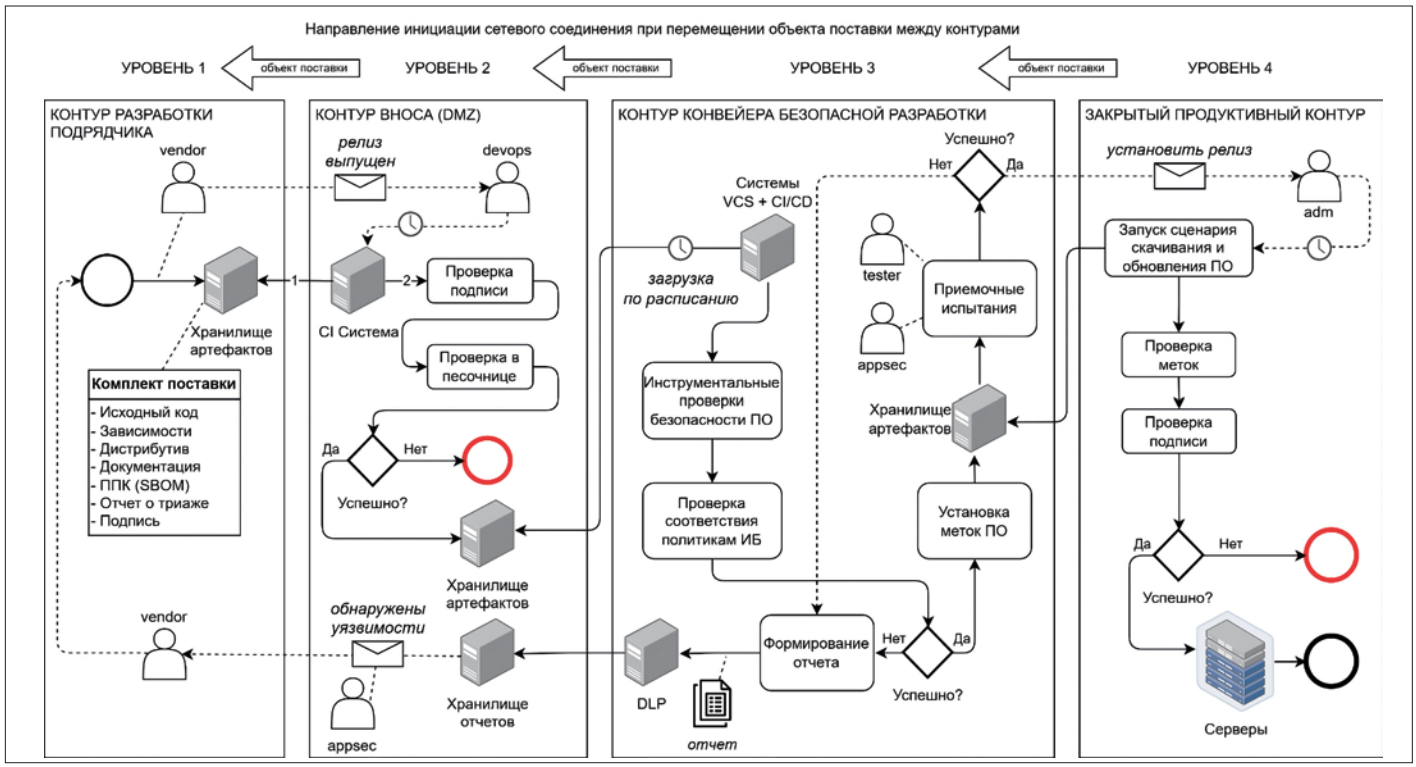


Рисунок 1. Должна быть запрещена инициация сетевых соединений из менее безопасных контуров к более безопасным, то есть доставка ПО должна осуществляться в итерационной последовательности

◆ на второй уровень через обращение к первому;

◆ на третий уровень через обращение ко второму;

◆ на четвертый уровень через обращение к третьему.

Рассмотрим ключевые этапы процесса доставки, начиная с момента готовности подрядчика провести отгрузку ПО. Представим, что объект поставки — это ZIP-архив, содержащий документацию, исходный код, зависимые компоненты приложения и собранный дистрибутив. С точки зрения процесса безопасной разработки, в него важно включить:

◆ ППК (перечень программных компонент) — специальный файл с описанием элементов поставляемого ПО, который позволяет на ранних этапах оценить безопасность зависимых компонент;

◆ Отчёт о триаже — размеченные результаты тестирования SAST, SCA, DAST и других ИБ-проверок;

◆ Цифровая подпись — файл подписи архива, который обеспечивает защиту от подмены при передаче.

Отдельно следует отметить практику предоставления отчёта о триаже в составе поставки. Наличие ложноположительных срабатываний в инструментах неизбежно, поэтому лучше сообщить о результатах вашего анализа уязвимостей до того, как они вернутся в виде замечаний от принимающей стороны. Это позволит значительно сократить время приёмки программного обеспечения и продемонстрирует ответственный подход подрядчика к безопасности собственного ПО.

Подрядчик уведомляет заказчика о готовности релиза, после чего специалист со стороны клиента **запускает процесс вноса дистрибутива** в контуре DMZ. В этот момент выполняется проверка подписи архива поставки и его отправка на сканирование решением класса «песочница» (sandbox). Если подпись верна и поведенческий анализ подтверждает чистоту архива, он перемещается в специальное файловое хранилище. В ином случае процесс завершается.

Рассмотрим контур конвейера безопасной разработки. Он включает следующие ключевые элементы:

◆ хранилище артефактов (например, Nexus Repository);

◆ система хранения кода, сборки и доставки ПО (например, GitLab);

◆ инструменты DevSecOps: анализаторы SAST, SCA, DAST и другие (подробнее об этих решениях можно прочитать в статье «Построение контура разработки безопасного ПО» в выпуске BIS Journal № 1 2025).

Процесс работы в контуре безопасной разработки начинается с получения объекта поставки из файлового хранилища в контуре DMZ. Это реализуется за счёт автоматической проверки наличия новых архивов в заданном каталоге, выполняемой по расписанию.

После этого запускаются проверки инструментами DevSecOps с целью подтверждения отсутствия недекларированных возможностей (НДВ) и вредоносных зависимостей. На данном этапе AppSec-инженер рассматривает отчёты о триаже подрядчика и переносит разметку о ложноположительных срабатываниях в проведённые сканирования. Если анализаторы подрядчика и заказчика совпадают, этот процесс можно автоматизировать, однако участие специалиста всё равно является обязательным для предотвращения случаев некорректной разметки.

По каждой из применяемых практик DevSecOps проводится оценка прохождения политик ИБ. Если они не пройдены, отчёт с обнаруженными уязвимостями возвращается в файловое хранилище контура вноса. Для предотвращения утечки конфиденциальной информации рекомендуется встроить в этот процесс DLP-систему. После исправления найденных уязвимостей цикл повторяется.

Когда проверки безопасности пройдены, артефакт подписывается и публикуется в хранилище, а также к нему добавляются специальные метки, например, SAST_SUCCESS. Доверие к этим меткам обеспечивается за счёт разграничения ролей в хранилище артефактов: установить метку может только специально выделенная техническая учётная запись, работающая в рамках пайплайна.

После того как мы убедились, что объект поставки проходит политики ИБ, проводятся приёмочные испытания. Они включают как функциональное, так и ручное тестирование безопасности с целью выявления, например, уязвимостей бизнес-логики ПО. В случае успеха направляется уведомление администратору по эксплуатации продуктивного контура о необходимости установки релиза.

Продуктивный контур содержит самые ценные активы: данные и серверные мощности, на которых исполняется ваше приложение. Процесс получения новых релизов должен инициироваться со стороны продуктивного контура следующим образом:

1. Администратор запускает сценарий обновления на новую версию ПО.
2. Скрипт обращается к хранилищу артефактов ПО, расположенному в контуре конвейера, для получения дистрибутива.
3. Перед загрузкой дистрибутива производится проверка скачиваемого артефакта на наличие меток об успешных ИБ-проверках. Если меток нет, процесс завершается.
4. После загрузки дистрибутива выполняется проверка его подписи. Если проверка не проходит, процедура прерывается.

Таким образом, в продуктивный контур попадают только те приложения, которые успешно прошли ИБ-сканирования и имеют корректную подпись.

* * *

Мы описали общий подход, который позволяет обеспечивать эффективное выполнение процессов безопасной разработки с внешним подрядчиком. Однако опыт реализованных нами проектов показывает, что в каждом случае нужно подстраиваться под имеющуюся инфраструктуру и организационные процессы компании, поэтому данный материал следует воспринимать как ориентир при проектировании архитектуры и процессов.

СОВРЕМЕННАЯ ЗАЩИТА ЦЕПОЧКИ ПОСТАВОК

И ПРИ ЧЁМ ЗДЕСЬ ХРАНИЛИЩЕ АРТЕФАКТОВ РАЗРАБОТКИ?

Дмитрий КЛЮЧНИКОВ
руководитель разработки продукта CodeScoring. Save

Когда команда, которая занимается безопасностью кода, начинает строить собственное хранилище артефактов, предсказуем вопрос: а зачем еще одно? Ведь на рынке уже есть Sonatype Nexus, JFrog Artifactory, Harbor, встроенные хранилища платформ разработки, а может быть и еще кто-то. На первый взгляд — выбор богатый. Но если копнуть глубже, становится понятно: выбор между хранилищами — это не выбор между наборами функций. Это выбор философии. И принципы безопасности занимают здесь не последнее место. Мы как разработчик хранилища артефактов хотим поделиться своим видением современного мира хранения компонентов (артефактов) программного обеспечения.

Современная разработка — это не только код. Это контейнерные образы, пакеты библиотек, Helm-чарты, ML и AI-модели, скомпилированные бинарные файлы. Всё, что возникает в результате сборки, тестирования и подготовки к развертыванию, принято называть артефактами. И у каждого из них должно быть место, где он хранится, версионируется, раздаётся потребителям и, к сожалению, пока только в идеале, проверяется на безопасность. Это место — **хранилище артефактов**, или менеджер репозиториев.

Долгое время выбор хранилища был вопросом сугубо инженерным: скорость работы, поддерживаемые форматы, удобство API, настройка проксирования внешних репозиториев. Но чем глубже артефакты проникают в цепочки поставки ПО, тем острее становится другой вопрос — вопрос безопасности. Масштаб хорошо иллюстрируют цифры: в 2025 году нашей командой было зарегистрировано 457 тыс. вредоносных библиотек, в 11 раз больше, чем годом ранее. Зафиксировано также 14 тыс. новых уязвимостей в открытых компонентах. При этом старые проблемы никуда не уходят, 15 тыс. пакетов экосистемы Java продолжают зависеть от уязвимой версии пресловутого log4j (уязвимость — Log4Shell). Логичным выглядит исследование Cloudsmith Artifact Management Survey 2025, которое показывает, что 56% инженерных команд уже считает главной задачей хранилища артефактов именно защиту цепочки поставки, а не удобство хранения.

Можно ли быть уверенным в том, что артефакт, который прямо сейчас разворачивается в продуктивной среде, не несёт в себе уязвимость, вредоносный код или нелицензионный компонент? На этот вопрос помогает ответить SBOM (Software Bill of Materials) — перечень компонентов программного обеспечения, который позволяет понять, из чего именно собран конкретный артефакт и отследить его цепочку зависимостей и «происхождение». Практики формирования SBOM закрепляются по всему миру, от зарубежных стандартов до ГОСТ Р 56939–2024 «Защита информации. Безопасная разработка. Общие требования». И именно этот сдвиг от вопроса «что хранить» к вопросу «чему доверять» сделал тему хранения артефактов по-настоящему актуальной для всех, кто занимается безопасностью разработки.

Если разложить существующие решения, получится не каталог технологий, а история эволюции идей. Каждое поколение хранилищ отвечало на вызовы своего времени — и каждое несло в себе компромиссы, ставшие очевидными лишь спустя годы.

КЛАССИКА ХРАНЕНИЯ АРТЕФАКТОВ

Sonatype Nexus и JFrog Artifactory — ветераны и де-факто стандарты. Именно они сформировали само понятие «универсального менеджера репозиториев»: поддержка десятков экосистем, многозадачные комбинации хранения данных, развитые механизмы репликации и масштабирования. Заслуженная зрелость и большая инсталляционная база. Для организаций, которым важна максимальная широта поддержки форматов и годами выстроенная экосистема интеграций и плагинов, эти решения по-прежнему остаются обоснованным выбором.

Но зрелость имеет обратную сторону. Обе системы — тяжёлые монолиты с высокими требованиями к ресурсам. Критичные для промышлен-

ной эксплуатации возможности — HA (высокая доступность), расширенное хранение, security-функционал — закрыты за дорогими лицензиями. Кластеризация превращается в отдельный инфраструктурный проект. Обновления болезненны: меняется схема БД, формат метаданных, модель плагинов. А вот уязвимости находятся часто, что создаёт неприятную вилку: обновляться — больно, не обновляться — страшно. Архитектурные решения, принятые пятнадцать лет назад, становятся не только устаревшими (легаси), но и ограничением для тех, кто хочет строить современные процессы.

ПРОСТЫЕ ХРАНИЛИЩА АРТЕФАКТОВ

Следующая волна решений взяла на флаг идею «чем проще — тем лучше». Harbor, проект CNCF, ограничился OCI-совместимыми артефактами и предложил разумный баланс между простотой и функциональностью: kube-native архитектура, интегрированные open source сканеры образов контейнеров, механизм проверки подписей. Для cloud-native команды, живущей контейнерами — то, что нужно. Harbor — отличный пример того, как фокус на конкретном формате позволяет довести пользовательский опыт до уровня, недоступного универсальным решениям.

Но если в стеке есть Maven, npm, PyPI или что-то ещё — нужно или второе хранилище, или набор упражнений для перестройки в формат OCI всех поступающих артефактов. На больших объемах неизбежно приходится бороться со сборкой мусора (garbage collection), а мажорные обновления требуют почти ручной миграции без волшебной кнопки «перенести». Это был справедливый компромисс для своего времени, но всё же компромисс.

ХРАНИЛИЩА АРТЕФАКТОВ НА ПЛАТФОРМАХ РАЗРАБОТКИ

Параллельно развивался другой подход: артефакты как бонус к платформе разработки. Встроенные хранилища GitLab, GitHub, Azure DevOps и ряда других платформ предложили единый пользовательский интерфейс (UI), общие права доступа, нативную (по умолчанию) интеграцию с CI — всё в одном месте. Главная сила подобных решений — околонулевая стоимость входа, ведь команда уже живет в этой экосистеме. На российском рынке, где потребность в быстром импортозамещении в какой-то момент стала критической, хостовые экосистемные решения упали в благодатную почву: они закрывали сразу множество задач одним инструментом. Хорошим примером можно назвать решения от GitFlic или Сфера.

Но платформенная привязка — палка о двух концах. Интеграция с внешними инструментами ограничена. Поддержка пакетных менеджеров часто реализована на уровне «минимально достаточного», с огрублениями протоколов. Data layer (уровень данных) привязан к самой платформе, масштабирование — только вместе со всем сервером, обновление реджистри отдельно невозможно. По сути, вы не выбираете хранилище — вы принимаете то, что даёт платформа.

НЕКАНОНИЧНЫЕ РЕАЛИЗАЦИИ

Наконец, есть категория решений, предлагающих принципиально иную логику. Проекты вроде Dragonfly (CNCF) переосмысляют саму модель распространения артефактов: P2P-дистрибуция образов поверх основного хранилища по аналогии с торрент-сетями. Ценностное предложение для бизнеса убедительно: радикальное снижение трафика, разгрузка центрального хранилища, эффективная раздача больших образов на сотни нод. Но это меняет всю экономику и модель доверия: образ приходит не из реджистри, а от «соседа» по кластеру, отладка запросов, гуляющих по пирам, нетривиальна, а порог входа для команды высок. Существуют и другие нишевые решения — Pulp для сценариев зеркалирования в изолированных средах, Zot Registry как минималистичное OCI-хранилище с фокусом на безопасность. Каждое точно решает свою задачу, но ни одно не претендует на универсальность.

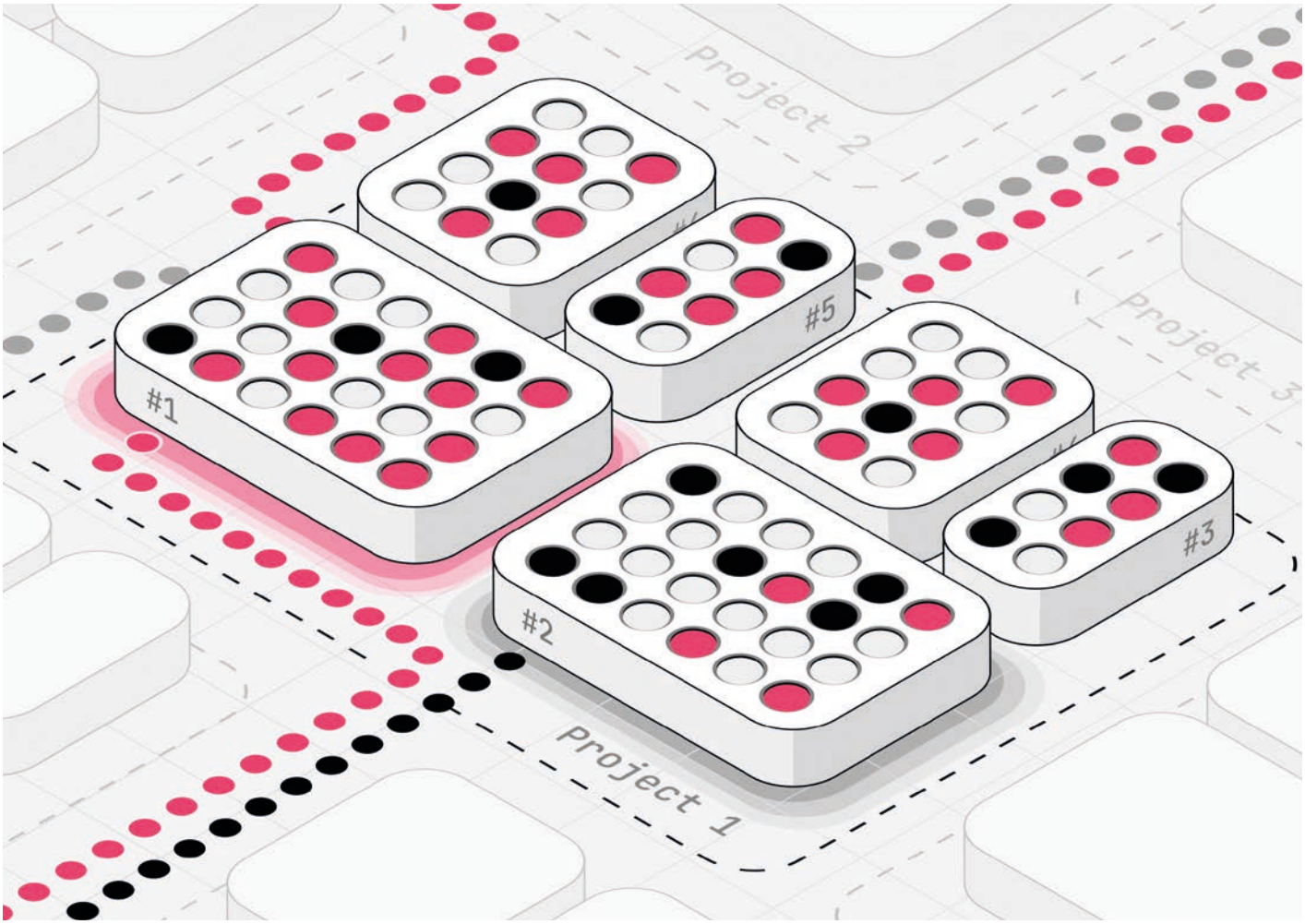
НАЗРЕВШАЯ ПОТРЕБНОСТЬ В ЭВОЛЮЦИИ ХРАНИЛИЩ АРТЕФАКТОВ

Мы выстроили эту классификацию не только из академического интереса. Она помогает увидеть не случайный набор конкурирующих инструментов, а эволюцию идей. Ключевой вывод не в том, что какое-то решение лучше или хуже: каждый класс хорош в своем контексте. Что-то для крупных инсталляций в устоявшихся компаниях с разношёрстным стеком, что-то для cloud-native команд, что-то для ценителей единой среды, а что-то для новаторов и задач, где, например, решение классической задачи транспортировки компонентов упрётся в потолок. Проблема не в инструментах и их выборе, а в том, что ландшафт изменился и появился контекст, для которого ни одно из имеющихся решений изначально не проектировалось.

Для компаний, которые занимаются безопасной разработкой, артефакт — это не просто бинарный файл, который нужно положить на полку и отдать по запросу. Это объект, у которого есть происхождение, зависимости, уязвимости, лицензионная история, SBOM. И хранилище должно это **учитывать нативно**, а не через внешние надстройки.

И вот мы подходим к тому, что стало для нас в CodeScoring отправной точкой. Главный вопрос к хранилищу артефактов сегодня — это давно не «можешь ли ты хранить контейнер или ML-модель?».

Главный вопрос звучит иначе: «можешь ли ты доказать, что этот артефакт безопасен?». Существующие решения отвечают на него по-разному. Nexus подключает отдельный IQ Server, JFrog — платформу XRay, Harbor — встроенные OSS-сканеры. Платформенные решения делегируют это внешним инструментам. Кто-то закрывает вопрос широко, кто-то точечно, но почти никто — оптимально. Безопасность в них «сбоку»: отдельный сервис, отдельная интеграция, отдельная лицензия. Хранилище и безопасность существуют параллельно, а не как единое целое. Говоря о современных реалиях, нельзя не упомянуть вектор угроз, напрямую



связанный с хранением артефактов. Исследование Техасского университета в Сан-Антонио (и нескольких участников из других американских университетов), в котором проводился анализ 576 000 фрагментов кода от 16 популярных LLM, показало, что в среднем около 20% рекомендуемых моделями пакетов не существует в реальных репозиториях. При этом 58% таких «выдуманных» пакетов стабильно воспроизводятся при повторных запросах. То есть это не случайный сбой, а устойчивый паттерн. Именно эта устойчивость открывает дорогу для slopsquatting-атак: злоумышленник заранее регистрирует пакет с именем, которое LLM будет рекомендовать снова и снова, превращая галлюцинацию в точку входа.

Именно этот контекст определил архитектурные решения, которые мы заложили в наше хранилище артефактов CodeScoring.Save. Не как попытку построить лучшую замену всему, а как набор требований сегодняшнего российского рынка.

Современный технологический стек и инженерные практики диктуют вполне конкретные ожидания к, в первую очередь, инфраструктурному ПО: контейнерная среда, горизонтальное масштабирование, разделение compute и storage, API-first подход к управлению. В современных хранилищах артефактов есть вещи, которые нужны на этапе проектирования, например: разработка на Go, kube-native архитектура с HA доступна сразу, модульная SOA-структура, отделяемые компоненты хранения, с реляционной базой данных и S3-хранилищем. Это не уникальные фичи, это отражение того, как строится инфраструктурное ПО сегодня, когда ему не нужно тащить на себе пятнадцатилетнее легаси. Поддержка популярных пакетных менеджеров, улучшенные возможности контроля и аудита — следствие того, что продукт пишется командой, для которой безопасная разработка — не надстройка, а исходная точка.

Отдельно стоит сказать о локальной специфике. Ни одно из существующих зарубежных решений не учитывает требования российских стандартов безопасной разработки — в частности, ГОСТ Р 56939–2024 и связанных с ним практик РБПО. Для команд, которым важно соответствие этим требованиям, возможности зарубежных хранилищ заканчиваются там, где начинается отечественная нормативная база.

Важно подчеркнуть: все предыдущие решения не «плохие». Каждое из них решало задачи своего времени, и многие продолжают успешно это делать по сей день. Но ландшафт изменился. Артефакт перестал быть просто файлом, а хранилище — просто полкой. И мы считаем, что пришло время для продукта, который проектировался именно для этой реальности, а не адаптировался к ней.

ТРИАЖ СЕКРЕТОВ

С ПРИМЕНЕНИЕМ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ В ПРОЦЕССАХ РБПО ПО ГОСТ Р 56939-2024

Александр ДЕМИДОВИЧ
ведущий эксперт Центра оценки соответствия и тестирования АО «НПО «Эшелон»

Утечки чувствительных данных остаются одной из наиболее опасных проблем современной разработки ПО, что подчёркивается включением отдельного процесса по выявлению и управлению секретами ГОСТ Р 56939–2024 (п. 5.15 «Обеспечение безопасности используемых секретов»). По мере роста числа интеграций, использования облачных сервисов и автоматизированных конвейеров секреты всё чаще появляются в исходном коде, конфигурационных файлах, сценариях сборки, логах и артефактах процессов непрерывной интеграции и непрерывного развёртывания (CI/CD). Основная проблема кроется в том, что секрет, единожды попав в систему управления версиями, навсегда там остается, в чем можно убедиться, просканировав историю изменений и обнаружив секреты даже из удаленных файлов. Именно поэтому такие утечки часто становятся входными точками для атак. Получив действующий токен или ключ, злоумышленник может обойти часть защитных механизмов, получить доступ к внутренним сервисам, облачной инфраструктуре, базам данных или сторонним API. В отличие от многих других уязвимостей, здесь не требуется сложная эксплуатация, поскольку сам факт раскрытия секрета уже создаёт условия для компрометации.

ПОИСК СЕКРЕТОВ И ОГРАНИЧЕНИЯ КЛАССИЧЕСКИХ СКАНЕРОВ

Для поиска секретов используются инструменты, основанные на поиске по шаблонам, регулярным выражениям. Подобный поиск присутствует и в статических анализаторах кода, которые могут выявлять жестко заданные значения. К числу распространённых решений по поиску секретов относятся такие инструменты как Gitleaks, TruffleHog, Detect-Secrets, GitGuardian, AWS git-secrets, Talisman, SpectralOps, а также встроенные механизмы GitHub Advanced Security.

Однако стандартные сканеры секретов почти не учитывают контекст использования найденной строки. Они хорошо выявляют подозрительные последовательности символов, но нередко помечают как секреты тестовые значения или случайные идентификаторы, не являющиеся секретами. Например, библиотека с открытым исходным кодом Gitleaks берёт за основу шаблоны и анализирует прежде всего внешний вид строки, а не её роль в программе или окружение, в котором она используется. В результате такой тривиальный поиск идентифицирует в качестве секретов случайный численно-буквенный набор символов или тестовые значения. Необходимость ручной разметки результатов, которые заведомо содержат большое количество ложноположительных срабатываний, значительно замедляет процессы разработки ПО.

ПРАКТИЧЕСКАЯ ОСОБЕННОСТЬ ТРИАЖА

Разметка и приоритизация результатов сканирования — это ключевой этап работы с секретами. Когда утилита находит десятки или сотни потенциальных секретов, необходимо понять, какие из них являются реальными секретами, а какие представляют собой ложные срабатывания. В контексте практик разработки безопасного ПО (РБПО) задача разметки результатов особенно важна, поскольку связанная с временными и ресурсными трудозатратами команды разработки. Поэтому после первичного поиска требуется дополнительная классификация результатов по степени риска, типу секрета, его актуальности и потенциальным последствиям компрометации. На практике при такой оценке учитываются не только формат найденного значения, но и его жизненный цикл, уровень привилегий, место обнаружения и связь с производственной средой. Например, истёкший тестовый ключ и активный привилегированный токен от продуктивного сервиса формально относятся к одному классу находок, но их реальная опасность принципиально различается.

ПРИМЕНЕНИЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ (LLM) ДЛЯ КОНТЕКСТНОЙ КЛАССИФИКАЦИИ СЕКРЕТОВ

На этом этапе особенно полезны большие языковые модели, способные анализировать не только саму строку, но и окружающий её контекст. В отличие от классических механизмов LLM позволяют перейти от вопроса «Похоже ли это на секрет?» к вопросу «Может ли найденное значение представлять угрозу, к какому типу секрета оно относится и как срочно необходимо отреагировать?» Такой подход даёт возможность использовать модель как слой интеллектуальной разметки поверх классических детекторов.

Алгоритм работы выглядит следующим образом: сканер первично формирует набор потенциальных секретов с сопутствующими метаданными, после чего результаты поступают в модуль LLM, где выполняется классификация. На практике в модель передаётся не только сама найденная строка, но и окружающий её контекст: фрагмент кода, имена пе-

Рисунок 1. Схема конвейера

ременных, путь к файлу и прочие метаданные. На этой основе система определяет, является ли найденное значение секретом, к какой категории оно может быть отнесено и какой уровень риска следует ему присвоить. В результате LLM используется не только как средство дополнительной проверки, но и как инструмент разметки, в которой решающую роль играют контекст, расположение файла, история изменений и признаки связи с продуктивной средой.

Архитектура системы разметки и приоритизации секретов на основе LLM представляет собой многоэтапный конвейер (рис. 1).

В модуле классификации каждая находка обрабатывается как отдельный объект анализа. Перед передачей данных в модель выполняется сокрытие содержимого секрета, что позволяет снизить риск утечки чувствительной информации при обращении к модели. После этого формируется фрагмент окружающего кода, имя файла, сведения о ветке, коммите и иные признаки контекста (рис. 2). На основе этих данных модели ставится задача определить, является ли найденное значение реальным секретом, к какому типу оно относится, каков уровень риска его компрометации и какие действия являются предпочтительными. Результат такой обработки может быть направлен либо в специализированный интерфейс анализа, либо непосредственно в систему управления инцидентами, средства мониторинга безопасности или корпоративную систему постановки задач. При этом аналитик получает не только итоговую категорию и уровень риска, но и краткое пояснение, позволяющее понять логику классификации.

```
{
  "secret_id": "finding-00125",
  "repository": "payments-service",
  "branch": "main",
  "commit": "a7f3c91",
  "file_path": "src/config/auth.js",
  "line_start": 42,
  "line_end": 42,
  "detector": "gitleaks",
  "secret_type_candidate": "aws_access_key",
  "masked_value": "AKIA*******7H2Q",
  "code_fragment": "const accessKey = \"AKIA*******7H2Q\";",
  "author": "ivan.petrov",
  "commit_date": "2026-03-20T10:14:00Z",
  "environment_candidate": "production",
  "is_public_repo": true,
  "days_exposed": 8,
  "context_tags": [
    "cloud",
    "credentials",
    "production-config"
  ]
}
```

Рисунок 2. Контекст найденного секрета

АВТОМАТИЗИРОВАННОЕ РЕАГИРОВАНИЕ И СВЯЗЬ С ПРОЦЕССАМИ РБПО

Следующим уровнем зрелости является автоматизация ответных действий. Если система обладает достаточной уверенностью в том, что обнаруженное значение представляет собой актуальный секрет, возможно автома-

тическое уведомление ответственных разработчиков ПО, запись инцидента в баг-трекер, открытие задачи на устранение или инициирование процедуры отзыва и замены ключа через систему управления секретами. Одновременно с этим должны сохраняться все необходимые артефакты, фиксирующие, какой найденный секрет был обработан, когда это произошло и каким компонентом системы было принято соответствующее решение. Практически эффективной может оказаться комбинированная схема, в которой один инструмент используется для быстрого локального контроля перед коммитом, а более глубокий анализ выполняется в централизованном режиме в процессе непрерывной интеграции с привлечением LLM-классификатора.

При этом не стоит забывать, что применение LLM в задачах обработки секретов требует соблюдения дополнительных мер защиты. Передача чувствительных данных во внешние модели без специальной защитной прослойки недопустима. Реальные ключи и токены должны удаляться из входных данных или заменяться нейтральными обозначениями ещё до обращения к модели. Во многих случаях политика безопасности организации может требовать, чтобы языковая модель разворачивалась исключительно во внутреннем контуре компании либо на изолированном вычислительном узле, а журналы запросов шифровались, ограничивались по сроку хранения и очищались после завершения анализа. Более безопасным считается подход, при котором модели передаются не сами секреты, а только их признаки и контекстные характеристики, например тип токена, уровень привилегий, место обнаружения и связь с производственной средой. При этом фактические значения секретов должны храниться и использоваться только в специализированном защищённом хранилище во время исполнения, не попадая в текстовые запросы к модели. Такой подход снижает вероятность как утечки данных, так и их непреднамеренного воспроизведения моделью.

ЗАКЛЮЧЕНИЕ

В итоге данный подход целесообразно рассматривать как часть системы контролируемых проверок и реагирования в жизненном цикле ПО. При корректной интеграции в процессы РБПО LLM-классификатор может повысить качество анализа результатов сканирования и сократить объём ручной работы. Однако важно отметить, что окончательное решение должен принимать ответственный специалист, поскольку часть результатов неизбежно будет относиться к неоднозначным и требующим дополнительной проверки. Именно поэтому на практике наибольшую устойчивость демонстрирует подход с участием человека в контуре принятия решений, при котором модель ускоряет обработку и снижает нагрузку на экспертов, но не исключает профессиональной верификации там, где цена ошибки особенно высока.

ПРИНЦИП GIGO

ЗАЧЕМ СОВРЕМЕННОЙ РАЗРАБОТКЕ ТОЧНЫЙ SAST

Антон МИХАЙЛОВ
владелец группы продуктов SASTAV

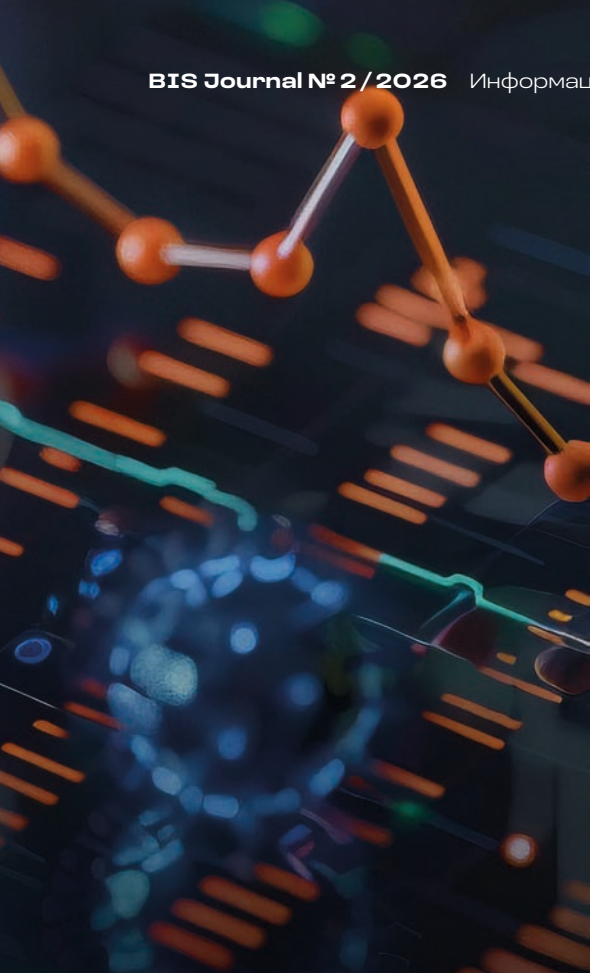
Дмитрий ПОЛИВАНОВ
архитектор отдела технических решений АО «ДиалогНаука»

Внедрение комплексных платформ управления безопасностью приложений (Application Security Posture Management, ASPM) набирает обороты: бизнесу нужна единая, управляемая картина рисков по всем продуктам и командам. Но любая платформа управления стоит ровно столько, сколько стоит качество данных на входе. Принцип Garbage In, Garbage Out (GIGO, «мусор на входе — мусор на выходе») здесь работает буквально: некорректные или «зашумлённые» результаты от инструментов анализа обесценивают даже сильную оркестрацию, корреляцию и отчётность. Поэтому статический анализ безопасности приложений (SAST) — не просто ещё один источник событий, а фундамент всей экосистемы AppSec.

СИСТЕМНЫЙ КРИЗИС ЛОЖНЫХ СРАБАТЫВАНИЙ: ПОЧЕМУ ТОЧНОСТЬ SAST ОПРЕДЕЛЯЕТ УСПЕХ DEVSECOPS

Исторически главный недостаток многих SAST-инструментов, особенно тех, что построены исключительно на сигнатурном анализе,— высокий процент ложных срабатываний (false positives). Это проблема не только операционная, но и экономическая: специалисты по безопасности и разработчики тратят существенную долю времени на верификацию предупреждений, что замедляет итерации и увеличивает стоимость владения процессом. В DevSecOps, где безопасность должна работать в такт быстрой поставке, такой объём ручной работы становится неприемлемым. Плюс постоянный шум приводит к «усталости от предупреждений» — и уже на этапе разбора результатов растёт риск пропустить настоящие угрозы из-за снижения внимания и приоритизации, а сам инструмент в лучшем случае начинают использовать формально, сводя на нет ценность всего пайплайна анализа.

В интегрированных цепочках, когда результаты SAST автоматически уходят в системы оркестрации и корреляции (ASOC) или в платформы стратегического управления (ASPM), эффект шума лавинообразно масштабируется. Если первичные данные низкого качества, то ломается приоритизация, искажаются метрики безопасности и в итоге ресурсы расходуются не на те задачи. По сути, неточные результаты SAST создают иллюзию контроля: платформы управления показывают красивые дашборды, но реальные риски остаются за кадром, маскируясь под шум или теряясь в потоке ложных срабатываний. Поэтому точность и надёжность SAST — это уже не внутренняя «техническая метрика», а параметр



управления рисками, который напрямую влияет на окупаемость инвестиций в безопасность.

SASTAV: АРХИТЕКТУРА, ОРИЕНТИРОВАННАЯ НА ДАННЫЕ ВЫСОКОГО КАЧЕСТВА

Решение SASTAV изначально проектировалось так, чтобы держать баланс между полнотой обнаружения (recall) и точностью (precision, доля истинных срабатываний). Архитектура и функциональность нацелены на то, чтобы данные, которые затем попадут в процессы первичной оценки инцидента (триаж) и в управленческие системы, были максимально надёжными и объяснимыми.

В основе подхода — комбинация оптимизированного статического анализатора и многоэтапной валидации результатов с применением ИИ. После первичного сканирования потенциальные уязвимости проходят каскад специализированных моделей. Ключевой момент — контекстный анализ без передачи в модель полного исходного кода, что важно для соблюдения требований конфиденциальности и внутренних политик работы с интеллектуальной собственностью. Вместо этого формируется набор запросов (промптов), включающий только релевантные фрагменты, информацию о потоках данных и метаданные. В результате система помогает отделить реальные проблемы от шума и даёт разработчику понятное объяснение. По результатам пилотных внедрений и контрольных выборок это позволяет сократить объём ложных срабатываний на десятки процентов, в отдельных сценариях — более чем на 80%, без ухудшения полноты на проверяемых наборах.

Дополнительно на качество результатов сильно влияет создание и отладка собственных правил, которые учитывают специфику кодовой базы: внутренние безопасные обёртки, соглашения, архитектурные паттерны. В SASTAV есть встроенный редактор правил с интерфейсом, близким к IDE: можно создавать, отлаживать и тестировать правила, опираясь на внутренние фреймворки и бизнес-логику, а не только на универсальные шаблоны. Поддержка широкого спектра языков (Java, C#, Python, Go, JavaScript, TypeScript, C++) и актуальных фреймворков помогает покрывать разнородный технологический стек.

Точность — не единственный параметр, по которому стоит оценивать SAST. Для встраивания в быстрые CI/CD-конвейеры критична скорость и предсказуемость анализа. Архитектура SASTAV поддерживает параллельное выполнение нескольких движков сканирования и рассчитана на контейнерные развёртывания (включая Kubernetes). Это даёт отказоустойчивость, горизонтальную масштабируемость и стабильное время анализа даже для крупных монолитов, снижая риск «узких мест» в поставке.

SASTAV поддерживает подход Shift Left Security («сдвиг влево»), интегрируясь с системами контроля версий (GitLab, GitHub, Bitbucket), CI/CD (Jenkins, GitLab CI, GitHub Actions, Azure DevOps), трекерами задач (Jira, YouTrack) и IDE. Развитый REST API позволяет встраивать проверки в существующие автоматизированные процессы и подключать результаты к платформам ASPM. Отдельно сделан акцент на миграционный сценарий: есть механизмы импорта и конвертации данных триажа из других SAST-решений, чтобы сохранить инвестиции в уже проделанную работу и снизить порог перехода.

Платформа поддерживает детальное разграничение прав доступа (RBAC) для больших команд, панели мониторинга и визуализацию потоков данных, чтобы разработчик видел контекст уязвимости. Практический эффект — можно быстрее разбирать результаты и устранять дефекты, а не спорить о том, «насколько это похоже на проблему».

SAST КАК СТРАТЕГИЧЕСКИЙ АКТИВ В АРХИТЕКТУРЕ APPSEC

Эволюция Application Security логично ведёт к централизации управления через платформы ASPM. Но их ценность определяется не количеством виджетов в интерфейсе, а достоверностью и воспроизводимостью данных, которые на них опираются. Инструменты вроде SASTAV, которые закрывают фундаментальную проблему качества первичных данных, становятся не просто сканерами, а частью управляемой архитектуры AppSec.

Их роль — обеспечить переход от реакции на шум к управлению реальными рисками. Для специалистов по безопасности это означает возможность сосредоточиться на стратегических задачах — архитектурном анализе, развитии практик безопасной разработки и поиске действительно сложных уязвимостей, требующих человеческого опыта, вместо бесконечной верификации ложных срабатываний. Разработчики же перестают отвлекаться на шумные уведомления и возвращаются к своей прямой задаче — созданию и поставке продукта. Кроме того, инвестиции в точный, быстрый и интегрируемый SAST — это инвестиции в качество всей цепочки: от коммита разработчика до отчёта для руководства. Если на входе чистые и объяснимые результаты, дальше можно масштабировать оркестрацию, метрики и автоматизацию без самообмана — и действительно ускорять разработку, не теряя безопасность.

ГОССОПКА И ЛЮДИ

ПОЧЕМУ ЦИФРОВОЙ ЩИТ НЕ СПАСЁТ ОТ ЧЕЛОВЕЧЕСКОЙ ОШИБКИ

Андрей ЖАРКЕВИЧ
эксперт Start X, ведущий рубрики

Любую систему национальной кибербезопасности принято описывать метафорой щита. Сенсоры, центры мониторинга, каналы обмена данными, регламенты реагирования образуют стену между страной и атакующими. ГосСОПКА в этом контексте выглядит как крепость: внутри безопасно, снаружи опасно, задача — укреплять стены.

Метафора красивая, но неточная. ГосСОПКА не стена. Это нервная система. Она не блокирует атаки сама по себе. Она собирает сигналы от тысяч организаций, синтезирует картину угроз и рассылает обратную связь. Её ценность не в толщине брони, а в скорости и точности передачи боли.

Но нервная система работает, только когда нервные волокна действительно передают сигнал. Не глушат его, не приукрашивают, не задерживают на неопределённый срок «до окончания согласований». Именно здесь начинаются проблемы, и они не в технологиях.

ЧТО ТРЕБУЕТ ГОССОПКА ОТ ЛЮДЕЙ

Формально ГосСОПКА — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак. Она агрегирует информацию от субъектов критической информационной инфраструктуры, формирует общую картину угроз, координирует реагирование через Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

Давайте переведём это с бюрократического на человеческий. ГосСОПКА требует, чтобы тысячи организаций по всей стране делали нечто глубоко противоестественное: добровольно, быстро и подробно рассказывали о собственных провалах. О том, что их взломали, что сотрудник попался на фишинг, патч не поставили вовремя или подрядчик имел доступ, которого не должен был иметь.

Если снять парадную обёртку, система национальной кибербезопасности — это инфраструктура коллективной честности. Она работает настолько, насколько участники готовы признавать собственные ошибки. Не «люди вообще» — а конкретные сотрудники на конкретных должностях, каждый из которых имеет свои причины скрывать правду.

ГосСОПКА требует, чтобы тысячи организаций по всей стране делали нечто глубоко противоестественное: добровольно, быстро и подробно рассказывали о собственных провалах

ЛЮДИ И РОЛИ

Когда говорят «человеческий фактор», обычно представляют бухгалтера, который кликнул по фишинговой ссылке. В реальности же риски человеческого фактора в контуре ГосСОПКА присутствуют в нескольких номенклатурных ролях.

Рядовые сотрудники. Они ведут себя небезопасно не потому, что глупы или необучены. Просто безопасность конкурирует с их основной работой. У бухгалтера KPI по количеству обработанных платежей. У менеджера — по скорости согласований и количеству привлечённых клиентов. У инженера — по аптайму системы. Безопасное поведение почти всегда медленнее небезопасного. Перезвонить контрагенту, чтобы подтвердить реквизиты, — лишние пять минут. Не открывать вложение и написать в ИБ — задержка задачи. Каждый раз человеку приходится делать микровыбор между «сделать работу быстро» и «сделать работу безопасно». Организации же в 99% случаев вознаграждают скорость и наказывают за медлительность.

Фишинговые письма, слабые пароли, пересылка документов через личную почту, установка «нужных программ» — не прояв-

ления безграмотности, а рациональное поведение людей в системе, наказывающей за осторожность.

ИТ- и ИБ-специалисты, которые должны обнаруживать инциденты, классифицировать их и передавать в ГосСОПКА. Казалось бы, их интересы совпадают с интересами системы. Но это не так.

ИБ-специалист, обнаруживший серьёзный инцидент, оказывается перед неприятным выбором. Честный и подробный отчёт в НКЦКИ означает, что кто-то наверху спросит: «А почему вы это допустили?» Неправильно настроенное журналирование, из-за которого часть событий пропала? Патч, который не поставили три недели? Всё это — вопросы к нему лично. Поэтому в ГосСОПКА нередко уходят «стерилизованные» карточки инцидентов: минимум деталей, обтекаемые формулировки, никаких индикаторов компрометации, которые позволили бы другим организациям защититься.

Хуже того, нагрузка на SOC-команды растёт быстрее, чем штат. Российский рынок ИБ переживает острый кадровый дефицит — десятки тысяч незакрытых вакансий. Люди перерабатывают, выгорают, и формальный подход к отчётности становится не ленью, а стратегией выживания: на «нормальные» отчёты просто нет ресурсов.

Менеджмент. На этом уровне рождается самая опасная разновидность человеческого фактора. Не ошибка и не выгорание, а осознанное решение не воспринимать кибербезопасность всерьёз.

И это тоже рационально. Безопасность — отрицательная метрика. Её не видно, когда она работает, но невозможно игнорировать, когда она провалилась. Для руководителя, мыслящего квартальными показателями, вложения в ИБ — расходы без материальной отдачи. В итоге требования ГосСОПКА воспринимаются как ещё одна регуляторная обязаловка, в одном ряду с пожарной инспекцией и экологической отчётностью. Обучение проводится для галочки. Рекомендации НКЦКИ ложатся в стол. Бюджет на ИБ выделяется по остаточному принципу.

Такое отношение руководства к безопасности мгновенно транслируется вниз по всей организации. Сотрудники понимают, что реально их поощряют за увеличение прибыли и оптимизацию бизнес-процессов, а не за движение к абстрактным целям, записанным в политике безопасности. И действуют соответственно.

Все три проблемы — конкуренция безопасности с продуктивностью, самосохранение ИБ-специалистов, безразличие менеджмента и его фиксация на бизнес-показателях — существовали и пять, и десять лет назад. Но сегодня на них давит новый фактор, который быстро ухудшает ситуацию, не давая организациям времени на адаптацию. И этот фактор не очередная хакерская группировка. Это генеративный искусственный интеллект (ИИ).

Людей нужно переучивать на принципиально другую модель — контекстную, а не контентную. Не «выглядит ли это письмо подозрительно?», а «ожидал ли я это письмо?»

ИИ-ФИШИНГ ОБЕСЦЕНИЛ СТАРЫЕ ПОДХОДЫ

Об ИИ-фишинге обычно говорят так: «Атаки стали более качественными». Но это лишь часть правды. Произошло кое-что более серьёзное.

Десятилетиями организации учили сотрудников распознавать фишинг по внешним признакам: кривой логотип, ошибки в русском языке, подозрительный домен отправителя, нелепые формулировки. Весь тренинг строился на идее, что подделку можно отличить от оригинала, если внимательно присмотреться.

Генеративный ИИ уничтожил эту парадигму. Сегодня фишинговое письмо может быть написано безупречным деловым языком, с правильным логотипом, корректным доменом и даже стилистически подстроено под манеру конкретного отправителя. Поддельные сайты неотличимы от настоящих. Визуальный чек-лист с перечнем типовых ошибок перестал работать — ошибок больше нет.

Это не количественное изменение, а качественное. Людей нужно переучивать на принципиально другую модель — контекстную, а не контентную. Не «выглядит ли это письмо подозрительно?», а «ожидал ли я это письмо? Нормально ли для нашего процесса получать такие запросы по этому каналу? Требует ли процедура подтверждения по другому каналу?»

К сожалению, большинство организаций по-прежнему обучают сотрудников по старым материалам, рассказывая о «подозрительных ссылках» и «ошибках в тексте». Они

тренируют людей обнаруживать канувшие в Лету признаки. Это не просто бесполезно, а даже опасно, потому что создаёт ложную уверенность: «Я прошёл тренинг, я умею распознавать фишинг». Нет. Правила игры изменились, а вам об этом не сказали.

Казалось бы, раз проблема с человеческим фактором и устаревшим подходом к обучению очевидна, регуляторы должны были на неё среагировать. Они среагировали. Но получилось не совсем то, что нужно.

ЛОВУШКА КОМПЛАЕНСА

В нормативной базе ГосСОПКА прямо прописаны обязательства по работе с человеческим фактором:

- обучение персонала, ответственного за обеспечение безопасности значимых объектов критической информационной инфраструктуры (КИИ);
- информирование пользователей об актуальных киберугрозах и правилах безопасной работы;
- периодическое подтверждение компетенций специалистов по ИБ.

Требования разумные. Проблема в том, что их формальное выполнение не увеличивает безопасность и не выполняет задачи, поставленные перед ГосСОПКА.

Организация провела обучение — показала слайды, собрала подписи, отчиталась. Теперь она «в комплаенсе». Руководство с чистой совестью считает проблему человеческого фактора решённой, ведь журнал инструктажа подписан. Спросите после этого рядового сотрудника:

- Чем нормальный рабочий процесс отличается от социальной инженерии?
- Куда и в какой форме сообщить о подозрительном письме?
- Как должна выглядеть легитимная просьба об изменении реквизитов?

Ответы вас сильно удивят.

Формальный комплаенс создаёт нечто более опасное, чем незнание,— иллюзию знания. В инженерии безопасности это называется нормализацией отклонений. Система выглядит работающей, все отчёты зелёные, реальная практика тихо дрейфует в произвольную сторону от регламентов, и никто не бьёт тревогу, потому что формально всё в порядке.

Для ГосСОПКА это означает подмену реальности на отчётность. Система вместо актуальной картины угроз получает красиво нарисованную картину комплаенса: X организаций «обучили персонал», Y «внедрили процедуры», Z «провели аудит». Ландшафт отчётности и ландшафт реальных рисков — два разных ландшафта, и с каждой итерацией их отличия всё сильнее. Коллективный иммунитет начинает ставить диагнозы и назначать лечение по данным, которые описывают не болезнь, а бумажное здоровье.

ГДЕ ЛОМАЕТСЯ ЦИКЛ

Идеальная модель работы ГосСОПКА — замкнутый цикл. Сотрудник замечает подозрительное письмо и сообщает в ИБ. Команда классифицирует инцидент, описывает подробно и честно, данные уходят в ГосСОПКА. Оттуда возвращаются индикаторы компрометации, рекомендации, информация о новых векторах. Организация обновляет правила, корректирует обучение. Цикл повторяется, каждый виток усиливает всю экосистему.

Реальность ломает этот цикл в каждой точке. И практически всегда причина в людях, которые играют роли.

Сотрудники молчат о странных письмах. Не потому что не заметили, а потому что боятся «выглядеть глупо» или «создать проблемы». В культуре, где за ошибки наказывают, рациональная стратегия — молчать и надеяться, что пронесёт.

ИБ-специалисты занижают критичность инцидентов, чтобы не запускать процедуру эскалации. Они переклассифицируют атаку в «аномалию», задерживают отчёт до момента, когда информация теряет оперативную ценность. Не потому что хотят навредить, а потому что подробный отчёт о серьёзном инциденте вызовет неприятные вопросы от руководства и регулятора.

Руководство отмахивается от рекомендаций. Не по злому умыслу, а потому что «и так работает». Инвестиции в предотвращение неслучившегося проигрывают инвестициям в видимый рост.

В результате одна и та же схема атаки проходит по отрасли, как огонь по сухостою: каждая следующая жертва не знает об опыте предыдущей, потому что предыдущая промолчала. Цикл не замыкается — он разрывается в точке, где человеку нужно выбрать между самосохранением и честностью. Самосохранение предсказуемо побеждает.

ЧТО РЕАЛЬНО ПОМОГАЕТ

Сказать «нужна культура безопасности» легко. Построить её означает преодолеть мощнейшее организационное сопротивление. Но это возможно, если понять, с чем именно приходится бороться. Вот что может помочь.

Разделить формальные и реальные цели. Первый и самый тяжёлый шаг. Руководство должно вслух произнести: «Наша за-

дача — не отчитаться перед НКЦКИ, а действительно снизить вероятность инцидентов. Это разные задачи, и мы осознанно выбираем вторую». Пока эти приоритеты смешаны, реальная безопасность всегда проиграет комплаенсу, потому что комплаенс проверяем, а безопасность невидима.

Описать нормальные процессы простым языком. Для ключевых сценариев, таких как платежи, изменение реквизитов, выдача доступов, согласование обновлений, должна существовать понятная инструкция, описывающая, как выглядит нормальный процесс. Не стостраничный регламент, а короткое описание, которое помнит каждый участник. Когда сотрудник знает, как должно быть, он способен заметить отклонение. Когда не знает, любая «срочная просьба от директора» выглядит правдоподобно.

Переучить людей на контекстную модель. Старые тренинги, рассказывающие, как искать ошибки в письме, пора списывать. Новая модель выглядит так: «проверяйте контекст, а не контент». Ожидал ли я это сообщение? Нормально ли для нашего процесса получать такие запросы по этому каналу? Есть ли процедура, требующая подтверждения по другому каналу? Это сложнее, чем «ищите кривой логотип», зато работает в эпоху генеративного ИИ.

Встроить ГосСОПКА в обучение как смысл, а не обязанность. Людям стоит объяснять, что происходит, когда они сообщают о подозрительной активности: как их сигнал попадает в национальную систему, как это помогает защитить не только их компанию, но и десятки других организаций по всей стране. Люди охотнее действуют правильно, когда понимают смысл своих действий, а не просто выполняют инструкцию «потому что так надо».

Убрать наказание за честность. Ключевой и самый контринтуитивный шаг.

Сотрудник, который сообщил о фишинге, на который чуть не попался,— герой, а не провинившийся. ИБ-команда, честно описавшая серьёзный инцидент,— ответственные профессионалы, а не виноватые в том, что инцидент произошёл. Пока честность наказывается, люди будут выбирать молчание, и нервная система страны останется слепой именно там, где зрение нужнее всего.

Сделать учения и разборы рутиной. Симулированные фишинговые кампании, сценарии «ложных» запросов от «службы безопасности», тренировки реагирования. Не менее важны разборы реальных инцидентов — без поиска виноватых, с фокусом на процесс: что должно было насторожить, как нужно было действовать. Когда разбор становится обучением, а не трибуналом, люди перестают прятать инциденты.

Чтобы всё сказанное не осталось абстракцией, разберём два вымышленных, но типичных сценария. Детали придуманы, а вот паттерны — нет: подобные ситуации регулярно возникают в российских компаниях, от энергетики до финансов.

СООБЩАТЬ ИЛИ МОЛЧАТЬ

Инженер, который знал процесс. Крупная энергетическая компания, региональный филиал. Инженер техподдержки получает письмо якобы от вендора автоматизированной системы управления технологическими процессами (АСУ ТП): «срочное обновление прошивки» во вложении. Письмо безупречно: правильный домен, корректный деловой стиль, логотип на месте. Ноль визуальных ошибок. Старый навык поиска кривого логотипа тут бы не помог. Но инженер знал, что обновления приходят только через внутренний портал, а не по почте. В итоге он не открывает вложение, а пересылает письмо в службу ИБ. Те обнаруживают вредоносный код и передают индикаторы в ГосСОПКА. В течение суток предупреждение получают десятки организаций отрасли. Нервная система сработала: сигнал прошёл от окончания до мозга и обратно ко всему телу.

Обратите внимание: инженера спасла не «осведомлённость о фишинге». Его спасло знание собственного рабочего процесса и культура, в которой сообщать о подозрительном — норма, а не «создание проблем».

Сотрудник, который не перезвонил. Финансовая организация, центральный офис. Бухгалтер получает в мессенджере сообщение от «руководителя» с просьбой срочно перевести средства на новый счёт контрагента. Аккаунт выглядит настоящим, тон привычный. Сотрудник выполняет перевод, не перезвонив руководителю и не сверившись с процедурой. Мошенничество обнаруживают через несколько часов. Дальше — второй провал: служба ИБ, стремясь минимизировать репутационные последствия, передаёт в ГосСОПКА сверхлаконичный отчёт с минимумом деталей. Деньги потеряны. Другие организации не узнают о схеме атаки. Мошенники продолжают использовать тот же сценарий, потому что нервная система заглушила сигнал на полпути.

Здесь система сломалась дважды: сначала у сотрудника, который не знал процесс или не привык перепроверять, затем у ИБ-команды, выбравшей самосохранение вместо честности.

Разница между двумя историями не в бюджетах на ИБ и не в технологиях. Разница в том, знает ли человек свой рабочий процесс, считает ли нормальным сообщать о подозрениях и не опасается ли наказания за честность.

ЧУВСТВИТЕЛЬНОСТЬ ВАЖНЕЕ ТОЛЩИНЫ БРОНИ

ГосСОПКА не бронежилет, который можно надеть и забыть. Это национальная нервная система, и её эффективность определяется не толщиной стен, а точностью и скоростью сигналов, которые по ней проходят. Сенсоры, регламенты, классификаторы — инфраструктура передачи информации. Но если люди на местах от бухгалтера в региональном филиале до CISO в головном офисе предпочитают молчать, потому что честность обходится дороже молчания, система остаётся слепой.

Человеческий фактор в контуре ГосСОПКА не досадная помеха, которую можно устранить автоматизацией. Это центральный элемент архитектуры. По замыслу система опирается на людей, принимающих правильные решения в правильный момент. Задача — не «убрать» человека из контура, а создать условия, в которых правильное решение становится лёгким, а честность безопасной.

В конечном счёте от того, нажмёт ли конкретный сотрудник кнопку «Сообщить о подозрительном письме», и от того, опишет ли ИБ-команда инцидент без прикрас и купюр, зависит не только безопасность одной организации. От этого зависит, будет ли национальная нервная система чувствовать боль вовремя или останется нечувствительной, пока не станет поздно.

МОНГОЛИЯ

ОБЗОР ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр ВИНОГРАДОВ
ФГУП «ЦНИИХМ»

Сергей МЕНЬШИКОВ
основатель Belarusian InfoSecurity Community

Андрей СИТНОВ
независимый эксперт

Наталья КАЗАНЦЕВА
независимый эксперт

Монголия предпринимает значительные шаги по урегулированию законодательства в сфере информации и её защиты, кибербезопасности. В 2021 году был принят комплект законов, которые составили в Монголии правовую основу для перехода к цифровой трансформации: Закон о прозрачности публичной информации, Закон о защите персональных данных, Закон об электронной подписи, Закон о поставщике услуг виртуальных активов и Закон о кибербезопасности.

Законодательство Монголии о защите персональных данных состоит из Конституции Монголии, Гражданского кодекса, Трудового кодекса, Закона о защите персональных данных, Закона о прозрачности публичной информации, Закона о кибербезопасности, Закона об электронной подписи и других.

ЗАКОН О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Закон о защите персональных данных от 17.12.2021 распространяется на всех физических, юридических лиц и организации без юридического статуса, собирающие, использующие и защищающие персональные данные на территории Монголии.

Данный закон не распространяется на сбор, использование и обеспечение сохранности информации, относящейся к физическому лицу или члену его семьи, если при этом не нарушаются права этого лица на неприкосновенность и свободу; размещение звуко-, видео- и аудиовизуальных записывающих устройств в целях охраны движимого и недвижимого имущества, находящегося в собственности, владении и пользовании лица, а также жизни и здоровья членов его семьи; использование собственной биометрической информации в целях защиты движимого и недвижимого имущества, находящегося в собственности, владении и пользовании лица, а также для хранения информации.

Закон выделяет следующие виды данных (информации):

- *биометрические данные* — данные о теле человека, такие как отпечатки пальцев, радужная оболочка глаз, лица, голоса и признаки физической активности, которые позволяют идентифицировать человека с помощью оборудования и программного обеспечения;
- *генетическая информация* — информация, указывающая на физические, медицинские и наследственные генетические характеристики человека, определяемые путём анализа биологических образцов;
- *информация о переписке* — информация, которой обмениваются с использованием писем, посылок, электронной почты, средств связи и информационных технологий;
- *информация об имуществе* — информация об имуществе, принадлежащем и используемом владельцем информации;
- *личная информация* относится к конфиденциальной информации о человеке и другой информации, которая может прямо или косвенно идентифицировать человека, например, имя родителей человека, его собственное имя, дата рождения, место рождения, место жительства, местонахождение, регистрационный номер гражданского состояния, активы, образование, членство, электронный идентификатор;

ОБЩИЕ СВЕДЕНИЯ

Монголия (монг. Монгол Улс) — государство с наименьшей плотностью населения в мире в Северо-Восточной Азии. Граничит с Россией на севере и Китаем на юге. Не имеет выхода к морю. День обретения независимости — 11 июля 1921 года.

Столица и крупнейший город — Улан-Батор.

Официальный язык — халха-монгольский, с письменностью на кириллице (раньше для его записи использовалось старомонгольское письмо).

Монголия является участником почти всех структур ООН, а также некоторых структур СНГ в качестве наблюдателя.

◆ *конфиденциальная информация о человеке* включает информацию о национальности, этнической принадлежности, религии, убеждениях, состоянии здоровья, переписке, генетической и биометрической информации, личных ключах к цифровой подписи, отбывает ли он наказание и другую. Закон отдельно определяет понятие цифрового идентификатора (имя пользователя информационной системы, которое идентифицирует человека в электронной среде, адрес проводных и беспроводных технологий для электронной почты, социальных сетей и коммуникаций, информации в других типах устройств и информационных системах);

◆ *медицинская информация* — информация о физическом или психическом здоровье человека и доступе к медицинскому обслуживанию.

Закон выделяет различные основания для обработки персональных данных различными субъектами: государственными органами; физическими, юридическими лицами и организациями без юридического статуса.

В законе даётся определение только оператора (контролера данных) — физического, юридического лица или иной организации, которые собирают и используют информацию в соответствии с законом или с согласия владельца информации (субъекта персональных данных). При этом закон проводит различие между оператором и обработчиком путём закрепления их прав и обязанностей, ответственности, способа и требований к правовому оформлению их правоотношений.

Оператор осуществляет сбор, обработку и использование персональных данных на основаниях, предусмотренных законодательством, или с согласия субъекта персональных данных. Оператор может передать ответственность за сбор и иную обработку данных обработчику данных на основании договора. Законодательством предусмотрено, что такой договор должен предусматривать цель сбора и обработки данных, перечень персональных данных и условия защиты прав субъекта персональных данных. Если иное не указано в договоре, обработчику данных запрещается передавать свои обязательства, а ответственность должна быть чётко определена в договоре.

Закон о защите персональных данных соответствует международным стандартам, установленным Общим регламентом Европейского союза по защите данных (GDPR), а также Руководящими принципами ОЭСР (OECD). Он направлен на укрепление доверия среди граждан и содействие инновациям, основанным на данных, при одновременном уважении прав и свобод личности.

Обеспечение соблюдения и регулирование защиты персональных данных в Монголии осуществляется сетью специализированных государственных органов, каждый из которых играет жизненно важную роль в обеспечении выполнения Закона о защите персональных данных. Главными из них являются Национальная комиссия по правам человека и Министерство цифрового развития, инноваций и коммуникаций.

Национальная комиссия по правам человека является надзорным органом и осуществляет следующие полномочия в отношении защиты данных:

◆ контроль выполнения законов и нормативных актов о защите персональных данных, организация работы по информированию и распространению информации относительно обработки персональных данных, представление требований и рекомендаций в соответствующие организации, принятие соответствующих нормативных актов;

◆ рассмотрение жалоб на нарушения прав и свобод человека, допущенные в процессе обработки и защиты персональных данных, либо в случае угрозы такого нарушения, осуществление расследования нарушений по собственной инициативе, представление требований и рекомендаций в соответствующие органы;

◆ предоставление требований и рекомендаций соответствующим организациям в области обработки и защиты чувствительных персональных данных и другие.

Министерство цифрового развития, инноваций и коммуникаций отвечает за формирование и обеспечение соблюдения политики, направленной на защиту персональных данных. Министерство разрабатывает руководящие принципы безопасного использования электронных подписей и защиты закрытых ключей цифровых подписей, а также контролирует выполнение Закона о кибербезопасности. Это гарантирует, что безопасность данных остаётся приоритетной задачей в быстроразвивающемся цифровом пространстве Монголии.

Законодательство в области кибербезопасности включает в себя Конституцию Монголии, Закон о кибербезопасности, Закон о национальной безопасности, Закон о вооружённых силах, Закон о государственной и служебной тайне, Закон о связи, Закон о раз-

ведывательном управлении, Закон о секретности организаций, Закон о прозрачности публичной информации, Закон о личной тайне, Закон об электронной подписи и другие.

ЗАКОН О КИБЕРБЕЗОПАСНОСТИ

Закон о кибербезопасности принят 17.12.2021 и регулирует отношения, касающиеся создания системы, принципов и правовой базы обеспечения кибербезопасности, а также обеспечения безопасности, конфиденциальности и доступности информации в киберпространстве и киберсреде.

К кибербезопасности закон относит обеспечение безопасности, конфиденциальности и доступности информации в киберсреде.

Под киберпространством понимаются материальные и нематериальные платформы, состоящие из интернета и других информационно-коммуникационных сетей, а также взаимозависимых систем, обеспечивающих их функционирование.

Киберсреда означает информационные системы и сетевые среды, обеспечивающие доступ, вход в систему, сбор, обработку, хранение и использование информации, а безопасность — защиту от несанкционированного удаления или изменения.

Обеспечение кибербезопасности включает следующие работы:

- политика, администрирование, содействие;
- технические и технологические меры по обеспечению кибербезопасности;
- предотвращение кибератак и нарушений, а также повышение осведомлённости о них;
- выявление кибератак и нарушений, прекращение их и реагирование на них, меры по восстановлению.

Правительство должно принять общие процедуры обеспечения кибербезопасности, предотвращения, обнаружения и противодействия киберпреступлениям. При этом юридические лица обязаны осуществлять:

- оценку рисков кибербезопасности (юридическое лицо должно иметь в своём штате сотрудника, прошедшего сертификацию в международной профессиональной или стандартизационной ассоциации или эквивалентной организации);
- проверки информационной безопасности (юридическое лицо должно иметь в штате сотрудника, сертифицированного международной профессиональной ассоциацией или организацией, занимающейся стандартизацией, или аналогичной организацией, для проведения аудитов информационной безопасности).

Указанную деятельность осуществляют юридические лица, зарегистрированные в государственном центральном административном органе, отвечающем за цифровое развитие и коммуникации.

Система кибербезопасности в Монголии включает: правительство, внештатный совет по кибербезопасности, центральный государственный административный орган, отвечающий за цифровое развитие и коммуникации, разведывательное агентство, вооружённые силы, полицию, государственные юридические лица, юридические лица, граждан, организации, обладающие критически важной информационной инфраструктурой.

Также законом предусмотрено построение системы борьбы с кибератаками и нарушениями, включающей:

- центр по борьбе с нападениями и нарушениями (национальный центр по борьбе с кибератаками и нарушениями, общественный центр по защите от кибератак и нарушений, центр вооружённых сил по борьбе с кибератаками и нарушениями);
- национальный центр, входящий в структуру разведывательного агентства;
- общественный центр, функционирующий под управлением государственной центральной административной организации, отвечающей за цифровое развитие и коммуникации;
- центр вооружённых сил, функционирующий в рамках структуры организации кибербезопасности вооружённых сил.

Благодаря принятию Закона о кибербезопасности сформированы система и правовая база обеспечения кибербезопасности, урегулированы вопросы координации, содействия и мониторинга между государством, частными и юридическими лицами в обеспечении кибербезопасности. Одним из достижений стало присвоение Монголии в 2024 году 3-й категории (уровень 3, «развивающаяся») в Глобальном индексе кибербезопасности (GCI), выпущенным Международным союзом электросвязи (ITU). Оценивались обязательства страны в области кибербезопасности по пяти показателям: правовому, техническому, организационному, развитию потенциала, сотрудничеству.

* * *

Надеемся, что данный обзор поможет не заблудиться в законодательстве Монголии. Мы постарались облегчить путь изучения и применения на практике нормативных законов и подзаконных актов в области ИБ.

«ОТ ГОСУДАРСТВЕННОГО КАНЦЛЕРА ГРАФА РУМЯНЦЕВА НА БЛАГОЕ ПРОСВЕЩЕНИЕ»

СЛОВОСОЧЕТАНИЯ «РУМЯНЦЕВСКАЯ БИБЛИОТЕКА» И «РУМЯНЦЕВСКИЙ МУЗЕЙ» ЗНАКОМЫ ВСЕМ, КОМУ БЛИЗКА ИСТОРИЯ МОСКВЫ И РОССИИ

Иллюстрация 1.
Румянцевский музей. Открытка

Борис СТОЛПАКОВ
историк криптографии

ДАР «НА ПОЛЬЗУ ОТЕЧЕСТВУ И БЛАГОЕ ПРОСВЕЩЕНИЕ»

200 лет назад в Петербурге скончался граф Николай Петрович Румянцев (1754–1826). Его крупное книжное собрание (более 28 тысяч томов), а также разнообразные коллекции редкостей вместе с особняком, где они размещались, были завещаны как дар — «на пользу Отечеству и благое просвещение».

Н. П. Румянцев замыслил общедоступный музей, знакомящий с историей, искусством и самобытностью России. В согласии с его волей собранные им книги и коллекции составили основу Румянцевского музея, учреждённого в марте 1828 г. указом императора Николая I.

ПУТЕШЕСТВИЕ ИЗ ПЕТЕРБУРГА В МОСКВУ

Интересно проследить замечательную судьбу румянцевских коллекций. В 1845 г. новый музей вошёл в состав Императорской публичной библиотеки. Со временем решено было перевести Румянцевский музей в Москву «в надежде, что его коллекции будут там более востребованы». В 1861 г., вместе с перевозкой коллекций в Москву, началось пополнение библиотечного фонда музея. В него добавили много русских, зарубежных и первопечатных книг из дублетов публичной библиотеки Петербурга.

Как известно, для размещения коллекций был выделен Дом Пашкова на Ваганьковском холме рядом с Кремлём. Там объединились собрания Московского публичного и Румянцевского музеев. Сразу же было утверждено поступление в библиотеку музеев обязательного экземпляра всех книг, выходящих из печати в России.

Московский публичный музей и Румянцевский музей — так официально именовалось новое культурное учреждение. Музеи включали в себя, кроме библиотеки, отделения рукописей, редких книг, древностей и изящных искусств, а также этнографическое, нумизматическое, археологическое и минералогическое отделения.

ДАРЕНИЯ И ПОЖЕРТВОВАНИЯ

Источником пополнения музейного фонда стали дарения и пожертвования. Уже вскоре после от-

Иллюстрация 2. Н. П. Румянцев. С портрета художника Д. Доу

крытия музеи приняли ещё более 300 книжных и рукописных коллекций. В прессе писали, что «Румянцевский музей создавался путём частных дарений и общественного почина». Одним из главных дарителей был император Александр II. Среди его вкладов — и ценные книги, и собрание гравюр из Эрмитажа, и более двухсот живописных полотен. Самым крупным даром стала известная картина «Явление Христа народу» работы А. А. Иванова с этюдами к ней. Их приобрели у наследников художника специально для Румянцевского музея. На начало 1917 г. в библиотеке Румянцевского музея значилось уже 1,2 миллиона единиц хранения.

ПЕРЕИМЕНОВАНИЯ И БЛАГОДАРНАЯ ПАМЯТЬ

С 1917 по 1922 год в ходе массовой национализации частных коллекций в фонды Румянцевского музея поступило огромное количество книг и музейных редкостей. Среди них собрания графов Шереметевых, знаменитого антиквара-букиниста П. П. Шибанова и много других ценностей. Тогда фонды музея выросли до 4 миллионов единиц хранения.

В начале 1920-х годов все некнижные коллекции (живописи, графики, нумизматики, фарфора, минералов и прочие) постепенно стали передавать в другие музеи. Они вошли в состав Государственной Третьяковской галереи, Государственного музея изобразительных искусств имени А. С. Пушкина, Государственного исторического музея и других крупных собраний.

В июле 1925 г. Центральный исполнительный комитет СССР принял постановление о создании на базе библиотеки Румянцевского музея Государственной библиотеки имени В. И. Ленина. Как мы знаем, в 1992 г. она преобразована в Российскую государственную библиотеку.

Такое развитие получило начинание Николая Петровича. Этого уже достаточно для благодарной памяти соотечественников. Но с именем Н. П. Румянцева связано ещё много полезного для нашего Отечества.

ОПЫТ ЕВРОПЫ — НА БЛАГО РОССИИ

Он был средним из трёх сыновей знаменитого полководца Петра Александровича Румянцева-Задунайского. Да и сам Николай Петрович занимал в начале XIX столетия ведущее положение во внутренних и внешних делах России. Опытный дипломат и знаток Европы, в 1802–1810 гг. он — министр коммерции. Одновременно в 1801–1809 гг.— директор Департамента водных коммуникаций. Именно тогда была построена известная Мариинская водная система, составившая основу нынешнего российского Волго-Балта.

При министре Румянцеве наметился подъём экономики России, подкреплённый разработкой нового таможенного тарифа и улучшением путей сообщения. Тогда же делались энергичные попытки увязать в единую систему русскую торговлю в Северной Америке, на Дальнем Востоке и в Китае.

ЗАБОТЫ О «РУССКОЙ АЛЯСКЕ»

Благодаря Румянцеву получила развитие Российско-американская компания, возникшая первоначально как сибирское купеческое объединение. В её задачу стало входить не только обеспечение русских поселенцев Аляски всем необходимым, но и всестороннее изучение новых земель. Император Александр I и Н. П. Румянцев вошли в состав акционеров компании.

Именно по инициативе Н. П. Румянцева и при финансовой поддержке Российско-американской компании в 1803–1806 гг. состоялась первая российская кругосветная экспедиция. Она известна как плавание двух шлюпов — «Надежда» и «Нева» — под командованием И. Ф. Крузенштерна и Ю. Ф. Лисянского.

НА ВЕРШИНЕ ЧИНОВНОЙ ИЕРАРХИИ

С февраля 1808 г. по август 1814 г. Н. П. Румянцев — министр иностранных дел России. Конечно, период говорит сам за себя. Напряжённая обстановка в Европе потребовала от нового министра неослабного внимания к шифровальным делам. За

Иллюстрация 3. Штат Аляска на месте владений Российско-американской компании

такую деятельность в канцелярии МИД отвечали три экспедиции (отделения), включая перлюстрацию. Это было время активного использования кодов. Постоянно требовались новые, усовершенствованные коды. Технический прогресс позволил заменить переписывание кодов их печатью. Для этого в шифровальной экспедиции имелась собственная литография.

Составление кодов и их печать сопровождались, разумеется, распоряжениями по канцелярии МИД. В одном из таких документов, опубликованных Т. А. Соболевой, говорится: «Г. Канцлеру угодно, чтобы Вы, милостивый государь мой, Христиан Иванович, немедленно занялись составлением двух совершенно полных лексиконов как для шифрования, равно как и расшифрования на российском и французском языках, и чтобы Вы снеслись по сему предмету с Александром Фёдоровичем Крейдеманом, стараясь соединёнными силами довести работу сию к скорейшему и успешнейшему окончанию. А. Жерве».

Здесь автор документа — А. А. Жерве, начальник канцелярии МИД при Н. П. Румянцеве. Указаны и двое сотрудников шифровальной экспедиции, Христиан Иванович — Х. И. Миллер — был её начальником. Сам Н. П. Румянцев назван в документе канцлером. Этот чин, высший в империи, Николай Петрович получил после заключения в сентябре 1809 г. весьма удачного мирного договора со Швецией, закрепившего за Россией Финляндию. А с января 1810 г. Н. П. Румянцев стал совмещать пост главы МИД с должностями председателя Государственного совета и Кабинета министров.

В ПАРИЖ «С ОСОБОЙ МИССИЕЙ»

В то время континентальная Европа была фактически объединена под главенством Франции. Возглавив МИД, Николай Петрович в октябре 1808 г. направился в Париж, где провёл четыре месяца «с особой миссией». Во французской столице тогда исполняли свои миссии два действующих министра иностранных дел Н. П. Румянцев и Ш. Талейран, а также два будущих министра — К. Меттерних, в ту пору австрийский посол в Париже, и К. Нессельроде — советник в российском посольстве. Именно Нессельроде составлял кодовые сообщения в Петербург от Н. П. Румянцева и российских послов П. А. Толстого и А. Б. Куракина.

КАК СООБЩАЛИ СЕКРЕТЫ «ТЕРЕНТИЯ ПЕТРОВИЧА» «ЛУИЗЕ»

Опубликованные материалы позволяют нам немного представить себе состав кодов, вышедших из шифровальной экспедиции МИД.

Так, в использовавшихся кодах Талейран обозначался как Мой кузен Анри, Анна Ивановна, Красавец Леандр, Наш книготорговец, Наш библиотекарь, Юрисконсульт. Наполеон именовался Терентий Петрович или Софи Смит. Сменивший Талейрана во главе МИД Франции Шампаньи имел обозначение Наш племянник Серж. Министр полиции Фуше фигурировал как Наташа, Бержьен, Президент.

Александр I именовался Луиза, Румянцев — Моя тётя Аврора, посол Куракин — Андрюша. Сам Нессельроде, не любивший танцы, получил обозначение Танцор. Положение во Франции обозначалось как Английское земледелие, Любовные шашни Бутягина (фамилия секретаря посольства в Париже) и т.д.

ПАМЯТНЫЙ 1812 ГОД

Вероятно, Румянцев добился немалого на поприще публичной и тайной дипломатии. В самом деле, российское руководство вступило в Отечественную войну 1812 года, заранее зная время и место её начала. Знали в Петербурге и численность армии вторжения, и военный план Наполеона. А вот французское руководство ожидали неприятные сюрпризы. Так, всего за месяц до вторжения «двунадесяти языков» Россия заключила мирный договор с Турцией, что позволило перебросить 52-тысячную Дунайскую армию на образующийся западный фронт. Кроме того, Россия вступила в войну, заключив союзные договоры со Швецией, Великобританией и Испанией.

Наполеон рассчитывал на быстрое завершение кампании после одной или нескольких побед в приграничных сражениях. Неожиданное и удачно проведённое отступление русской армии вглубь России сломало этот план, заставив Наполеона задержаться в Вильне на 18 дней. Дальнейший ход военных событий всем хорошо известен.

К сожалению, многолетнее напряжение привело российского канцлера к инсульту с тяжёлыми последствиями. У Румянцева ослабело зрение, он почти потерял слух. Весной 1813 г. он подал прошение об отставке, но получил её лишь спустя год, при этом он пожизненно оставался канцлером.

НОВОЕ ПОПРИЩЕ — БЫТЬ БЛАГОДЕЯТЕЛЬНЫМ

Его деятельная и благородная натура, привычная к принятию обдуманных решений, быстро нашла себе применение. Николай Петрович просто и ясно сформулировал свой замысел в одном из писем к давнему единомышленнику Ивану Фёдоровичу Крузенштерну: «Станем служить всеобщему просвещению, Вы своими пространными познаниями, а я горячим усердием». Напомним, что это было ещё время неоткрытых земель и неизведанных путей.

ИЖДИВЕНИЕМ ГРАФА РУМЯНЦЕВА...

Он организовал на свои средства несколько дальних морских экспедиций. Уже в 1815 г. иждивением графа Румянцева была организована кругосветная экспедиция для открытия Северо-западного прохода: морского пути, соединяющего Тихий и Атлантический океаны в арктических широтах. По представлению Крузенштерна начальником экспедиции на бриге «Рюрик» был назначен О. Е. Коцебу. Но арктические льды перекрыли все пути. В 1818 г. «Рюрик» вернулся в Кронштадт.

Уже в 1819 г. к полярным льдам отправились две новые экспедиции. Румянцев инициировал первую русскую антарктическую экспедицию 1819–1821 гг. на шлюпах «Мирный» и «Восток» под руководством Ф. Ф. Беллинсгаузена и М. П. Лазарева. Как мы знаем, она впервые успешно достигла берегов Антарктиды. Одновременно Николай Петрович снарядил экспедицию М. Н. Васильева и Г. С. Шишмарёва, посланную на шлюпах «Открытие» и «Благонамеренный» в северные полярные воды. Цель этого плавания была та же, что и у плавания брига «Рюрик»,— поиск Северо-Западного прохода..

Поиск Северо-западного прохода ещё сильнее интересовал тогда британское адмиралтейство, да и возможностей у него было побольше. Ведь для достижения цели в Арктике британским кораблям не нужно было совершать кругосветные плавания. Весной 1818 г. на поиск Северо-западного прохода отправились сразу две британские экспедиции. Одна из них на двух кораблях попыталась пройти восточнее Гренландии, держа курс сначала на Север, а затем к Берингову проливу, но не добилась успеха из-за тяжёлых льдов. Другая экспедиция, также на двух кораблях, направилась вдоль западного берега Гренландии, но далее путь и ей преградили льды. Насколько тяжело было британским и российским морякам добиваться своей цели, можно судить хотя бы по тому, что из Северной Атлантики в Тихий океан впервые удалось пройти полностью по воде лишь в 1903–1906 гг. Р. Амундсену на моторной яхте.

«РУМЯНЦЕВСКИЙ КРУЖОК»

Как ни притягательны были морские дали, всё же основным интересом канцлера Румянцева после отставки стали история и археология, поиск и собирание древних реликвий, рукописей и сказаний, издание исторических источников. Как писал В. О. Ключевский, Н. П. Румянцев «стал горячим поклонником национальной русской старины и неутомимым собирателем её памятников».

Вокруг него сложилась большая группа увлечённых людей — «Румянцевский кружок», так его позже стали именовать. Конечно, состав «кружка» весьма условен и к нему относят всех, кому в той или иной форме помогал Николай Петрович. Таких насчитывают до трёхсот человек. «Со многи-

Иллюстрация 4.
Памятник Н. П. Румянцеву в Гомеле

Иллюстрация 5. Особняк Румянцева в Петербурге

ми из своих подопечных он никогда не встречался, ограничиваясь перепиской и денежными премиями. Большую часть времени Румянцев проводил в своём имении в Гомеле и не считал необходимым отвлекать своих корреспондентов от работы, в то же время старался составить протекцию талантливым учёным, помочь им в поисках сподвижников и реализации своих начинаний». Он знакомил, сводил и объединял людей, написал массу рекомендаций, добивался для своих единомышленников разрешения на работу в ведомственных архивах. Многим из тех, с кем общался по переписке, он выделял разовые вознаграждения, некоторым выплачивал ежемесячное пособие.

КАНЦЛЕР-БЛАГОТВОРИТЕЛЬ

Его служение Отечеству и просвещению было искренним и бескорыстным, своим энтузиазмом и интересами он зажигал людей, а его материальная помощь поддерживала их увлечённость. В те годы канцлеру-благотворителю пришлось даже выделить Академии наук крупную сумму на издание её архива, который иначе лежал бы неподвижно в хранилищах. Помогал Румянцев и библиотекам, где работали его стипендиаты, и архиву МИД.

Книги, документы и реликвии вызывали у него особый интерес, даже любовь. Румянцев собрал уникальную библиотеку, а также великолепные коллекции старинных редкостей, монет, медалей, художественных произведений. В своём огромном особняке на Английской набережной в Петербурге он занимал лишь часть этажа, остальное было отдано под размещение коллекций. Умирая, Румянцев завещал передать библиотеку и коллекции Министерству народного просвещения.

ЛЮБИМЫЙ ГОМЕЛЬ

Одновременно с деятельностью на обширном культурном поприще Николай Петрович увлёкся ещё одним делом — обустройством города Гомеля. Гомель достался ему в наследство от отца — прославленного полководца, получившего этот город в потомственное владение при Екатерине II. Именно здесь прошло детство Николая Петровича, родившегося в Петербурге, здесь он провёл в основном и годы зрелости после отставки. Им был разработан генеральный план Гомеля, в соответствии с которым активно велось строительство. Здесь в разное время — и при жизни Н. П. Румянцева, и после его смерти — появились храмы и административные здания, лицей и училища, аптека и больница, гостиный двор и трактиры. Улицы утопали в садах и парках. Немало из созданного тогда сохранилось доныне либо восстановлено по прежним планам.

Николай Петрович Румянцев скончался в Петербурге, но, согласно своему желанию, похоронен в Гомеле, в Петропавловском соборе.

ПАМЯТНАЯ НАДПИСЬ

В центре Петербурга красуется особняк Н. П. Румянцева, лучше сказать, его дворец. Этот замечательный особняк на Английской набережной является ныне филиалом Музея истории Петербурга. О передаче особняка в дар свидетельствует восстановленная надпись под его фронтоном — «от государственного канцлера графа Румянцева на благое просвещение».

«ПРЕДПОЧИТАЮ ЖИВЫХ ЭКСПЕРТОВ...»

PR-ДИРЕКТОР ДВУХ ИБ-КОМПАНИЙ ВЕРОНИКА ГОРЯЧЕВА — О ТОМ, КАК ЖЕНЩИНЕ СТАТЬ СВОЕЙ СРЕДИ БЕЗОПАСНИКОВ И В ЧЁМ ЦЕННОСТЬ PR ДЛЯ БИЗНЕСА, КОТОРЫЙ «ЛЮБИТ ТИШИНУ»

— Вы сейчас возглавляете PR-направление двух ИБ-компаний: Servicepipe и «Спикател». Как получилось, что вы попали в ИБ?

— Мой интерес к самой отрасли возник случайно. В 2016 году я работала в газете «Коммерсант» в отделе финансов. Однажды попала на круглый стол, где обсуждались атаки на банки через АРМ КБР (автоматизированное рабочее место клиента Банка России). Как журналист я понимала, что тема важна и интересна, но участники круглого стола говорили на таком профессиональном языке — с терминами и аббревиатурами, было непонятно. После мероприятия я буквально схватила первого попавшегося безопасника и сказала: «Я журналист, объясните, пожалуйста, о чём шла речь». Он спросил: «Что ты не поняла?» — «Примерно всё». Тогда он начал объяснять — расшифровывая термины, упрощая, опускаясь на базовый уровень и постепенно снова поднимаясь к более сложным вещам. И в какой-то момент я действительно поняла, как это работает, стала задавать вопросы дальше. Так появилась моя первая заметка по ИБ. Насколько я помню, это была едва ли не единственная публикация с той конференции — многие журналисты просто не разобрались в теме. С тех пор я начала писать про информационную безопасность и буквально влюбилась в этот рынок.

— Было сложно войти в этот «рынок»? Есть стереотип, что ИБ — «не для женщин».

— Сложно было, но скорее не из-за гендера, а из-за специфики рынка. В ИБ очень сильное профес-

сиональное комьюнити, где многое строится на репутации, и в целом безопасность любит тишину. Спикеры общаются между собой, знают друг друга, и о журналисте быстро складывается определённое мнение. Чтобы с тобой общались и доверяли, важно доказать, что ты в теме, честна, не стремишься хайповать и сказанное «оф рекордс» так и останется между тобой и спикером. Когда эксперты начинают тебе доверять и обсуждать даже очень чувствительные вопросы, это и есть результат работы с репутацией. Позже, перейдя в пиар, я, по сути, стала заниматься тем же самым, только уже работая с репутацией компании.

— Как произошёл переход из журналистики в пиар?

— В какой-то момент я поняла, что достигла определённого потолка в журналистике — хотелось развития, новых сложных задач, нового масштаба ответственности. И я развернулась и пошла туда, где было сложнее и интереснее. Когда работаешь в ежедневной газете, то привыкаешь к быстрому темпу смены информационной повестки, большому объёму информации, которую необходимо отслеживать, моментально реагировать. И при работе в PR в информационной безопасности, по сути, тот же драйв — появляются новые типы атак, тактики злоумышленников, развиваются продукты, технологии.

Например, когда я пришла в Servicepipe, я и представить себе не могла, что сервис-провайдер защиты от DDoS-атак может активно комментировать тему искусственного интеллекта (ИИ). Но ландшафт киберугроз меняется, компания начала активно внедрять ИИ в свои продукты, наращивать экспертный опыт, и я погрузилась в мир искусственного интеллекта и теперь активно отслеживаю инфополе по этому вопросу, чтоб видеть тренды, предлагать инфоповоды и узнавать у технических специалистов, как тот или иной тренд отразится на нас и на рынке. Сейчас компания активно внедряет технологию fingerprint, а это опять же новый рынок, новые технологии.

В пиаре кибербеза, чтобы оставаться на месте, нужно бежать очень быстро. Чтобы двигаться вперёд — бежать вдвое быстрее.

— Как вас приняла команда?

— Отлично, хотя первое время моя профессия вызывала вопросы. Когда в компании до твоего появления не было PR как функции, то многим кажется непонятным, зачем ты здесь, какая польза от твоего появления. Для технарей пиар — это что-то из области «чёрной магии»: маркетинг приносит лиды, сейл доводит лиды до сделок, дизайнер красивые картинки создаёт, а пиарщик — он про репутацию, что-то абстрактное.

Например, на самом начальном этапе, когда я шла за уточнениями к технарям, часто ловила на себе недоумённый взгляд: «а тебе зачем так глубоко погружаться». Но пиарщику в ИБ важно разобраться, докопаться до сути. И потому, если мне, условно, важно понять, как работает новая тактика при DDoS-атаках, я пойду к тем, кто эти атаки отражал, посмотрю графики атак и т.д.

— Когда стало понятно, что пиар действительно работает, даёт эффект бизнесу?

— PR — в верхней части воронки продаж: сформированное доверие и продемонстрированная экспертность влияют на выбор поставщика, сокращают цикл сделки. Но одно дело — когда я говорю это команде, другое — когда к нам пришёл крупный заказчик и сказал: «Мы прочитали о вас в BIS Journal, готовы поговорить про пилот». Я прекрасно понимаю: лиды — не цель PR, и то, что заказчик связал публикацию с желанием сотрудничать с компанией — косвенный эффект работы. Но тогда мои коллеги увидели прямую связь между тем, что я делаю, и потенциальной выручкой.

К сожалению, эффект от PR в ИБ редко бывает быстрым, доверие в сфере кибербеза формируется годами. Это не история про два пресс-релиза, колонку в «Форбс» и мгновенную известность. Быстро можно стать звездой только на хайпе, комментируя простые популярные темы «для людей». Но какой бы охват и цитируемость ни дал комментарий «самый безопасный пароль для электронной почты», это не повысит доверие целевой аудитории. И потому доверие зарабатываешь медленно, шаг за шагом.

— А собственная оценка эффективности PR в ИБ?

— Есть, конечно, стандартные показатели работы пиарщиков — охват, цитируемость, медиаиндекс и т.д. Но для меня намного важнее ощущение управления инфополем. Когда не просто отвечаешь на запросы СМИ, а буквально задаёшь вектор развития новостной повестке. Например, так пару лет назад мы буквально ввели на рынке термин «ковровые DDoS-атаки», заговорили о сетевых атаках с использованием ИИ, о том, что решения по защите от ботовых атак должны видеть ИИ-агентов... Естественно, все эти треки идут рука об руку с технологиями и экспертизой компании.

Сейчас наши материалы охотно берут СМИ, комментарии запрашивают, компания участвует в престижных рейтингах, продукты получают широкий информационный охват. По сути, задача пиара — сделать так, чтобы потенциальный за-

Одно дело — когда я говорю это команде, другое — когда к нам пришёл крупный заказчик и сказал: «Мы прочитали о вас в BIS Journal, готовы поговорить про пилот»

казчик доверял вам, чтобы сказал сам себе: «Это крутые ребята, я их знаю». А дальше уже начинаются лиды и продажи — работа моих коллег, без которых тоже никуда. И наши сейлы всё чаще слышат эту фразу из уст потенциальных заказчиков. И это моя маленькая победа.

— Вы много говорите о доверии. Оно так важно именно для ИБ-рынка или же это работа PR во всех отраслях?

— Я бы сказала так: потенциальный заказчик должен доверять потенциальному поставщику. Точка. Но в ИБ доверие к экспертизе имеет куда большее значение. Помню показательный кейс с нашего рынка: лет 10 назад представитель некоей компании «А» выступил на профильной конференции с очень-очень слабым, безграмотным докладом. Он широко обсуждался профессиональным сообществом. И до сих пор порой слышу от знакомых CISO утверждение: в компании «А» работают непрофессионалы. Хотя уже никто не помнит, кто именно выступал и в чём была ошибка.

И потому тут ещё один важный момент работы в ИБ. PR часто называют зеркалом бизнеса. И если в некоторых отраслях это зеркало может сильно-сильно приукрашивать реальность без рисков или даже спокойно комментировать малознакомые темы, то в ИБ так нельзя: слишком велика цена ошибки. Потому пиару важно понимать, в чём вы действительно являетесь экспертами и можете озвучивать свою позицию, а какие темы лучше оставить для комментариев другим игрокам рынка.

— Сначала вы пришли в компанию Servicepipe, а в мае прошлого года стали продвигать другую ИБ-компанию — «Спикател». Насколько эти два кейса похожи друг на друга? С чем было сложно или не сложно работать со «Спикателем»?

— Это два совершенно разных кейса и разные стратегии. Когда я пришла в Servicepipe, это была уже известная в профсообществе компания, с репутацией, постоянными серьёзными клиентами. Тут моя задача была просто вынести уже существующую экспертизу и опыт в публичное поле, показать, как динамично развивается компания и её продукты.

Кейс «Спикател» принципиально другой. Компания существовала на рынке с 2018 года — небольшой телеком-игрок с многолетними убытками, название также типично телекомовское. И тут у компании меняется собственник, направление деятельности, фокусировка ИБ, приходит новая команда, привлекаются инвестиции, под капотом продуктов «Спикател» — решения ведущих вендоров... То есть в мае 2025 года появился, по сути, уже совершенно иной «Спикател», которого нужно было вывести на ИБ-рынок.

— Получилось?

— Я считаю, что получилось. Компания в инфополе всего полгода, что является очень небольшим сроком для PR. Особенно на таком высококонкурентном рынке, где игроки с многолетним стажем и историей. Тем не менее голос «Спикател» уже слышен: колонки экспертов компании берут федеральные СМИ, профильные журналисты, весьма придирчиво относящиеся к источникам информации, публикуются исследования «Спикател»... То есть мы идём в нужном направлении, хотя тут работать, работать и ещё раз работать.

— А какие именно шаги были предприняты при создании репутации с нуля?

— Прежде всего, компания должна чётко заявить о себе: кто она, куда движется, какие у неё эксперты, какие инвестиции. Информация должна быть открытой, доступной и прозрачной. Кроме того, при выводе новой компании на рынок также важна репутация — репутация PR-специалиста. Нередко от журналистов можно слышать, мол, пиарщики «достали», «бесполезные создания». Это потому, что на рынке есть действительно определённое количество непрофессионалов, которые в стремлении заработать KPI по цитируемости, охвату не учитывают формат издания, специфику работы самого журналиста, в каком виде необходимо подготовить материал. И потому на первых этапах вывода на рынок, когда ни компанию, ни её экспертов никто не знает, важно активно работать с журналистами, причём не с «Коммерсантом» или «Ведомостями» условно, а с конкретной Марией, которая не любит зубодробительной техники в комментариях и всегда просит абсолюты. Или с Романом, который отлично смотрит на данные в процентах, но ему нужно найти интересный поворот в технологиях и т.д. У меня, например, не возникает вопроса «кому отдать новость», потому что непосредственно во время её подготовки сразу становится ясно, кому из знакомых журналистов она будет интересна. Естественно, и журналисту интересно, когда ему присылают информацию в нужном и удобном лично ему формате.

Второй важный момент — скорость и острота комментария. У некоторых крупных компаний согласование комментария эксперта — это большая цепочка, и каждый из участников этой цепочки убирает то, что его смущает. В итоге комментарии готовятся долго и часто бывают слишком стерильными и скучными. В то же время бывает, когда ответ нужен в течение часа. И именно в небольшой компании, где я могу быстро позвонить техническому директору, за две минуты получить ответ, расшифровать, в мессенджере согласовать и отправить, возможно сделать комментарий за час. В итоге мы выигрываем и по скорости, и по фактуре, так как у нас в комментарии живая нестандартная мысль реального человека, а не плод Chat GPT и коллективного разума из 10 человек.

— Вы против ИИ в работе PR?

— Напротив, я очень даже за. Другое дело, как этот инструмент использовать. Например, ИИ от-

лично помогает расшифровать новые, незнакомые термины, помочь «перевести» сложную статью в профильном СМИ с ИТ-шного языка на русский, найти исследования по нужной тематике. Мало того, я активно использую ИИ-агента, который ежедневно собирает для меня все новости и публикации по интересующей тематике. Но подготовленный экспертом комментарий и текст ИИ — это два разных текста, поскольку искусственный интеллект никогда не даст такой глубины, такого нестандартного взгляда на проблему, как это может сделать живой эксперт.

— Скажите, а как наработать компетенции, чтобы общаться и с журналистами, и с экспертами на одном языке?

— Чтобы наработать компетенции общения, нужно больше общаться. Например, пошла вместе с техническим специалистом кофе попить — он тебе на салфетке прямо в кофе-поинт нарисовал принцип эшелонированной защиты. Правда, это было давно, когда только пришла в компанию, сейчас мне на салфетках ребята куда более сложные вещи рисуют, а когда непонятно, то возвращаются с ноутом, на дашбордах наши решения показывают. При частом общении привыкаешь к профессиональному сленгу, терминам, набираешь экспертный опыт. А дальше просто: сама поняла, значит, могу объяснить другому. Экспертам это также полезно: если он сумел пояснить мне, то сможет при выступлении перед студентами или заказчиками так же легко и просто объяснить сложные вещи.

— Ваши эксперты читают лекции в вузах?

— Иногда. На самом деле всё немного шире: в компании Servicepipe больше года действует образовательный проект по взаимодействию с вузами. Так получилось, что инициировал его PR: я всегда свято верила, что сильная ИБ-компания должна работать с молодёжью, рассказывая о профессии, привлекая в неё новых людей. И мой порыв поддержали наши технари, а также HR — теперь мы организуем разные активности в вузах, ведём канал Service Pipa для юных ИТ- и ИБ-специалистов, экскурсии планируем проводить, ИБ-рилсы снимать. На самом деле это очень классное направление в моей работе, потому как все участники проекта — добровольцы, которым действительно интересно работать с молодёжью. Может, потому наш проект активно развивается без бюджета, рекламы и т.д.

— Как вам удаётся совмещать работу PR-директором сразу в двух компаниях?

— Поверьте, значительно сложнее было совмещать работу в «Коммерсанте» и троих маленьких детей. Например, гуляешь в субботу с детьми в парке, а тут звонит спикер и внезапно хочет дать суперважный комментарий и только сейчас, и ты одной рукой качаешь качели, другой записываешь быстро в блокноте, что он там говорит. Или в дедлайн, во время сдачи статьи редактору у

тебя срочный звонок: «фонетический разбор слова „воробьи“». Если серьёзно, именно многодетность помогла приучиться к тайм-менеджменту, умению работать в условиях многозадачности. Звучит немного пафосно, но это так: мне для переключения с одного проекта на другой, на новую задачу нужны считаные секунды.

— А как вы отдыхаете? Хобби есть?

— Моя подруга часто шутит: «Люди так не работают, как ты отдыхаешь». Для меня отдых — это в первую очередь путешествие, причём не на пляже с бокалом пинаколады, а разные поездки и экскурсии, когда за день проходишь 20 тысяч шагов и узнаёшь столько нового, что вместила б в себя Большая советская энциклопедия. Если говорить о хобби, то люблю пробовать новое: сегодня я занимаюсь боксом, завтра танцую бачату, послезавтра пойду с дочкой на мастер-класс по живописи. Я не боюсь перемен, готова искать своё. Я сменила четыре вуза (в том числе училась на художника-модельера и на инженера-оптика), несколько профессий (от бухгалтера до выпускающего редактора глянцевого журнала). Я привыкла бежать в таком темпе по жизни, мне нравится. И сейчас своё я нашла совершенно точно — это пиар в сфере кибербезопасности.

Беседовала Арина Малькова, студентка 2 курса МосГУ

96,4 ПРОЦЕНТА

Андрей ЖАРКЕВИЧ

В четверг вечером Аня нашла в почтовом ящике письмо. Оно скромно притаилось между квитанцией за коммуналку и рекламой стоматологии. Обычный белый конверт без обратного адреса. Внутри — два листа, исписанных от руки. Почерк она узнала сразу. Серёжа.

Они расстались в октябре — тихо, без скандала. Так, как расстаются взрослые люди, которые не смогли найти друг для друга понятные слова. Он говорил: «Мне нужно время». Она слышала: «Ты мне не нужна». Разница между тем, что человек говорит, и тем, что другой человек слышит,— территория, на которой гибнут отношения.

Четыре месяца тишины. Аня сначала удалила его номер, а потом восстановила из резервной копии. Он не писал в мессенджерах, не звонил. Иногда она видела его активность в соцсетях: лайк под чьим-то постом, комментарий к фотографии. Каждый раз приходилось напоминать себе, что чужая лента — это не реальность, а её кураторская проекция, подобранная алгоритмом специально, чтобы Аня видела именно Серёжину активность, потому что алгоритм знал, что ей интересно, лучше, чем она сама.

Аня села на кухне, включила чайник и начала читать.

Письмо было настоящим. Так ей показалось в первую секунду. И это «показалось» уже ощущалось проблемой, потому что раньше не приходилось оценивать подлинность чужих слов. Раньше письмо было письмом. Теперь оно стало объектом верификации.

Он писал, что скучает. Не красиво, не литературно, а сбивчиво, с повторами, как пишут люди, которые не привыкли формулировать чувства на бумаге. Перечёркнутое слово на первой странице. Смазанные чернила в углу второй. «Я не знаю, зачем пишу это от руки. Наверное, чтобы ты поверила, что это я. Хотя теперь и это не гарантия». Фраза, от которой у Ани сжалось что-то в районе солнечного сплетения — не потому, что красиво сказано, а потому, что это была грустная правда.

Она дочитала. Отложила листы. Допила чай.

Потом достала телефон. Рука сделала это сама — новая привычка, рефлекс, как проверять уведомления или смотреть на часы. Открыла «Контент-щит» — приложение стояло у всех, как антивирус, как определитель номера. Сфотографировала первую страницу. Вторую. Нажала «Проверить».

Четыре секунды. Аня считала про себя.

96,4% — выдало приложение.

Она смотрела на цифру и чувствовала, как что-то внутри, согретое письмом, быстро остывает, как горячий чай, забытый на подоконнике в ноябре.

Нейрогенерация с вероятностью 96,4 процента.

Конечно, она знала, что детекторы врут. Все знали. Об этом писали колонки, получавшие высокие оценки, снимали ролики, которые алгоритм подбирал индивидуально, генерировали автоматические мемы. Но знать — одно, а чувствовать — другое. 96,4 процента — не абстрактная статистика. Это конкретный показатель, доказывающий, что он не писал это сам, а скормил модели промпт «напиши трогательное письмо бывшей девушке, чтобы выглядело как написанное от руки».

Модели научились генерировать «несовершенства» — повторы, оговорки, помарки. Аня даже видела рекламу сервиса, который печатал тексты рукописным шрифтом, неотличимым от реального почерка, на реальной бумаге, с реальными неровностями. Тысяча двести рублей за страницу. Конверт с маркой — бесплатно. Подруга Катя рассказывала, как получила «рукописное» признание от парня с «VK Знакомств» — красивое, трогательное, на двух страницах. А потом нашла тот же текст, слово в слово, в телеграм-канале с промптами для романтических писем. Только имя было другое.

Она набрала его номер. Он ответил после третьего гудка.

— Аня?

— Я получила твоё письмо.

Пауза. Она слышала, как он дышит — или как телефонный микрофон обрабатывает тишину. Сейчас и в этом нельзя было быть уверенным.

— И?..

— Серёж. Ты его сам написал?

Пауза длиннее. Потом — голос, тихий, с той особой интонацией, которая бывает у людей, когда их обвиняют в том, чего они не делали, но не могут доказать:

— Да. Сам. Ручкой. Два часа сидел.

— Я прогнала через «Контент-щит». 96,4.

— Аня...

— Я не говорю, что не верю тебе. Но мне выдало 96,4 процента.

— Ты же знаешь, что эти детекторы...

— Знаю. Всё знаю. И всё равно. Мне нужно быть уверенной, понимаешь? Ты пишешь, что скучаешь. Что думал обо мне каждый день. Это... это важные слова. И мне нужно знать, что их написал ты, а не модель.

Он молчал. Она слушала тишину. Где-то за стеной сосед смотрел сериал, созданный нейросетью специально для него, с актёрами, которых не существовало, по сценарию, который никто не писал.

— Аня,— сказал он наконец.— Если бы я сгенерировал письмо, оно было бы лучше. Без повторов и помарок. Без этого дурацкого предложения на второй странице, которое я переписывал четыре раза и всё равно получилось криво.

Она посмотрела на вторую страницу. «Я не хочу, чтобы ты думала, что я хочу вернуться, то есть я хочу, но не поэтому пишу, а потому что». Предложение, которое не смогло себя закончить. Как их отношения.

— Это и есть доказательство,— сказал он.— Нейросеть не написала бы так плохо.

— Написала бы,— сказала Аня.— Если в промпте указать «пиши коряво, с повторами, как человек, который не умеет выражать чувства».

Тишина.

Она была права. Он тоже был прав. И в этом состояла проблема: оба были правы одновременно, и истина не лежала посередине — она лежала нигде.

Аня могла поверить ему. Решить, что письмо настоящее, что 96,4 — ложное срабатывание, что все мысли и чувства — его. Это был бы акт доверия — тот самый, на котором держатся отношения. Но доверие работает, когда у тебя нет инструмента проверки. Когда единственный способ узнать правду — поверить. А у Ани был «Контент-щит», и цифра 96,4 стояла перед глазами, как диагноз, который нельзя забыть, даже если знаешь, что лаборатория ненадёжная.

— Серёж,— сказала она.— Я не знаю.

— Что ты не знаешь?

— Ничего. Я ничего не знаю.

Она повесила трубку. Положила телефон на стол. Посмотрела на письмо.

Два листа бумаги. Чернила. Почерк, который она узнала бы из тысячи — мелкий, с характерным наклоном влево, с незакрытыми «о» и «а», похожими друг на друга. Слова, от которых полчаса назад сжималось в солнечном сплетении. И число, которое всё отравило — как капля йода на стакан воды: вроде немного, но пить невозможно.

Раньше, до детекторов, до маркировок, до всего вот этого, у людей была роскошь наивности. Получил письмо — читаешь и чувствуешь. Не анализируешь частоту тире, не сканируешь на «паттерны нейрогенерации», не вычисляешь перплексию каждого предложения. Просто читаешь. Просто веришь. Или не веришь — но по человеческим причинам: потому что знаешь, что он врун, или потому что слова расходятся с поступками. А не потому, что приложение на телефоне выдало процент вероятности нейроконтента.

Аня встала, подошла к окну. Внизу суетилась вечерняя Москва. На фасаде дома напротив переливалась вывеска, подобранная персонально для жильца третьего этажа. В кофейне на углу витрина показывала каждому прохожему его любимый десерт. Мир, в котором всё, казалось, было создано для тебя,— и ничего из этого не было настоящим.

Она вернулась к столу. Взяла письмо. Перечитала последнюю строчку: «Не проверяй это через детектор. Пожалуйста. Просто прочитай».

Она его прочитала. Но всё-таки проверила.

Аня аккуратно сложила листы обратно в конверт. Положила конверт на полку у входа — туда, где копились квитанции и непрочитанная реклама на выброс. Ещё одна бумага, на которую можно не отвечать.

Она так и не перезвонила.

ЗАРАЗА ОПТИМИЗМА? ТАК ТОЧНО!

ЗАМЕТКИ БЕЗОПАСНИКА

Александр ИГОНИН
эксперт BIS Journal,
ведущий рубрики

Автору статьи уже очень давно кажется, что практически все большие (а порой и не очень) компании чрезвычайно похожи на армию: куча людей, мало знакомых друг с другом; бесчисленное количество регламентов, которые полностью никто не знает и которые просто невозможно соблюсти, даже если целыми днями только этим и заниматься; чрезвычайно смутная (если вообще имеющаяся) для рядовых исполнителей цель всего происходящего.

Одну из замечательных армейских традиций можно наблюдать, когда в казарму заходит вышестоящий офицер. Дежурный при этом командует «Смирно!», после чего производится доклад, сообщающий, что происшествий не случилось. Причём эта формулировка не изменится, даже если только что произошёл пожар и бóльшая часть казармы уже превратилась в горящие головешки, а китель дежурного объят пламенем.

Примерно такое поведение зачастую взращивается в компаниях. Люди, которые жалуются на завышенные ожидания и нехватку ресурсов, неприятны, неинтересны и не нужны. Менеджмент желает видеть целеустремлённых, настроенных на успех лидеров, которых не пугают амбициозные цели. Мы хотим 24/7 сервис, но у нас только три человека в штате? Не проблема. Компания 10 лет ничего не вкладывала в кибербезопасность, а теперь нужно за полгода всё обезопасить? Сделаем! Ну и традиционный любимый вопрос: как хорошо мы защищены от атак? Очень, очень хорошо защищены — практически полностью.

Однако у красивых презентаций и сладких обещаний есть одна проблема: однажды количество неполной, недостоверной или даже ложной информации с реальностью достигнет закритического уровня, и система начнёт «сыпаться». На практике это может проявиться в виде как некрупных (пропущенная атака или проваленный аудит), так и очень серьёзных последствий вплоть до тяжёлых финансовых проблем. Перед самой катастрофой отчёты и заявления часто становятся особенно оптимистичными и уверенными (вспомним известное «Девальвации не будет... твёрдо и чётко»: кто знает — может, и там за кулисами на самом деле надеялись на хороший вариант).

Конечно, всегда нужно искать какой-то баланс между хмурым пессимистом, заранее убеждённым, что ничего не получится и нет смысла даже пробовать, и радужным оптимистом, готовым за сутки решить проблему, над которой вся индустрия бьётся последние 10 лет. Второй полюс всегда выглядит для собеседников заметно более приятным, но как избыток сахара в организме ведёт к ожирению, так и избыток корпоративного оптимизма может сильно навредить. Давайте в меру наших сил попытаемся почаще «есть овощи», трезво оценивать ситуацию и поменьше её приукрашивать.

Рисунок Йозефа Лады «Солдат Швейк»

Контур Эгида

Экипировка для информационной безопасности

Эгида — сервисы для защиты бизнеса от внутренних угроз

Kaspersky
Unified Monitoring
and Analysis Platform

Мощная и быстрая платформа с расширенными ИИ-возможностями

kaspersky активируй будущее